Algèbre de groupe en caractéristique 1 et distances invariantes sur un groupe fini

Dominique Castella, Stephane Gaubert

Algèbre de groupe en caractéristique 1 et distances invariantes sur un groupe fini

Dominique Castella · Stéphane Gaubert

7 Septembre, 2017

Invariant metrics on a finite group arise in particular in statistics. They turn out to be closely related to the idempotent elements of the group algebra over the min-plus semifield. The central idempotents (corresponding to bi-invariant metrics) are given by the characters of linear representations of this group. We show that these characters can be obtained from irreducible characters, and more generally, that every idempotent has a unique decomposition as a sum of minimal idempotents. We characterize the minimal idempotents, and construct the irreducible characters from the conjugacy classes of the group. This shows in particular that all the invariant metrics are generated by a finite parametric family of invariant metrics, which are Cayley metrics of cyclic subgroups. The usual distances over S_n are easily recovered from this construction. These result partly carry over to infinite groups.

Résumé . Les distances et plus généralement les métriques invariantes sur un groupe fini, utilisées en particulier en statistique, sont étroitement liées aux idempotents de l'algèbre du groupe sur le semi-corps idempotent des réels min-plus. Comme dans le cas classique, les idempotents centraux (qui correspondent aux distances bi-invariantes) sont donnés par les caractères de représentations linéaires de ce groupe. Nous montrons que ces caractères s'obtiennent encore à partir de caractères irréductibles et que plus généralement les idempotents admettent une décomposition unique en somme d'idempotents minimaux. Nous déterminons de façon explicite les idempotents minimaux et nous donnons de même la construction des caractères irréductibles à partir des classes de conjugaison du groupe. Ce travail conduit en particulier à la mise en valeur d'une famille finie de métriques invariantes, à valeurs entières, engendrant toutes les autres : ce sont les métriques de

Dominique Castella
Université de la Réunion
Laboratoire d'Informatique et de Mathématiques, Pôle Technologique Universitaire,
97490 Sainte Clotilde, France
E-mail: dominique.castella@univ-reunion.fr,

Stéphane Gaubert
INRIA Saclay-Île-de France and CMAP,École Polythechnique, UMR 7641 CNRS
CMAP, Route de Saclay, 91128 Palaiseau Cedex, France
E-mail: Stephane.Gaubert@inria.fr

Cayley associées aux sous-groupes monogènes. Les distances usuelles sur S_n s'interprètent alors facilement dans cette construction. Ces résultats se généralisent en partie aux groupes infinis.

1 Introduction

Les métriques sur un ensemble fini ont été étudiées en combinatoire et en programmation linéaire (voir en particulier [CD79], [Avi80], [DP00], [DDP02] ou encore [BD92]). Elles interviennent notamment en analyse phylogénétique ([Bun74], ou [DT98] ou bien [DMT96]). La situation où l'ensemble est muni d'une structure de groupe et où la métrique est invariante (d'un côté ou des deux) apparaît en statistique, voir [Dia88] ou [Cri85], mais aussi en théorie des codes correcteurs. Ces métriques sont alors données par les fonctions longueurs sur le groupe. Les métriques invariantes sur le groupe symétrique S_n, qui incluent par exemple la distance de Hamming, ont été particulièrement étudiées. Nous renvoyons le lecteur à [DH98] pour un tour d'horizon.

Dans cet article, nous considérons les métriques sur un groupe du point de vue de l'algèbre tropicale : la construction de l'algèbre de groupe $k[G]$ s'étend au cas où k est le semi-corps des réels min-plus, $\mathbb{R}_{\min}$. Ce dernier est constitué des éléments de $\mathbb{R} \cup \{+\infty\}$ et muni de l'addition $(a, b) \mapsto \min(a, b)$ et de la multiplication $(a, b) \mapsto a + b$. des réels min-plus. La donnée d'une métrique, invariante d'un côté, équivaut alors à la donnée d'un idempotent de la semi-algèbre de groupe $\mathbb{R}_{\min}[G]$, la donnée d'une métrique invariante des deux côtés à celle d'un idempotent central de cette algèbre. Ceci nous permet de traduire les questions de décomposition des métriques invariantes en termes d'algèbre de groupe, au sens tropical.

Dans le cas classique, l'étude de l'algèbre de groupe $k[G]$ sur un corps k est équivalente à l'étude des représentations linéaires de ce groupe et les idempotents centraux sont donnés par les caractères à valeurs dans le corps. Ils sont donnés par les caractères irréductibles qui forment une base des fonctions centrales sur le groupe. Plus généralement, quand la caractéristique du corps ne divise pas l'ordre du groupe, les idempotents sont sommes d'idempotents minimaux correspondant à des sous-modules simples de l'algèbre de groupe (voir par exemple [Ser78], [CR81] ou [Ren75]).

Nous généralisons ici au cas tropical ces propriétés et, malgré des différences inévitables, nous obtenons des résultats assez similaires qui permettent de décrire les idempotents à partir d'idempotents "minimaux" et les idempotents centraux à l'aide de caractères irréductibles. Ceci permet de décomposer les distances invariantes sur un groupe comme infimum d'une famille de distances associées aux graphes de Cayley des sous-groupes cycliques.

Ces décompositions sont d'autre part étroitement liées à la structure du groupe et en particulier au problème de l'écriture minimale d'un groupe comme réunion de sous-groupes propres ([Bha09], [Coh94] ou [CMN08]).

2 Semi-algèbre de groupe sur un semi-corps idempotent.

2.1 Définitions

Les semi-corps idempotents apparaissent comme les "corps" de la caractéristique 1 et il est possible de développer une algèbre linéaire dans ce cadre ; pour les généralités sur ces structures, on pourra se reporter à [But03] ou encore à [GP97], [CC10], [Gol99], [Les09] ou [Cas10] .

On définit sans difficultés la notion de module sur un tel semi-corps (voir par exemple [CGQ04]).

Dans toute la suite $(k, +, \times)$ désigne un semi-corps idempotent totalement ordonné pour la relation d'ordre induite par l'addition ($a \leqslant b$ si $a + b = b$) ; les éléments neutres respectifs de l'addition et de la multiplication seront notés 0_k et 1_k et G est un groupe fini.

On peut, comme dans le cas classique, considérer l'algèbre de groupe $k[G]$, qui est le k-module libre de base G, la multiplication se déduisant par bilinéarité de la loi de G. On notera 1_G l'élément neutre de G, qui est donc aussi l'élément unité de $k[G]$.

$k[G]$ est un semi-anneau idempotent, intègre (mais non simplifiable, puisque $(1_G + g)^2 \neq 1_G + g^2$ pour $g \neq 1_G$), non commutatif si G n'est pas abélien. On appellera support d'un élément $x = \sum_g x_g g \in k[G]$ la partie de G formée des éléments tels que $x_g \neq 0_k$, (notée $\mathrm{supp}(x)$).

Un élément $e \in k[G]$, $e = \sum_{g\in G} \chi(g)g$ est un idempotent ($e = e^2$) si et seulement si la fonction associée χ, vérifie les égalités $\chi(g) = \sum_{h\in G} \chi(h)\chi(h^{-1}g)$ pour tout $g \in G$, c'est-à-dire si la fonction χ est idempotente pour le produit de convolution.

Dans la suite le terme idempotent sera utilisé au sens d'idempotent *non nul*. On utilisera les deux fonctions suivantes de $k[G]$ dans k :

Définition 1 *Soit $x = \sum_{g\in G} \chi(g)g \in k[G]$; on lui associera les scalaires*

$$M(x) = \sum_{g\in G} \chi(g)$$

et

$$N(x) = \sum_{g\in G, g\neq 1_G} \chi(g) \ .$$

Remarque 2 *On vérifie par un simple calcul que pour tous $x, y \in k[G]$,*

$$M(xy) = M(x)M(y) \ .$$

Proposition 3 *Un élément non nul $e \in k[G]$, $e = \sum_{g\in G} \chi(g)g$ est un idempotent si et seulement si la fonction associée χ, vérifie $\chi(1_G) = 1_k$ ainsi que les inégalités $\chi(gh) \geqslant \chi(g)\chi(h)$ pour tout $(g, h) \in G^2$. $\chi(g)$ est alors nécessairement inférieur ou égal à 1_k pour tout $g \in G$.*

Démonstration L'inégalité $\chi(gh) \geqslant \chi(g)\chi(h)$ résulte aussitôt de l'idempotence. Si e est idempotent, il vient $M(e) = M(e)^2$, et donc $M(e) = 0_k$ ou $M(e) = 1_k$. Le premier cas est exclu car on a supposé $e \neq 0$ et donc $M(e) = 1_k$. Il en résulte que $\chi(g) \leq 1_k$ pour tout $g \in G$ et que $\chi(h) = 1_k$ pour au moins un $h \in G$. Comme $h^n = 1_G$ pour un certain entier n, il vient $\chi(1_G) \geq \chi(h)^n = 1_k$ et donc $\chi(1_G) = 1_k$. Par ailleurs, les conditions énoncées dans la proposition sont trivialement suffisantes.

Remarque 4 *Sur le semi-corps $k = \mathbb{R}_{\min}$ des réels "min-plus", c'est à dire sur le semi-corps $(\mathbb{R} \cup \{+\infty\}, \min, +)$, $e = \sum_g \ell(g)g$ est donc un idempotent si et seulement pour tout couple (g, h) d'éléments de G, $\ell(gh) \leqslant \ell(g) + \ell(h)$, et $\ell(1_G) = 1_k = 0$; ℓ est alors à valeurs positives et est une fonction longueur (ou norme au sens de [Bat95]) sur G (non nécessairement symétrique), ou ce qui est équivalent, la fonction d, définie par $d(g, h) = \ell(g^{-1}h)$ est une métrique invariante à gauche.*

Il est facile de voir que cette fonction d est une distance (finie) si et seulement si, pour tout élément de G, $g \neq 1_G$, $0 < \ell(g^{-1}) = \ell(g) < +\infty$.

Les points dont la distance à l'élément neutre est finie forment un sous-groupe K de G et de même les points dont la distance à 1_G est nulle forment un sous-groupe H ; ces deux sous-groupes sont normaux si d est bi-invariante et dans ce cas la semi-métrique sur G provient donc d'une métrique sur le groupe quotient K/H :

Lemme 5 *Si $e = \sum_{g \in G} \chi(g)g$ est un idempotent d'un groupe fini G, l'ensemble des $g \in G$ tels que $\chi(g) = 1_k$ et l'ensemble des $g \in G$ tels que $\chi(g) > 0_k$ sont des sous-groupes de G.*

Démonstration La fonction χ est idempotente, d'où : $1_k \geqslant \chi(gh) \geqslant \chi(g)\chi(h)$, pour tout couple $(g, h) \in G^2$, ce qui prouve que $H = \chi^{-1}(1_k)$ et $K = \chi^{-1}(]0_k, 1_k])$ sont stables par produit et sont donc des sous-groupes (puisqu'ils contiennent l'élément neutre).

2.2 Idempotents indécomposables

Définition 6 *Un idempotent $e \in k[G]$ est dit indécomposable s'il n'est pas somme d'idempotents strictement plus petits (i.e. vérifie la condition : $e = \sum_i e_i$ où les e_i sont des idempotents, implique que $e = e_i$, pour au moins un i).*
On dira de même qu'une fonction de G dans k idempotente (pour le produit de convolution) est indécomposable si l'idempotent associé l'est, c'est-à-dire que, si elle est la somme d'autres fonctions idempotentes, elle doit être égale à l'une d'elles.

Proposition 7 *Soit n l'ordre du groupe fini G. Pour tout $x = \sum_{g \in G} x_g g \in k[G]$, tel que $M(x) \leqslant 1_k$, on peut définir l'étoile de Kleene de x :*
$x^* = \sum_{k \in \mathbb{N}} x^k = \sum_{0 \leqslant k \leqslant n-1} x^k$ et x^* est un idempotent de $k[G]$.

Démonstration Cette série est stationnaire à partir du rang $n-1$: le support de x^* est inclus dans le sous-groupe H d'ordre $m \leqslant n$, engendré par le support de x. Toute décomposition minimale d'un élément de H en produit g_i d'éléments du support de x, $h = g_1 \cdots g_k$ (i.e. avec k tel que les $g_1 \cdots g_s$ soient tous distincts pour $s \leqslant k$), a donc au plus $m-1$ éléments et les autres décompositions ont des coefficients inférieurs puisque les x_g sont plus petit que 1_k.
Il est alors clair que x^* est bien idempotent.

Proposition 8 *Soit G un groupe fini d'ordre n.*
1) $N(ef) = N(e) + N(f)$ pour tout couple d'idempotents de $k[G]$.
2) A tout élément $g \neq 1_G$ de G, et tout $\lambda \in k$, $\lambda \leqslant 1_k$, on peut associer l'idempotent $e_{\lambda,g} = (\lambda g)^* = \sum_0^{n-1} (\lambda g)^k$ de $k[G]$.
3) Si $f = e_{\lambda,g}$, $N(f) = \lambda$.
Les idempotents $e_{\lambda,g}$ et $e_{\mu,h}$ associés à deux éléments distincts g et h du groupe sont donc différents si $0 < \lambda < 1_k$ ou $0 < \mu < 1_k$.

Démonstration 1) En notant $e = \sum \chi(g)g$, $f = \sum \psi(g)g$ et $ef = \sum \theta(g)g$, on a, pour $g \neq 1_G$, $\theta(g) = \sum_{hk=g} \chi(h)\psi(k) \leqslant N(e) + N(f)$. Comme e et f sont des idempotents $\theta(g) \geqslant \chi(g)\psi(1_G) + \chi(1_G)\psi(g) = \chi(g) + \psi(g)$, d'où l'autre inégalité.

2) Ceci découle de la proposition précédente.

3) Comme $\lambda \leqslant 1_k$, il est immédiat que $N((\lambda g)^*) = \lambda$; si $e_{\lambda,g} = e_{\mu,h}$ on a donc $\lambda = \mu$ et si $0 < \lambda < 1_k$, pour tout $u \in G$, $u \neq 1_G$, $u \neq g$, le coefficient de u est strictement inférieur à celui de g ce qui impose donc $h = g$.

Nous allons montrer que ces idempotents, qui se classent en familles indicées par $[0_k, 1_k]$ dans k, attachées aux éléments de G, sont les idempotents indécomposables et permettent d'obtenir tous les idempotents de $k[G]$:

Proposition 9 *Soit G un groupe fini d'ordre n. Tous les idempotents sont sommes d'une famille finie d'iidempotents $e_{\lambda,g}$, $0_k \leqslant \lambda \leqslant 1_k$, $g \in G$.*
Tous les idempotents indécomposables sont donc de cette forme et les idempotents de cette forme sont tous indécomposables.

Démonstration Soit $e = \sum_g \chi(g)g$ un idempotent de $k[G]$:
considérons les idempotents $f_g = (\chi(g)g)^*$, $(g \neq 1_G)$ et $f = \sum_g f_g$; comme, pour tout g, $e \geqslant \chi(g)g$, on a aussi $e \geqslant f_g$ et donc $e \geqslant f$. Mais $e = \sum_g \chi(g)g \leqslant \sum_g f_g = f$ et on a donc l'égalité.
Ceci prouve que tous les idempotents sont sommes d'une famille finie de f_g et si de plus e est indécomposable, c'est donc l'un de ces idempotents.
Soit maintenant $e = (\lambda g)^*$ pour $\lambda \leqslant 1_k$, $g \in G$:
Si e est la somme d'une famille finie d'idempotents (e_i), chaque e_i étant lui même somme d'idempotents $e_{i,j} = (\lambda_{i,j} g_{i,j})^*$, e peut donc s'écrire comme somme de ces idempotents.
On a nécessairement $\lambda = N(e) \geqslant N(e_{i,j}) = \lambda_{i,j} \geqslant \lambda_{i,j}^{k_{i,j}} = \lambda$, pour au moins un

couple (i,j), avec $g = g_{i,j}^{k_{i,j}}$; on a alors nécessairement, si $\lambda < 1_k$, $k_{i,j} = 1$ et $\lambda = \lambda_{i,j}$, ce qui donne $e = e_{i,j}$ et prouve donc bien que e est indécomposable ; si $\lambda = 1_k$, ce qui précède montre que g appartient au sous-groupe engendré par $g_{i,j}$ et d'autre part $e \geqslant e_{i,j}$ montre réciproquement que $g_{i,j}$ est dans le support de e et appartient au sous-groupe engendré par g ; on a donc encore que $e = g^* = g_{i,j}^* = e_{i,j}$.

Lemme 10 *On a $e_{\lambda,g} \leqslant e_{\mu,h}$, pour deux idempotents indécomposables, si et seulement si g appartient au sous-groupe engendré par h et $\lambda \leqslant \mu^k$ où k est le plus petit entier tel que $g = h^k$.*

Démonstration La condition est nécessaire puisque le coefficient de g dans $e_{\mu,h}$ est justement μ^k.
Réciproquement $\lambda g \leqslant e_{\mu,h}$ implique bien $e_{\lambda,g} = (\lambda g)^* \leqslant e_{\mu,h}$.

La proposition suivante montre qu'un idempotent admet une unique décomposition (à l'ordre près) en somme d'idempotents indécomposables, qui est la somme des indécomposables maximaux parmi ceux inférieurs à cet idempotent :

Proposition 11 *Soit $e = \sum_{g\in G} \theta(g)g$ un idempotent de $k[G]$. Soient $\mathcal{E}$ l'ensemble des idempotents $f_g = (\theta(g)g)^*$ et F l'ensemble des $g \in G$ tels que f_g soit maximal dans $\mathcal{E}$: l'écriture $e = \sum_{g\in F} f_g$ est minimale et toute décomposition de e en somme d'idempotents indécomposables contient ces idempotents.*

Démonstration D'après la proposition précédente, il est clair que l'on a bien $e = \sum_{g\in F} f_g$.
On peut alors remarquer que $e_{\lambda,g} + e_{\mu,g} = e_{\lambda+\mu,g}$ et donc qu'une écriture minimale (c'est-à-dire dont on ne peut enlever aucun terme) comportera au plus un idempotent indécomposable défini par chaque $g \in G$.
Soit alors une telle décomposition en somme d'idempotents indécomposables de e : $e = \sum_{g\in K}(\mu_g g)^*$; pour $g \in F$, $e \geqslant f_g$ implique qu'il existe $h \in G$ tel que $h^k = g$ et $\mu_h^k \geqslant \theta(g)$, soit $(\mu_h h)^* \geqslant f_g$, ce qui par définition de F donne $e_{\mu,h} = (\mu_h h)^* = f_g$.

Remarque 12 *Distance de Cayley :*

Pour obtenir un idempotent à coefficients non nuls, il suffit de partir d'une famille génératrice S et de considérer l'idempotent $e_\lambda = (\lambda \sum_{g\in S} g)^*$ ou, plus généralement, l'idempotent $e_\lambda = (\sum_{g\in S} \lambda^{\ell(g)} g)^*$ où ℓ est définie sur S.
On a alors $e_\lambda = \sum \lambda^{\ell_S(g)} g$ où ℓ_S est ici la fonction longueur prolongée à G en posant $\ell_S(g) = \inf\{\ell(g_1) + \cdots + \ell(g_k) \ / \ g_1 \cdots g_k = g, \forall i, g_i \in S\}$.
Par exemple, pour S_n si l'on prend pour S la classe des transpositions, la longueur d'une transposition est la longueur de sa décomposition minimale en produit de transpositions et la distance associée est la distance de Cayley.
La distance de Hamming s'obtient de même à partir de la famille génératrice S composée des cycles, mais avec $\ell(\sigma)$ égal à la longueur du cycle σ : la distance à l'unité d'un cycle pour la distance de Hamming est égale à la longueur du cycle et pour une permutation le nombre d'éléments déplacés est inférieur ou égal à la somme des longueurs des cycles ; le minimum de cette somme est donc obtenue avec la décomposition en produit de cycles de supports disjoints et est bien égal à la distance de Hamming entre cette transposition et l'identité.

Corollaire 13 *En posant* $\ell_g(h) = \inf\{k \in \mathbb{N} \ / \ h = g^k\}$ *si* h *est dans le sous-groupe engendré par* g*, et* $+\infty$ *sinon, on obtient donc une famille de fonctions longueurs à valeurs entières (et donc de métriques invariantes associées) telle que toute fonction longueur puisse s'écrire comme minimum d'au plus* $n-1$ *fonctions longueurs* $\alpha_g \ell_g$*,* $0 < \alpha_g$*.* ℓ_g *est la fonction longueur associée au graphe de Cayley du sous-groupe monogène engendré par* g*.*

Remarque 14 *Pour* $\lambda = 1_k$*, l'écriture minimale de l'idempotent* $\omega_G = \sum_{g \in G} g$ *donnée par la décomposition en idempotents indécomposables obtenue ci-dessus s'obtient en gardant les* g^* *tels que* g *engendre un sous-groupe cyclique maximal, puisque si* g *engendre le sous-groupe* H*,* $g^* = \omega_H = \sum_{h \in H} h$ *; cette décomposition est donc équivalente à l'écriture de* G *comme réunion de ses sous-groupes cycliques maximaux (en effet* $G = \cup_i H_i$ *équivaut à* $\omega_G = \sum_i \omega_{H_i}$*) ([CMN13] ou [LG16]).*

3 Centre de l'algèbre et caractères

3.1 Centre de l'algèbre

Soient G un groupe fini et k un semi-corps idempotent totalement ordonné. Le centre de ce semi-anneau $Z = Z(k[G])$ est engendré comme habituellement par les éléments $a_C = \sum_{g \in C} g$, où C est une classe de conjugaison de G (puisque pour $x \in Z$ et pour tout $g \in G$, $gxg^{-1} = x$, ce qui implique que les coefficients de deux éléments conjugués sont les mèmes). C'est donc encore un k-module libre de dimension le nombre de classes de conjugaison de G.

La base (θ_C), duale de la base (a_C) de Z, est donc une base de l'ensemble des fonctions centrales (i.e. constantes sur les classes de conjugaison) sur G à valeurs dans k. Un idempotent e est central si et seulement si la fonction idempotente associée χ, (telle donc que $e = \sum_{g \in G} \chi(g) g$) est centrale (i.e. constante sur les classes de conjugaison) et on peut alors écrire $e = \sum_C \chi(a_C) a_C$, où C parcourt l'ensemble des classes de conjugaison de G.

Définition 15 *Une fonction centrale idempotente (pour le produit de convolution) sera appelée caractère idempotent de* G*.*

Remarque 16 *Un caractère idempotent* χ *définit donc un idempotent central de l'algèbre de groupe* $e = \sum \chi(g) g$*.*
La valeur en g *du caractère* χ *est la trace de l'endomorphisme de* $k[G]$*,* $h \longmapsto eg^{-1}h$ *(multiplication par* eg^{-1}*) : ce qui correspond dans le cas classique au fait que le caractère considéré est la trace de la représentation sur* $ek[G]$*, sous-représentation de la représentation régulière.*

On appellera m le nombre de classes de conjugaison distinctes de G, qui est donc aussi la dimension du centre Z de $k[G]$.

3.2 Idempotents irréductibles

Définition 17 *Un idempotent e est dit irréductible s'il est central et s'il n'est pas la somme d'une famille finie d'idempotents centraux strictement inférieurs :*
i.e. si $e = \sum_{i=1}^{n} e_i$, où les e_i sont des idempotents centraux et $n \in \mathbb{N}$, implique que $e = e_i$, pour au moins un i.

On dira de même qu'un caractère idempotent est irréductible si l'idempotent associé l'est, c'est à dire que, s'il est la somme d'autres caractères idempotents, il doit être égal à l'un d'eux.

Nous allons montrer que ces idempotents irréductibles, permettent d'obtenir tous les caractères idempotents et donc tous les idempotents centraux de $k[G]$, et se classent en familles indexées par $[0_k, 1_k]$ dans k, attachées aux classes de conjugaison de G :

Proposition 18 *Soit C_1 la classe de conjugaison réduite à l'élément neutre de G.*
1) Pour toute classe de conjugaison C de G, la suite $((C_1 \cup C)^k)_k$ est croissante et stationnaire à partir d'un rang $p \leqslant m-1$.
2) Pour toute classe de conjugaison C de G et tout $\lambda \in k, \lambda \leqslant 1_k$, la série $(\sum \lambda^k a_C^k)$ converge et $(\lambda a_C)^* = \sum_{n\in\mathbb{N}} (\lambda a_C)^n = \sum_0^{m-1} \lambda^k a_C^k$.
$e_{\lambda,C} = (\lambda a_C)^*$ est un idempotent central de $k[G]$, de caractère associé $(\lambda\theta_C)^*$ (l'étoile s'entendant ici au sens du produit de convolution des fonctions centrales sur G).
3) Tous les idempotents centraux sont sommes d'une famille finie d'idempotents $e_{\lambda,C}$, C parcourant les classes de conjugaison de G, $0 \leqslant \lambda \leqslant 1_k$. Tous les idempotents irréductibles sont donc de cette forme et les idempotents de cette forme sont tous irréductibles.
4) La décomposition minimale d'un idempotent central en somme d'irréductibles est unique (à l'ordre près).

Démonstration 1) Pour tout k, $(C_1 \cup C)^k$ est une réunion de classes de conjugaison : soit n_k le nombre de ces classes. La suite $((C_1 \cup C)^k)$ est croissante et stationne dès que deux termes consécutifs sont égaux ; il en est donc de même de la suite (n_k). Dans le cas non trivial où $C \neq C_1$, $n_1 = 2$ et $n_k \leqslant m$, le résultat est clair.

2) La convergence résulte du a) et le reste de l'assertion se vérifie de manière élémentaire.

3) La preuve est analogue à celle concernant les idempotents indécomposables :
Soit $e = \sum_g \mu_g g = \sum_C \mu_C a_C$ un idempotent central de $k[G]$: considérons les idempotents $f_C = (\mu_C a_C)^*$ et $f = \sum_C f_C$; comme, pour toute classe C, $e \geqslant \mu_C a_C$, on a aussi $e \geqslant f_C$ et donc $e \geqslant f$.
Mais $e = \sum_C \mu_C a_C \leqslant \sum_C f_C = f$ et on a donc l'égalité.
Ceci prouve que tous les idempotents centraux sont sommes des f_C et si de plus e est irréductible, c'est donc l'un de ces idempotents.
Soit $e = e_{\lambda,C}$ pour $\lambda \leqslant 1_k$, C désignant une classe de conjugaison de G.
Si e est la somme d'une famille finie d'idempotents centraux, chacun étant lui

même somme d'idempotents associés à des classes de conjugaisons, il suffit donc, ici encore, de considérer une décomposition $e = \sum(\lambda_i a_{C_i})^*$ et de montrer que l'un de ces idempotents est nécessairement égal à e :
on a donc pour $g \in C$, $\lambda = \lambda_i^r$ pour au moins un i et un $r \in \mathbb{N}$ tel que $C \subset C_i^r$; on a d'autre part $N(e) = \lambda \geqslant N((\lambda_i a_{C_i})^*) = \lambda_i$. D'où, si $\lambda \neq 1_k$, $r = 1$, soit $C = C_i$ et $\lambda = \lambda_i$, ce qui donne le résultat. Si $\lambda = 1_k$, ce qui précède montre que C est incluse dans le sous-groupe H_i engendré par C_i.
L'inclusion de H_i dans le sous-groupe $H = \mathrm{supp}(e)$ est donné par l'inégalité $e \geqslant (\lambda_i a_{C_i})^*$. L'égalité des sous-groupes équivaut ici à l'égalité des idempotents.

4) L'unicité se démontre aussi en suivant la même méthode que pour la décomposition en indécomposables :
on peut d'abord remarquer que $e_{\lambda,C} + e_{\mu,C} = e_{\lambda+\mu,C}$ et donc qu'une écriture minimale comportera au plus un idempotent irréductible défini par chaque classe $C \subset G$.
D'autre part on a encore $e_{\lambda,C} \leqslant e_{\mu,D}$ si et seulement si il existe k tel que $C \subset D^k$ et $\lambda \leqslant \mu^k$. L'écriture minimale de $f = \sum f_C a_C$ s'obtient en prenant uniquement la somme des $e_{f_C,C}$ maximaux dans la famille.

Remarque 19 *Pour $\lambda = 1_k$, la décomposition de l'idempotent $\omega = \sum_{g\in G} g$ obtenue ci-dessus revient à écrire le groupe G comme réunion de sous-groupes normaux engendrés par certaines classes de conjugaisons, et ces sous-groupes seront propres si aucune classe de conjugaisons n'engendre le groupe. Un groupe sera donc "anti-simple" si et seulement l'idempotent ω n'est pas irréductible ([Bha09]).*

La proposition précédente permet aussi de donner une caractérisation simple des idempotents irréductibles, qui ne sont pas de la forme ω_H pour un sous-groupe H de G :

Proposition 20 *1) Si e et f sont deux idempotents centraux, $e + f$ est un idempotent si et seulement si $ef = e + f$.*
2) Un idempotent e, tel que $N(e) \neq 1_k$, est irréductible s'il est central et vérifie la condition :
$e = fg$ où f et g sont deux idempotents centraux implique $e = f$ ou $e = g$.

Démonstration 1) Comme les idempotents sont tous supérieurs à 1_G, ef est un idempotent (car e et f sont centraux) supérieur à $e + f$. Or $(e + f)^2 = e + f + ef$.

2) Supposons vérifiée la condition du 2) : si $e = e_1 + e_2 \cdots + e_n$: on a de même $e \leqslant e_1 e_2 \cdots e_n \leqslant e^n = e$, d'où $e = e_1$ ou $e = e_2 \cdots e_n$ et on a donc le résultat par itération.
Réciproquement il suffit, d'après la proposition précédente, de montrer que les $e_{\lambda,C} = (\lambda a_C)^*$ vérifient cette condition, soit donc que $e_{\lambda,C} = fg$ où f et g sont deux idempotents centraux, implique $e = f$ ou $e = g$:
or on peut écrire $f = \sum e_{\lambda_i,C_i}$ et $g = \sum e_{\mu_i,C_i}$, $1 \leqslant i \leqslant m$ où les C_i sont les m classes de conjugaisons et les λ_i, μ_i des scalaires inférieurs à 1_k.
De l'égalité $e = \sum_{i,j} e_{\lambda_i,C_i} e_{\mu_j,C_j}$ et de $e_{\lambda_i,C_i} e_{\mu_j,C_j} = \sum_{k,l} \lambda_i^k \mu_j^l a_{C_i}^k a_{C_j}^l$ on tire

aisément $N(e) = \lambda = \sum_{i,j}(\lambda_i + \mu_j)$, soit $\lambda = \sup_{i,j}(\lambda_i, \mu_j)$. On peut donc supposer qu'il existe un i tel que $\lambda = \lambda_i$ est maximal (quitte à intervertir f et g) ce qui implique aussi, puisque $\lambda < 1$, $C = C_i$ et donne bien finalement $e \geqslant f \geqslant e_{\lambda_i, C_i} = e$.

Exemple 21 *Mais d'autre part une somme d'idempotents irréductibles n'est pas nécessairement un idempotent :*
En prenant pour G le groupe à 4 éléments $(\mathbb{Z}/2\mathbb{Z})^2 = \{1, a, b, c\}$, avec donc $a^2 = b^2 = c^2 = 1$ et $ab = c$, $1 + a$ et $1 + b$ sont bien deux idempotents irréductibles et $1 + a + b$ n'est pas un idempotent.

Pour remédier à cet état de fait et obtenir une construction directe des idempotents centraux à partir des irréductibles, on peut utiliser d'après ce qui précède le produit au lieu de la somme (le produit de deux idempotents centraux étant bien lui un idempotent) :

Proposition 22 *Les idempotents centraux sont exactement les produits d'idempotents irréductibles.*

Démonstration En effet si e est un idempotent central, on a vu que e était somme d'une famille finie d'idempotents irréductibles, $(f_i)_{1 \leqslant i \leqslant n}$, et $e \geqslant f_i$ pour tout i,ce qui implique $e = e^n \geqslant f_1 \cdots f_n$ et ce produit étant supérieur à la somme est bien aussi plus grand que e.

Remarque 23 *1) Il y a donc $m - 1$ familles d'idempotents irréductibles, données par $m - 1$ familles de caractères irréductibles, pour un groupe G ayant m classes de conjugaison. L'idempotent 1_G qui correspond à la classe de l'élément neutre, s'obtient aussi en faisant $\lambda = 0_k$ dans une de ces familles, si le groupe n'est pas réduit à un élément .*
2) Les idempotents centraux de $k[G]$, et donc les distances bi-invariantes sur G, forment un treillis pour la relation d'ordre usuelle (sur un semi-anneau idempotent) $e \geqslant f$ si $e + f = e$ et donc $ef = e$, puisque les idempotents sont supérieurs à 1_G. $e \geqslant f$ équivaut donc à $ek[G] \subset fk[G]$; cet ordre est donc l'opposé de celui défini par l'inclusion (à l'inverse du cas classique où $ef = e$ indique que f se décompose en $e + (1 - e)f$) :
Le sup de e et f est en effet ef (puisque $ef \geqslant e$, $ef \geqslant f$ et $g \geqslant e$, $g \geqslant f$ implique $g = g^2 \geqslant ef$) et l'inf est $h = \sum \inf(\chi(g), \psi(g))g$ si $e = \sum \chi(g)g$ et $f = \sum \psi(g)$, (puisque h ainsi défini est bien un idempotent inférieur à e et f et que $k \leqslant e$ et $k \leqslant f$ implique $k \leqslant h$).

3.3 Calcul des caractères irréductibles

Proposition 24 *Soit C une classe de conjugaison d'un groupe fini G et $\lambda < 1_k$. On définit, pour g appartenant à la classe de conjugaison D, $i = i(g, C) = i(D, C)$ comme le plus petit entier tel qu'un élément $g \in G$ appartienne à la réunion de classes C^i, s'il existe, sinon on pose $i(g, C) = +\infty$. On a alors pour tout $g \in G$, $\chi_{\lambda,C}(g) = \lambda^{i(g,C)}$, et donc : $e_{\lambda,C} = \sum \lambda^{i(D,C)} a_D$.*
(avec les conventions $C^0 = \{1\}$, et donc $i(1, C) = 0$ pour toute classe C, et $\lambda^{+\infty} = 0_k$, si $\lambda < 1_k$).

Démonstration La proposition découle du calcul de $e_{\lambda,C} = (\lambda a_C)^* = \sum_0^{m-1} \lambda^k C^k$: le coefficient de g dans cette somme est en effet λ^i où i est le premier indice tel que $g \in C^i$.

Remarque 25 *1) Si D n'est pas la classe de 1, les $i(C,D)$ finis sont donc tous inférieurs ou égaux à $m-1$.*
2) En posant, pour chaque classe de conjugaison C, $\ell_C(h) = \inf\{k \in \mathbb{N} \ / \ h \in C^k\}$, si h est dans le sous-groupe engendré par C et $+\infty$ sinon, on obtient donc une famille de fonctions longueurs à valeurs entières, centrales, (et donc de distances bi-invariantes associées) telle que toute fonction longueur centrale puisse s'écrire comme infimum d'au plus $m-1$ fonctions longueurs $\alpha_C \ell_C$, $\alpha_C > 0$.

4 Exemples

Exemple 26 *Pour $G = A_3$ (ou $\mathbb{Z}/3\mathbb{Z}$), et $\rho = (1,2,3)$ les classes sont réduites à un élément et les deux familles d'idempotents irréductibles sont les familles $e_\lambda = (\lambda\rho)^* = 1 + \lambda\rho + \lambda^2\rho^2$, et $f_\lambda = (\lambda\rho^2)^* = 1 + \lambda\rho^2 + \lambda^2\rho$, pour $\lambda \leqslant 1_k$.*

Exemple 27 *Pour G cyclique d'ordre 4 engendré par g, les classes sont aussi réduites à un élément et les trois familles d'idempotents irréductibles sont : $e_\lambda = (\lambda g)^* = 1 + \lambda g + \lambda^2 g^2 + \lambda^3 g^3$, $f_\lambda = (\lambda g^2)^* = 1 + \lambda g^2$, et $h_\lambda = (\lambda g^3)^* = 1 + \lambda g^3 + \lambda^2 g^2 + \lambda^3 g$, pour $\lambda \leqslant 1_k$.*

Exemple 28 *Pour $G = S_3$, en notant σ la transposition $(1,2)$, les classes sont $C_1 = \{1\}$, $C_2 = \{\rho, \rho^2\}$, $C_3 = \{\sigma, \sigma\rho, \sigma\rho^2\}$ et les éléments centraux correspondants 1, $a_2 = \rho + \rho^2$, $a_3 = \sigma + \sigma\rho + \sigma\rho^2$.*
Un calcul facile donne donc ici les deux familles d'idempotents centraux correspondant aux éléments de base : $1 + \lambda a_2, 1 + \lambda^2 a_2 + \lambda a_3$.

Exemple 29 *Pour $G = A_4$, il y a 4 classes de conjugaison, $C_1 = \{1\}$, C_2 formée des produits de deux transpositions de supports disjoints, et deux classes C_3 et C_4 formées des 3-cycles, C_4 étant composée des inverses des éléments de C_3 et vérifiant $C_3^2 = C_4$, $C_4^2 = C_3$, $C_3 C_4 = C_2$.*
Il y a donc aussi 4 éléments dans la base associée du centre qui seront notés a_i pour $1 \leqslant i \leqslant 4$.
Les familles d'idempotents irréductibles associées à ces classes sont :
$(\lambda a_2)^* = 1 + \lambda a_2$
$(\lambda a_3)^* = 1 + \lambda a_3 + \lambda^2 a_4 + \lambda^3 a_2$
et $(\lambda a_4)^* = 1 + \lambda a_4 + \lambda^2 a_3 + \lambda^3 a_2$.

Exemple 30 *Pour $G = S_4$, il y a 5 classes de conjugaison (dont 3 dans A_4) : $C_1 = \{1\}$, C_2 formée des produits de deux transpositions de supports disjoints, D_3 formée des cycles de longueur 3, D_4 formée des transpositions et D_5 des cycles de longueur 4.*
Il y a donc aussi 5 éléments dans la base associée du centre qui seront notés

a_1, a_2, b_3, b_4, b_5 pour éviter la confusion avec les éléments centraux de $k[A_4]$, qui ne le sont plus dans $k[S_4]$ ($b_3 = a_3 + a_4$ donc).
Les 4 familles d'idempotents correspondantes sont :
$e_{2,\lambda} = 1 + \lambda a_2$,
$e_{3,\lambda} = 1 + \lambda^2 a_2 + \lambda b_3$,
$e_{4,\lambda} = 1 + \lambda^2(a_2 + b_3) + \lambda b_4 + \lambda^3 b_5$,
$e_{5,\lambda} = 1 + \lambda^2(a_2 + b_3) + \lambda^3 b_4 + \lambda b_5$.

A noter que $e_{3,\lambda}$ qui est donc irréductible dans $k[S_4]$, ne l'est pas dans $k[A_4]$.

Remarque 31 *On peut voir facilement que la distance de Cayley sur S_n est définie par le caractère associé à la classe des transpositions, et donc dans cet exemple,à D_4 et à l'idempotent $e_{4,\lambda}$; par contre la distance de Hamming n'est pas "irréductible" ; elle est associée sur S_4 à l'idempotent central $1+\lambda^4 a_2+\lambda^3 b_3+\lambda^2 b_4+\lambda^5 b_5$ et donc définie à partir de la distance à l'identité des cycles, égale à leurs longueurs. Une décomposition minimale de cet idempotent est $e_{4,\lambda^2} + e_{3,\lambda^3} + e_{5,\lambda^5}$.*

Exemple 32 *Soit $Q = \{1, -1, i, -i, j, -j, k, -k\}$ le groupe des quaternions.*
Les classes de conjugaison en sont : $C_1 = \{1\}$, $C_2 = \{-1\}$, $C_3 = \{i, -i\}$,$C_4 = \{j, -j\}$ et $C_5 = \{k, -k\}$.
En notant $a_i = \sum_{g \in C_i} g$ pour $1 \leqslant i \leqslant 5$, les familles d'idempotents irréductibles associées aux classes sont :
$1 + \lambda a_2$, $1 + \lambda^2 a_2 + \lambda a_3$, $1 + \lambda^2 a_2 + \lambda a_4$, $1 + \lambda^2 a_2 + \lambda a_5$.

5 Idempotents et caractères symétriques

Les fonctions coordonnées "symétriques" i.e. vérifiant $\chi(g) = \chi(g^{-1})$ correspondent aux fonctions longueurs symétriques et donc aux "métriques symétriques". Dans le cas de S_n les fonctions coordonnées, et donc les caractères centraux, sont tous symétriques car g et g^{-1} sont toujours conjugués (g et g^{-1} ayant même formule). Les distances faibles sont donc toutes des distances.

Pour A_3 (exemple 1) ce sont ceux qui vérifient $\chi(\rho) = \chi(\rho^2)$. Il ne sont donc pas en général irréductibles, sauf 1 et $1 + a_2 + a_3$.

En général les idempotents symétriques sont sommes d'idempotents symétriques minimaux :

Proposition 33 *1) Les idempotents $f_{\lambda,g} = (\lambda(g + g^{-1}))^*$ sont symétriques et tous les idempotents symétriques sont sommes d'idempotents $f_{\lambda,g}$.*
2) $f_{\lambda,g} = e_{\lambda,g} + e_{\lambda,g^{-1}} = (\lambda g)^* + (\lambda g^{-1})^*$.

Démonstration 1) En effet si $f = \sum x_g g$ est un idempotent symétrique et $f \geqslant e_{\lambda,g}$ alors $f \geqslant x_g g^{-1}$ et donc $f \geqslant f_{\lambda,g}$.

2) $(\lambda g + \lambda g^{-1})^* = \sum (\lambda g + \lambda g^{-1})^k = \sum (\lambda g)^k + (\lambda g^{-1})^k$, $\lambda \leqslant 1$ assurant que les autres termes sont plus petits.

Plus généralement si S est une famille génératrice du groupe G, l'idempotent $(\sum_{g\in S}\lambda_g g)^*$ est un idempotent symétrique si S l'est et $\lambda_g = \lambda_{g^{-1}}$ pour tout $g \in S$.

Pour une classe de conjugaison C, on notera C^- la classe des g^{-1} pour $g \in C$; on peut alors donner une famille génératrice d'idempotents "symétriques irréductibles" :

Proposition 34 *Les idempotents centraux $f_{\lambda,C} = (\lambda(a_C + a_{C^-}))^*$ sont symétriques et tous les idempotents symétriques sont sommes d'idempotents $f_{\lambda,C}$.*

Démonstration En effet si $f = \sum_C \lambda_C a_C$ est un idempotent central symétrique, on a $f \geqslant \lambda_C a_C$, d'où $f \geqslant \lambda_C a_{C^-}$ et donc $f \geqslant f_{\lambda,C}$.

Remarque 35 *1) En général $f_{\lambda,C} \neq e_{\lambda,C} + e_{\lambda,C^-}$.*
2) Si l'on regarde les distances classiques invariantes d'un seul côté sur S_n (cf. [Dia88]), associées donc à l'idempotent $e_d = \sum \lambda^{d(1,\sigma)}\sigma$:
- la distance I dite "Kendall's tau", qui compte le nombre minimal de transpositions adjacentes dans la décomposition d'une permutation, est définie par la famille génératrice des $(i, i+1)$, et donc par l'idempotent $e_I = (\lambda \sum(i, i+1))^*$.
- la distance D dite "Footrule" sur S_4 qui provient de la norme 1, ($D(\pi,\sigma) = \sum|\pi(i) - \sigma(i)|$) est aussi définie à partir de la distance à l'identité des permutations et est donc associée à l'idempotent $e_D = (\lambda((1,2)+(2,3)+(3,4))+\lambda^2((1,3)+(2,4)) + \lambda^3(1,4))^*$.
- on peut vérifier que la distance L de Ulam sur S_4, qui pour $\sigma \in S_4$ vaut 4 moins la longueur maximale d'une sous-suite croissante dans la famille $(\sigma(i))$, correspond elle à l'idempotent $e_L = (\lambda((1,2) + (2,3) + (3,4) + (2,3,4) + (1,3,2) + (2,4,3) + (1,2,3,4) + (1,4,3,2)))^*$, c'est à dire qu'elle est entièrement déterminée par les éléments dont la distance à l'identité est 1 (pour lesquels il existe donc une suite croissante de 3 éléments dans l'image).

On peut constater que les familles génératrices considérées sont bien symétriques et que pour la distance de Cayley, il s'agit bien d'une classe de conjugaison de S_n.
On peut voir aussi que pour toutes ces distances usuelles, les transpositions $(i, i+1)$ ont une distance à l'identité égale à 1 et qu'elles sont donc toutes inférieures à la distance de Kendall ; en termes d'algèbre de groupe cela se traduit par le fait que l'idempotent e_I associé à la distance de Kendall est inférieur à celui associé à chacune des autres distances, qui appartient donc toujours à l'idéal $k[G]e_I$: si $e = e^2 \geqslant e_I$, on a $e^2 \geqslant ee_I \geqslant e$ (puisque $e_I \geqslant I_d$) et donc bien $e = ee_I$; ceci peut s'interpréter, par analogie avec le cas classique, en disant que ces distances sont associées à des sous-représentations de la représentation associée à la distance de Kendall.

6 Extension aux groupes infinis

6.1 Cas général

Le semi-corps de base est ici le semi-corps des réels positifs max-plus $k = \mathbb{R}_{\max} = (\mathbb{R}_+, \max, \times)$ (l'ordre de $\mathbb{R}_{\max}$ est donc l'ordre usuel).

Une partie des résultats précédents se généralise aux groupes infinis ; en particulier le lien entre les fonctions idempotentes et les distances invariantes subsiste, ainsi que la décomposition des fonctions idempotentes en sommes (i.e. sup) de fonctions élémentaires :
soit G un groupe ; l'espace des toutes les fonctions de G dans k (dual de l'algèbre de groupe dans le cas fini) sera ici remplacé par l'espace des fonctions majorées :

Remarque 36 *En prenant comme semi-corps de base le semi-corps des réels min-plus $k = \mathbb{R}_{\min} = (\mathbb{R} \cup \{+\infty\}, \min, +)$, l'ordre est inversé par rapport à l'ordre usuel et il faudrait donc considérer l'espace des fonctions minorées (pour l'ordre usuel).*

Définition 37 *Soit G un groupe et k le semi-corps $\mathbb{R}_{\max} = (\mathbb{R}_+, \max, \times)$.*
1) $S(G)$ désignera l'ensemble des fonctions majorées de G dans k.
2) On notera δ_g la fonction de Dirac en $g \in G$ (valant 1_k sur g et 0_k ailleurs).

Proposition 38 *1) $S(G)$ est muni du produit de convolution.*
2) Soit M la fonction définie sur $S(G)$ par $M(\psi) = \sum_g \psi(g)$. La fonction M est multiplicative.

Démonstration 1) En effet le $\chi * \psi(g) = \sup_h \chi(h)\psi(h^{-1}g)$ est fini pour tout $g \in G$ et majoré car pour tout h, $\chi(h)\psi(h^{-1}g) \leqslant M_1 M_2$, si χ est majorée par M_1 et ψ par M_2.

2) Soient ψ_1 et ψ_2 deux éléments de $S(G)$ et (g_n) et (h_n) deux suites d'éléments de G telles que les suites $(\psi_1(g_n))$, $(\psi_2(h_n)))$ tendent respectivement vers $M(\psi_1)$ et $M(\psi_2)$. La suite $(\psi_1(g_n)\psi_2(h_n))$ tend vers $M(\psi_1)M(\psi_2)$ en étant majorée par $M(\psi_1 * \psi_2)$. L'autre inégalité est triviale.

Définition 39 *Soit G un groupe.*
1) On appelera idempotent de $S(G)$ une fonction idempotente de $S(G)$ (pour le produit de convolution), valant 1_k sur 1_G (i.e. égale à son étoile de Kleene).
2) Un caractère de G est un idempotent de $S(G)$ central sur G (i.e. invariant sur les classes de conjugaison de G) .

Proposition 40 *1) Pour $\lambda \in [0,1]$ et $g \in G$, les fonctions $\phi_{\lambda,g} = \sum \lambda^k \delta_{g^k} = (\lambda\delta_g)^*$, sont des idempotents de $S(G)$.*
2) Un idempotent de $S(G)$ est à valeurs dans $[0,1]$.
3) Pour deux idempotents de $S(G)$, ϕ et ψ, $N(\phi * \psi) = N(\phi) + N(\psi)$.

Démonstration 1) Ces fonctions sont clairement bornées et idempotentes et valent bien 1_k sur 1_G.
2) Soit $\psi \in S(G)$ une fonction idempotente non nulle ; on a donc $M(\psi^2) = M(\psi)$ d'où $M(\psi) = 1_k$ puisque $M(\psi)$ ne peut être ni nul ni infini.
3) Ceci résulte aisément de ce que $\phi(1_G) = \psi(1_G) = 1_k$.

Remarque 41 *Les idempotents ψ de $S(G)$, correspondent donc encore aux fonctions longueurs ℓ sur G, par $\ell(g) = -\ln(\psi(g))$ (et directement en prenant comme corps de base $k = \mathbb{R}_{\min}$).*

On obtient comme dans le cas fini une décomposition en somme (ici infinie) d'idempotents élémentaires $(\lambda\delta_g)^*$:

Proposition 42 *Soit G un groupe.*
Tous les idempotents sont sommes d'une famille d'idempotents $(\phi_{\lambda_g,g})$, pour une famille $(\lambda_g)_{g\in G}$, avec $0_k \leqslant \lambda_g \leqslant 1_k$ pour tout g.

Démonstration Soit $\chi = \sum_g \chi(g)\delta_g$ un idempotent de $S(G)$:
considérons les idempotents $f_g = (\chi(g)\delta_g)^*$, $(g \neq 1_G)$ et $f = \sum_g f_g$; comme, pour tout g, $\chi \geqslant \chi(g)g$, on a aussi $\chi \geqslant f_g$ et donc $\chi \geqslant f$.
Mais $\chi = \sum_g \chi(g)\delta_g \leqslant \sum_g f_g = f$ et on a donc l'égalité. Ceci prouve que tous les idempotents sont sommes des f_g.

6.2 Groupes topologiques séparés

Dans le cas des groupes dénombrables on obtient donc une décomposition des idempotents de $S(G)$ en sommes dénombrables d'idempotents élémentaires. Nous indiquons ci-dessous comment on peut généraliser ces décompositions "hilbertiennes" au cas des groupes topologiques séparés, pour les fonctions idempotentes correspondant aux métriques dont les boules sont compactes.

Définition 43 *Soit G un groupe topologique séparé et k le semi-corps $\mathbb{R}_{\max} = (\mathbb{R}_+, \max, \times)$.*
1) Soit f une fonction de G dans k. On dira que f tend vers 0 à l'infini si et seulement si pour tout $\alpha > 0$, $\{g \in G/\chi(g) \geqslant \alpha\}$ est compact.
On notera $S_0(G)$ le sous-espace de $S(G)$ des fonctions tendant vers zéro à l'infini.
2) Pour une partie V de G, on notera I_V la fonction valant 1 sur V et 0 ailleurs.

Proposition 44 *1) Les fonctions tendant vers zéro à l'infini sont semi-continues supérieurement et sont donc aussi bornées sur G.*
2) Pour tout $\lambda \in [0,1[$ et toute partie compacte V de G, la fonction $\phi_{\lambda,V} = \sum \lambda^k I_{V^k} = (\lambda I_V)^*$, est un idempotent de $S_0(G)$.
3) Toute fonction $f \in S_0(G)$ idempotente (non nulle) vérifie $f(1_G) = 1_k$ et est donc un idempotent de $S(G)$, au sens ci-dessus.

Démonstration 1) Comme pour tout $\alpha > 0$, $\{g \in G/\chi(g) \geqslant \alpha\}$ est compact et donc fermé et $\{g \in G/\chi(g) \geqslant 0\} = G$, χ est bien semi-continue supérieurement. Soit alors $H = \{g \in G/\chi(g) \geqslant 1_k\}$; χ étant semi-continue supérieurement est majorée sur H et donc sur G.

2) Comme $\lambda < 1$, pour tout $\alpha > 0$, la partie $\{h \in G \ / \ \phi_{\lambda,V}(h) \geqslant \alpha\} = \{\cup_i V^i \ / \ \lambda^i \geqslant \alpha\}$ est une réunion finie de produits finis de compacts et est donc compacte et fermée.
Les fonctions $\phi_{\lambda,V}$ définies ci-dessus, tendent donc vers 0 à l'infini et appartiennent

bien à $S_0(G)$.

3) Puisque f tend vers zéro à l'infini il existe un compact K tel que $M(f) = \sum_{g\in K} f(g)$ et comme f est semi-continue supérieurement ce sup est atteint sur K : il existe donc un $h \in G$ tel que $f(h) = M(f) = 1_k$.
$H = f^{-1}(1) = \{g \in G / f(g) \geqslant 1_k\}$ est alors une partie de G, non vide, stable (puisque f étant idempotente on a $f(gh) \geqslant f(g)f(h)$) et compacte par hypothèse : on peut alors extraire de la suite (h^n) d'éléments de H une sous-suite convergente (h^{n_k}) et la suite $(h^{n_{k+1}-n_k})$ est alors une suite d'éléments de H qui converge vers 1_G. ; 1_G appartient donc à H et on a bien $f(1_G) = 1_k$.

Remarque 45 *1) Si G est un groupe compact les fonctions semi-continues supérieurement sont bornées et tendent vers 0 à l'infini.*
2) Les fonctions $\phi_{\lambda,V}$ sont semi-continues supérieurement, mais ne sont pas en général continues : si g est d'ordre infini, on peut construire comme ci-dessus une suite (g^{m_k}) convergeant vers 1_G alors que, avec $V = \{g\}$ et $\lambda < 1$, la suite de terme général $\phi_{\lambda,V}(g^{m_k}) = \lambda^{m_k}$ converge vers 0.
3) Les fonctions I_V sont symétriques si V l'est et centrales si V est réunion de classes de conjugaison.
4) Si $\chi \in S(G)$ est une fonction idempotente symétrique, on obtient facilement que $\chi(1_G) = 1$ et ainsi le lien avec les fonctions longueurs (symétriques), en remarquant que $\chi(1_G) \geqslant \chi(g)^2$, pour tout $g \in G$.
5) Les idempotents de $S_0(G)$ correspondent aux métriques invariantes sur G dont les boules sont compactes.

On peut encore obtenir à partir de ces idempotents une décomposition en somme dénombrable des idempotents de $S_0(G)$:

Proposition 46 *Soit G un groupe topologique séparé.*
1) Pour tout idempotent ψ de $S_0(G)$, il existe une famille dénombrable de parties compactes (V_n) et une suite (λ_n) d'éléments de k telles que $\psi = \sum_n (\lambda_n I_{V_n})^*$.
2) Tout caractère de G est somme d'une famille dénombrable de caractères $(\lambda_n I_{V_n})^*$.

Démonstration 1) Soit $(\lambda_n)_{n\in\mathbb{N}}$ une partie dénombrable de $]0,1[$, dense dans $[0,1]$: on considère les $V_n = \{g \in G / \psi(g) \geqslant \lambda_n\}$, non vides qui sont bien des parties compactes de G, par hypothèse. ψ est alors égal à $\phi = \sum_n (\lambda_n I_{V_n})^*$:
Il est clair que $\psi \geqslant \lambda_n I_{V_n}$ et donc $\psi \geqslant (\lambda_n I_{V_n})^*$ pour tout n, (puisque $\psi \geqslant 1 = I_{\{1\}}$) ; on a ainsi $\psi \geqslant \phi$. Pour $g \in G$, et tout $\epsilon > 0$, il existe un p tel que $\psi(g) \geqslant \lambda_p \geqslant \psi(g) - \epsilon$; on a alors $\phi(g) \geqslant (\lambda_p I_{V_p})^*(g) \geqslant \psi(g) - \epsilon$. On a donc $\phi(g) \geqslant \psi(g)$ pour chaque g et finalement donc l'autre inégalité.
On a donc bien $\psi = \sup_n (\lambda_n I_{V_n})^*$.
2) Si de plus ψ est centrale, les $V_n = \{g \in G / \psi(g) \geqslant \lambda_n\}$ sont compactes (car ψ tend vers 0 à l'infini), stables par conjugaisons et donc réunions de classes. Les idempotents $(\lambda_n I_{V_n})^*$ sont donc bien aussi centraux.

Remarque 47 *1) On peut donc associer à un compact V de G la métrique invariante élémentaire d_V, telle que $d_V(g) = k$ si $g \in V^k - \cup_{i<k} V^i$.*

d_V est une distance si V est réunion de classes et si la réunion des puissances de V recouvre tout le groupe.
2) Si le groupe est localement compact, muni d'une distance invariante d, celle-ci est donc donnée par une fonction ψ qui appartient à $S_0(G)$ et se décompose donc en somme de fonctions élémentaires ϕ_{α_p,V_p} : la distance est donc, elle, l'inf de la famille de métriques élémentaires associées.

Acknowledgements Le rapporteur a contribué par ses conseils et suggestions à l'enrichissement de cet article, en particulier de la partie sur les groupes infinis, et à sa lisibilité par sa relecture attentive.
Le premier auteur souhaite aussi particulièrement remercier l'équipe Max-Plus pour ses invitations répétées et son hospitalité.

Références

Avi80. D. Avis. On the extreme rays of the metric cone. *Can. J. Math.*, XXXII(1) :126–144, 1980.

Bat95. V. Batagelj. Norms and distances over finite groups. *J. Combinatorics ISS*, 20 :243–252, 1995.

BD92. H.J. Bandelt and A. Dress. A canonical decomposition theory for metrics on a finite set. *Adv. in Math.*, 92 :47–105, 1992.

Bha09. M. Bhargava. Groups as unions of proper subgroups. *Amer. Math. Monthly*, 116 :413–422, 2009.

Bun74. P. Buneman. A note on the metric properties of trees. *J. of Comb. Th. (B)*, 17 :48–50, 1974.

But03. P. Butkovič. Max-algebra : the linear algebra of combinatorics ? *Linear Algebra Appl.*, 367 :313–335, 2003.

Cas10. D. Castella. Éléments d'algèbre linéaire tropicale. *Linear Algebra Appl.*, 432(6) :1460–1474, 2010.

CC10. A. Connes and C. Consani. Schemes over $\mathbb{F}_1$ and zeta functions. *Compos. Math.*, 146(6) :1383–1415, 2010.

CD79. G. Cohen and M. Deza. Distances invariantes et l-cliques sur certains demi-groupes finis. *Mathématiques et sciences humaines*, 67 :49–69, 1979.

CGQ04. G. Cohen, S. Gaubert, and J. P. Quadrat. Duality and separation theorems in idempotent semimodules. *Linear Algebra Appl.*, 379 :395–422, 2004. E-print arXiv:math.FA/0212294.

CMN08. G.A. Cannon, C.J. Maxso, and K.M. Neuerburg. Rings and covered groups. *J. of Algebra*, 320 :1586–1598, 2008.

CMN13. G.A. Cannon, C.J. Maxso, and K.M. Neuerburg. Ring determined by cyclic covers of groups. *J. of Algebra*, 396 :1–9, 2013.

Coh94. J.H.E. Cohn. On n-sum groups. *Math. Scand.*, 75 :44–58, 1994.

CR81. C. Curtis and I. Reiner. *Methods of Representation Theory*. Wiley, New York, 1981.

Cri85. D. E. Critchlow. *Metric methods for analyzing partially ranked data*, volume 34. Springer-Verlag, 1985.

DDP02. M. Deza, M. Dufour, and E. Panteleeva. Small cones of oriented semi-metrics. *Am. J. Math. and Manag. Sc.*, 22 :199–225, 2002.

DH98. M. Deza and T. Huang. Metrics on permutations, a survey. *J. Combinatorics ISS*, 23 :173–185, 1998.

Dia88. P. Diaconis. *Group representations in probability and statistics*, volume 11 of *Lecture Notes - Monograph Series*. Institute of Mathematical Statistics, Hayward, California, 1988. Edited by Shanti S. Gupta.

DMT96. A. Dress, V. Moulton, and W. Terhalle. T-theory : An overview. *Europ. J. Combinatorics*, 17 :161–175, 1996.

DP00. M. Deza and E. Panteleeva. Quasi-semi-metrics, oriented multi-cuts and related polyhedra. *Europ. J. Combinatorics*, 21 :777–795, 2000.

DT98. A. Dress and W. Terhalle. The tree of life and other affine buildings. *Doc. math.*, ICM III :565–574, 1998.

Gol99. J. Golan. *Semi-rings and their applications*. Kluwer Academic Publishers, Dordrecht, 1999. (Updated and expanded version of The theory of semi-rings, with applications to mathematics and theoretical computer science).

GP97. S. Gaubert and M. Plus. Methods and applications of (max,+) linear algebra. In R. Reischuk and M. Morvan, editors, *Proceedings of the 14th Annual Symposium on Theoretical Aspects of Computer Science (STACS'97)*, number 1200 in Lecture Notes in Comput. Sci., Lübeck, March 1997. Springer.

Les09. P. Lescot. Algèbre absolue. *Ann.Sci.Math.Québec*, 33(1) :63–82, 2009.

LG16. A. Lucchini and M. Garonzi. Irredundant and minimal covers of finite groups. *Com. In Algebra*, 44 :1722–1727, 2016.

Ren75. G. Renault. *Algèbre non commutative*. Herman, Paris, 1975.

Ser78. J.P. Serre. *Représentations linéaires des groupes finis*. Collection Méthodes. Herman, Paris, 1978.