Représentations linéaires des groupes finis

Table des matières

1 Introduction et vocabulaire

1.1 Introduction

Historiquement, la théorie des représentations est apparue pour comprendre un groupe G. Pour cela, un des procédés à notre disposition est de faire agir ce groupe sur un ensemble. Par exemple on fait agir le groupe diédral sur un polygone régulier, le groupe symétrique sur $\{1, \dots, n\}$, le groupe orthogonal sur la sphère, etc. Lorsque l'ensemble possède des éléments remarquables (point distingué, symétries, structure d'espace vectoriel, produit scalaire) il est intéressant de regarder les actions qui respectent des éléments. La théorie des *représentations linéaires* s'intéresse aux actions de groupes sur des espaces vectoriels et cherche à exploiter tous les outils fournis par l'algèbre linéaire pour en tirer des informations sur G.

Un autre point de vue sur la théorie des représentations est fourni par la réduction des endomorphismes d'un espace vectoriel V. Une fois bien connue la théorie de la réduction dans le cas d'un endomorphisme, on passe à la réduction simultanée d'une famille d'endomorphismes. On gagne en souplesse en remplaçant la famille par la sous-algèbre A de $\mathrm{End}(V)$ qu'elle engendre, ou, si les endomorphismes sont tous inversibles, par le sous-groupe G de $\mathrm{GL}(V)$ engendré. Le cas de familles commutantes reste plutôt bien contrôlé (on a par exemple de bons résultats de codiagonalisation ou cotrigonalisation pour ces familles). Dans ce point de vue, on peut considérer que la théorie des représentations linéaires des groupes vise à s'attaquer au cas non commutatif. Dans le cas d'un groupe G fini, dans lequel les éléments sont individuellement d'ordre fini donc diagonalisables (au moins si on est sur le corps des complexes), c'est en tout cas cet aspect non commutatif qui constitue la nouveauté principale.

L'introduction du chapitre du livre de Colmez [Col12] sur les représentations peut être consultée pour avoir quelques compléments.

1.2 Bibliographie

Je recommande particulièrement 4 livres : Colmez [Col12], Peyré [Pey04], Rauch [Rau00], et Serre [Ser98]. Le chapitre de Colmez sur les représentations offre un traitement clair et rapide jusqu'aux relations d'orthogonalité des caractères. Il n'introduit pas l'algèbre de groupe mais introduit explicitement l'opérateur de moyenne. La représentation régulière est introduite en remarque, sans lien avec l'algèbre de groupe, et est peu exploitée. Il est un peu court vers la fin (notamment ne parle pas de transformation de Fourier dans le cas non abélien). Le livre de Peyré est le plus utile pour le cas des groupes abéliens, notamment en ce qui concerne la transformée de Fourier rapide et son application aux calculs de produits de polynômes (chapitre I, puis §§ III.2 et IV.5). Il contient aussi un chapitre bien fait sur la théorie générale dans le cas non abélien (chapitre III). Le livre de Rauch contient de nombreuses remarques intéressantes, et des énoncés qui peuvent faire l'objet d'un développement, par exemple autour des propriétés d'intégralité des caractères (chapitre 6). Par ailleurs, dans les chapitres 4 à 8, les dernières pages proposent une étude détaillée des groupes $\mathbb{D}_4$ $\mathfrak{A}_4$, $\mathfrak{A}_5$, $\mathfrak{S}_4$, $\mathfrak{S}_5$. Ceci inclut la description géométrique de certaines représentations irréductibles liées au cube et aux autres solides platoniciens qui sont tous dessinés, ce qui est remarquable et fort utile pour celle ou celui qui prépare l'Agrégation. Enfin, le livre de Serre est extrêmement complet. La rédaction est claire mais le chapitre 1, rédigé à l'attention d'étudiants chimistes, évite malheureusement l'utilisation de certains outils théoriques et les remplace par des calculs explicites un peu pénibles, par exemple pour démontrer les relations d'orthogonalité. Il ne formule pas vraiment la transformée de Fourier (le terme n'apparaît pas vraiment ; seule est mentionnée la transformée de Fourier inverse).

1.3 Vocabulaire des représentations linéaires

Soient G un groupe. On considère des espaces vectoriels sur un corps K. Pour nos besoins, le corps $\mathbb{C}$ convient pour à peu près tout, même si les corps $\mathbb{R}$ et $\mathbb{Q}$ sont intéressants dans quelques situations. Notre attitude sur ce point sera la suivante : nous travaillons initialement sur K quelconque, et nous ajoutons des conditions au fur et à mesure des besoins. Si V et V' sont deux espaces vectoriels, on note $\mathrm{Hom}(V, V')$ et $\mathrm{End}(V)$ les ensembles d'applications linéaires (ces notations sont plus utilisées que $\mathscr{L}(V, V')$ et $\mathscr{L}(V)$ en théorie des représentations).

1.3.1 Définitions. (1) Une *représentation* de G est la donnée d'un espace vectoriel V et d'un morphisme de groupes $\rho : G \to \mathrm{GL}(V)$. La représentation est dite *fidèle* si ρ est injectif. On appelle *dimension* ou *degré* de la représentation, la dimension de V.

Notation : la représentation est souvent notée V, l'action ρ étant sous-entendue. Pour $g \in G$, l'endomorphisme $\rho(g)$ est fréquemment noté g_V ou simplement g, lorsque cela n'entraîne pas de confusion (il est plus agréable de lire $g_V(x)$ que $\rho(g)(x)$, pour $x \in V$).

(2) Un *morphisme* de $\rho : G \to \mathrm{GL}(V)$ dans $\rho' : G \to \mathrm{GL}(V')$, ou simplement de V dans V', est une application linéaire $f : V \to V'$ telle que $f \circ \rho(g) = \rho'(g) \circ f$, pour tout $g \in G$. On dit aussi que ρ est un G-morphisme de V dans V' et on note $\mathrm{Hom}_G(V, V')$ l'ensemble de ces morphismes. Un *isomorphisme* de V dans V' est un morphisme bijectif.

(3) Une *sous-représentation* W de V est un sous-espace vectoriel qui est G-stable, c'est-à-dire tel que $g(W) \subset W$ pour tout $g \in G$. La *représentation quotient* de V par W est la représentation $\overline{\rho} : G \to \mathrm{GL}(V/W)$ telle que $\overline{\rho}(g) : V/W \to V/W$ est le morphisme induit de $\rho(g) : V \to V$.

1.3.2 Exemples. (1) Tout espace vectoriel V donne naissance à une *représentation triviale* V^{triv} de n'importe quel groupe G, telle que $\rho(g) = \mathrm{id}_V$ pour tout g.

(2) Soit V un espace vectoriel et G un sous-groupe de $\mathrm{GL}(V)$. Alors l'inclusion $G \hookrightarrow \mathrm{GL}(V)$ définit une représentation, qu'on appelle la représentation *naturelle*, ou *tautologique*, de G.

(3) La donnée d'une représentation de $\mathbb{Z}$ (resp. de $\mathbb{Z}^r$) dans V est équivalente à la donnée d'un endomorphisme $f : V \to V$ (resp. de r endomorphismes $f_1, \ldots, f_r$ qui commutent deux à deux). La donnée d'une représentation de $\mathbb{Z}/n\mathbb{Z}$ dans V est équivalente à la donnée d'un endomorphisme f tel que $f^n = \mathrm{id}$.

(4) L'action du groupe symétrique $\mathfrak{S}_3$ sur $V = K^3$ par permutation des coordonnées est une représentation linéaire (le morphisme ρ est donné par les matrices de permutation). L'hyperplan d'équation $x + y + z = 0$ est stable, donc définit une sous-représentation W de dimension 2.

(5) Ici $K = \mathbb{R}$. Le groupe G des isométries (positives ou négatives) du polygone régulier à n côtés est isomorphe à $\mathbb{D}_n$. On obtient ainsi une représentation linéaire réelle de dimension 2 de $\mathbb{D}_n$.

(6) Ici $K = \mathbb{R}$. Le groupe G des isométries positives (déplacements) du cube de $\mathbb{R}^3$ agit sur l'ensemble des quatre grandes diagonales du cube, induisant un isomorphisme $G \xrightarrow{\sim} \mathfrak{S}_4$. On obtient une représentation réelle de dimension 3 de $\mathfrak{S}_4$.

(7) Soit X un ensemble sur lequel G agit. On définit la *représentation de permutation* associée comme étant l'espace vectoriel V de base $(e_x)_{x \in X}$ muni de l'action définie par $g.e_x = e_{gx}$ et étendue par linéarité. Une autre manière de définir cette représentation est de prendre pour V' l'espace vectoriel des fonctions à support fini $a : X \to K$ et de définir l'action par $g.a = a \circ g^{-1}$. On obtient un isomorphisme de représentations $V \simeq V'$ en associant à chaque vecteur $v = \sum_{x \in X} a_x e_x$ la fonction $a : X \to K$ définie par $a(x) = a_x$ (celle-ci est une fonction à support fini par les propriétés d'une base). Cette application $V \to V'$ est bien linéaire, bijective, et le fait que ce soit un G-morphisme provient du calcul suivant : $gv = \sum_{x \in X} a_x g e_x = \sum_{x \in X} a_x e_{gx} = \sum_{y \in X} a_{g^{-1}y} e_y$.

1.3.3 Lemme. *Soit $f : V \to V'$ un morphisme de représentations de G. Alors, le noyau* $\ker(f)$ *est une sous-représentation de V, l'image* $\mathrm{im}(f)$ *est une sous-représentation de V', et l'isomorphisme* $V/\ker(f) \simeq \mathrm{im}(f)$ *est un isomorphisme de représentations.*

Démonstration : Exercice. □

Les constructions habituelles d'algèbre linéaire permettent de fabriquer de nouvelles représentations à partir d'anciennes ; voici quelques exemples.

1.3.4 Définitions. Soient V, V' deux représentations linéaires du groupe G.
(1) La *représentation somme directe* $V \oplus V'$ est définie par $g(v \oplus v') = g(v) \oplus g(v')$.
(2) La *représentation des morphismes* $\mathrm{Hom}(V, V')$ est définie par $g(\varphi) = g \circ \varphi \circ g^{-1}$.
(3) La *représentation duale* V^* est définie par $g(\varphi) = \varphi \circ g^{-1}$.
(4) La *représentation sur les formes bilinéaires* $\mathrm{Bilin}(V)$ est définie par $gb : (x, y) \mapsto b(g^{-1}x, g^{-1}y)$. On notera que l'isomorphisme linéaire $\mathrm{Bilin}(V) \simeq \mathrm{Hom}(V, V^*)$ qui associe à b l'application $u : V \to V^*$, $x \mapsto b(x, -)$, et réciproquement associe à $u : V \to V^*$ la forme bilinéaire b définie par $b(x, y) = [u(x)](y)$, est un isomorphisme de représentations (cela résulte des définitions).

1.3.5 Exercice. Soit V une représentation linéaire de G. Montrez que pour la structure de représentation sur $\mathrm{End}(V)$ définie dans 1.3.4(2), l'action de G se fait par automorphismes de K-algèbre.

Par ailleurs, deux constructions classiques dans le contexte des actions de groupes permettent d'associer à une représentation linéaire un espace vectoriel qui hérite par construction d'une action *triviale* de G : l'espace des points fixes, et l'espace quotient. Voici leur définition précise.

1.3.6 Définitions. Soit V une représentation linéaire du groupe G.
(1) L'*espace des points fixes de V sous G*, ou *invariants de V sous G*, est le sous-espace vectoriel V^G ensemble des $v \in V$ tels que $g(v) = v$ pour tout $g \in G$.
(2) L'*espace quotient de V pour l'action de G* est le quotient $V/G := V/W$ où W est le sous-espace engendré par les vecteurs de la forme $g(v) - v$, pour $v \in V$ et $g \in G$.

Par exemple, si $\varphi \in \mathrm{Hom}(V, V')$ est un point fixe sous l'action de G définie en 1.3.4, pour tout $g \in G$ on a $g \circ \varphi \circ g^{-1} = \varphi$. En appliquant ceci à g^{-1} on obtient $\varphi \circ g = g \circ \varphi$, ce qui signifie que φ est un G-morphisme. En conclusion $\mathrm{Hom}_G(V, V') = \mathrm{Hom}(V, V')^G$.

1.3.7 Lemme. *Soit V une représentation linéaire de G. Alors :*

(1) *tout G-morphisme $f : V' \to V$ de source une représentation triviale $V' = (V')^{\mathrm{triv}}$ se factorise de manière unique en $V' \to V^G \hookrightarrow V$,*

(2) *tout G-morphisme $f : V \to V'$ de but une représentation triviale $V' = (V')^{\mathrm{triv}}$ se factorise de manière unique en $V \to V/G \to V'$.*

Démonstration : Exercice. □

2 L'algèbre d'un groupe fini et la représentation régulière

On suppose dans toute la suite du texte que le groupe G est fini.

2.1 L'espace des fonctions

On note $\mathscr{F}(G,K)$ ou $K[G]$ l'espace vectoriel des fonctions $\varphi : G \to K$. Pour tout élément $g \in G$, on note δ_g la fonction indicatrice définie par $\delta_g(h) = 1$ si $h = g$ et 0 sinon. La famille $\{\delta_g\}$ est une base de $K[G]$; l'espace $K[G]$ est donc de dimension $|G|$. L'écriture d'un élément dans cette base sera de la forme $\varphi = \sum_{g\in G} \varphi(g)\delta_g$ (on écrit parfois aussi $\varphi = \sum_{g\in G} \varphi_g\delta_g$). Cet espace des fonctions possède deux structures remarquables d'algèbre, que nous allons décrire.

2.2 L'algèbre de groupe $(K[G], *)$

Il existe une multiplication qui étend la multiplication de G et qu'il est plus agréable de définir avec la convention de noter simplement g au lieu de δ_g. Un élément typique de $K[G]$ est noté $\varphi = \sum \varphi(g)\, g$. En particulier, on a une injection ensembliste $G \hookrightarrow K[G]$. Il y a une unique manière de définir un produit dans $K[G]$ de manière à ce qu'il soit bilinéaire et étende le produit de G :

$$\varphi * \psi \overset{\text{def}}{=} \Big(\sum_h \varphi(h)\, h\Big)\Big(\sum_k \psi(k)\, k\Big) = \sum_{h,k} \varphi(h)\psi(k)\, hk = \sum_g \Big(\sum_{hk=g} \varphi(h)\psi(k)\Big)\, g.$$

Ce produit est associatif et unitaire, l'unité multiplicative étant l'élément neutre 1 de G.

2.2.1 Définition. Le produit $\varphi * \psi$ ainsi défini est nommé *produit de convolution* de φ et ψ, et l'algèbre $(K[G], *)$ est appelée *algèbre de groupe* du groupe G (ou simplement *algèbre de* G).

On note parfois $\varphi\psi$ au lieu de $\varphi * \psi$. On voit donc que $(\varphi * \psi)(g) = \sum_h \varphi(h)\psi(h^{-1}g)$ et c'est la ressemblance formelle avec une expression du type $(\varphi * \psi)(x) = \int \varphi(t)\psi(x-t)dt$ pour la convolution en analyse qui est à l'origine de la terminologie.

2.2.2 Exemple. Soit G un groupe cyclique d'ordre n. Notons γ un générateur. Considérons le morphisme de K-algèbres $K[X] \to K[G]$ qui envoie l'indéterminée X sur γ, c'est-à-dire le morphisme $P \mapsto P(\gamma)$ d'évaluation en γ. Ce morphisme est surjectif, puisque l'image contient les éléments de G qui engendrent $K[G]$. L'idéal $(X^n - 1)$ est inclus dans le noyau, et on obtient un morphisme induit $K[X]/(X^n - 1) \to K[G]$ qui est un isomorphisme pour des raisons de dimension. (On se méfiera des réflexes liés à la manipulation d'anneaux commutatifs. Les lectrices et lecteurs les plus curieux pourront aller voir l'exercice 8.9 pour la description de l'algèbre de groupe du groupe diédral comme quotient d'un anneau de polynômes non commutatifs.)

Deux propriétés se voient sur la construction. D'abord l'algèbre $K[G]$ est commutative si et seulement si le groupe G l'est. Ensuite, tout élément de G est inversible dans $K[G]$, puisque son inverse dans G est un inverse dans $K[G]$. Mieux, tout morphisme de K-algèbres associatives unitaires $f : K[G] \to A$ envoie G dans le groupe $A^\times$ des inversibles de A, puisque $f(g)f(g^{-1}) = f(gg^{-1}) = f(1) = 1$. En fait, on a la propriété suivante qui caractérise $K[G]$:

2.2.3 Proposition. *Si A est une K-algèbre associative unitaire, l'application qui à $f : K[G] \to A$ associe sa restriction $f_{|G} : G \to A^\times$ est une bijection :*

$$\mathrm{Hom}_{k\text{-Alg}}(K[G], A) \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{Gr}}(G, A^\times).$$

En particulier, si $A = \mathrm{End}(V)$ est l'algèbre des endomorphismes d'un espace vectoriel, toute représentation $G \to \mathrm{GL}(V)$ s'étend de manière unique en un morphisme de K-algèbres $K[G] \to \mathrm{End}(V)$.

$$\begin{array}{ccc} G & \xrightarrow{\forall \rho} & \mathrm{GL}(V) \\ \cap & & \cap \\ K[G] & \dashrightarrow^{\exists ! \widetilde{\rho}} & \mathrm{End}(V) \end{array}$$

Démonstration : Soit $\rho : G \to A^\times$ un morphisme de groupes. Si $\widetilde{\rho} : K[G] \to A$ est un morphisme d'algèbres qui étend ρ, alors par linéarité on doit avoir $\widetilde{\rho}(\sum \varphi(g)\, g) = \sum \varphi(g)\, \widetilde{\rho}(g) = \sum \varphi(g)\, \rho(g)$. Or on vérifie que cette expression, la seule possible pour $\widetilde{\rho}$, définit bien un morphisme d'algèbres. Nous laissons à la lectrice le soin de vérifier que ceci suffit pour établir toutes les assertions de l'énoncé. □

La proposition donne une correspondance entre représentations linéaires de G et représentations linéaires de $K[G]$. Si une représentation d'algèbre $f : K[G] \to \mathrm{End}(V)$ est fidèle, la représentation de groupe $\rho = f_{|G} : G \to \mathrm{GL}(V)$ est fidèle, mais on fera attention au fait que l'inverse n'est pas vrai en général. L'exercice suivant donne un contre-exemple.

2.2.4 Exercice. Ici $K = \mathbb{R}$. Soit G le groupe diédral $\mathbb{D}_3$ à six éléments, engendré par deux éléments r, s tels que $r^3 = s^2 = (rs)^2 = 1$. On représente G dans $\mathbb{R}^2$ par son action sur le triangle équilatéral, i.e. on considère le morphisme injectif $\rho : G \to \mathrm{GL}_2(\mathbb{R})$ qui envoie r sur la matrice de la rotation d'angle $2\pi/3$ et s sur la matrice de la réflexion par rapport à l'axe des abscisses. Montrez que le morphisme $f : \mathbb{R}[G] \to \mathrm{M}_2(\mathbb{R})$ obtenu en étendant ρ n'est pas injectif (regardez les dimensions !). Plus précisément, vous pourrez montrer que le noyau de f est l'idéal bilatère (idéal à gauche et à droite) engendré par $1 + r + r^2$.

Nous terminons en décrivant le centre de $K[G]$. Pour que φ appartienne au centre de $K[G]$, il faut (clairement) et il suffit (car les éléments de G engendrent $K[G]$) que $h\varphi h^{-1} = \varphi$ pour tout $h \in G$. Écrivons $\varphi = \sum \varphi(g)\, g$. En changeant l'indice g en $h^{-1}gh$ dans la somme, on a :

$$h\varphi h^{-1} = \sum_g \varphi(g)\, hgh^{-1} = \sum_g \varphi(h^{-1}gh)\, g.$$

Ainsi $h\varphi h^{-1} = \varphi$ si et seulement si $\varphi(g) = \varphi(h^{-1}gh)$ pour tous g, h. Les fonctions qui vérifient cette propriété portent un nom.

2.2.5 Définition. Une fonction $\varphi : G \to K$ est *centrale* si elle vérifie $\varphi(hgh^{-1}) = \varphi(g)$ pour tous $g, h \in G$, ou de manière équivalente, $\varphi(gh) = \varphi(hg)$ pour tous $g, h \in G$.

Une fonction centrale est une fonction qui est constante sur les classes de conjugaison de G, i.e. une fonction qui passe au quotient en une fonction sur l'ensemble $\mathrm{Conj}(G)$ des classes de conjugaison. Comme sous-algèbre de $K[G]$, le centre de $K[G]$, ensemble des fonctions centrales sur G, s'identifie à l'espace $K[\mathrm{Conj}(G)] \subset K[G]$ dont une base est donnée par les fonctions $\delta_C := \sum_{g \in C} g$, pour $C \in \mathrm{Conj}(G)$. En particulier, sa dimension est égale au nombre de classes de conjugaison de G.

2.3 La représentation régulière

2.3.1 Définition. La *représentation régulière* $R : G \to \mathrm{GL}(K[G])$ est la représentation de G sur $K[G]$ définie par l'action de G par multiplication à gauche, i.e.

$$g(\sum_h \varphi(h)\, h) \overset{\text{def}}{=} \sum_h \varphi(h)\, gh = \sum_k \varphi(g^{-1}k)\, k.$$

Si on pense aux éléments de $K[G]$ comme à des fonctions $\varphi : G \to K$, alors $g\varphi = \varphi \circ g^{-1}$.

2.3.2 Remarque. La représentation définie ci-dessus doit en fait être appelée *représentation régulière gauche*, car il existe une *représentation régulière droite* $R_{\mathrm{d}} : G \to \mathrm{GL}(K[G])$, moins utilisée. Elle est définie par l'action (à gauche) de G par multiplication à droite sur $K[G]$ i.e.

$$g(\sum_h \varphi(h)\, h) \overset{\text{def}}{=} \sum_h \varphi(h)\, hg^{-1} = \sum_k \varphi(kg)\, k.$$

2.3.3 Lemme. *La représentation régulière $R : G \to \mathrm{GL}(K[G])$ est fidèle, et s'étend en un morphisme injectif $f : K[G] \hookrightarrow \mathrm{End}(K[G])$.*

Démonstration : Soit $\varphi \in K[G]$ tel que $f(\varphi) = 0$. Ceci signifie que $\varphi\psi = 0$ pour tout $\psi \in K[G]$, en particulier pour $\psi = 1$ on obtient $\varphi = 0$. □

On voit que la représentation régulière possède la vertu de donner lieu à une représentation matricielle de l'algèbre $K[G]$, ce que ne permettent pas toutes les représentations fidèles, voir 2.2.4. Elle fournit une description de l'algèbre de groupe $\mathbb{R}[\mathbb{D}_3]$ comme sous-algèbre de $\mathrm{M}_6(\mathbb{R})$.

2.4 L'opérateur de moyenne

On suppose toujours que G est fini et, dans toute la suite, que son cardinal est inversible dans K.

En théorie des représentations, l'idée de moyenniser pour rendre invariant est fondamentale. Elle se concrétise souvent par l'utilisation de la « moyenne des éléments de G » qui est l'élément

$$M \overset{\text{def}}{=} \frac{1}{|G|}\sum_{g\in G} g$$

de $K[G]$. Cet élément agira comme un opérateur dans toutes les représentations de G. Il est introduit dans [Col12], exemple I.1.15. Nous l'appellerons *opérateur de moyenne* ou *moyenniseur*.

2.4.1 Lemme. *L'élément $M = \frac{1}{|G|}\sum_{g\in G} g$ possède les propriétés suivantes :*

(1) *$gM = Mg = M$ pour tout $g \in G$. En d'autres termes, M est central dans $K[G]$.*

(2) *$M^2 = M$. En d'autres termes, M est idempotent.*

Pour toute représentation linéaire $\rho : G \to \mathrm{GL}(V)$, l'image de M par l'extension $\widetilde{\rho} : K[G] \to \mathrm{End}(V)$ définit un endomorphisme $M_V : V \to V$ qui est un projecteur d'image égale au sous-espace des points fixes de V.

Démonstration : Notons $M = \frac{1}{|G|}\sum_h h$, en changeant l'indice h en $g^{-1}h$ on obtient :

$$gM = \frac{1}{|G|}\sum_h gh = \frac{1}{|G|}\sum_h h = M.$$

On montre de même que $Mg = M$ pour tout g. Ensuite on calcule :

$$M^2 = \left(\frac{1}{|G|}\sum_g g\right)M = \left(\frac{1}{|G|}\sum_g gM\right) = \left(\frac{1}{|G|}\sum_g M\right) = M.$$

Pour une représentation linéaire $\rho : G \to \mathrm{GL}(V)$, on en déduit immédiatement que M induit un projecteur $M_V : V \to V$ d'image incluse dans le sous-espace V^G des points fixes de V. En fait cette inclusion est une égalité, car si $x \in V^G$ on a $g_V(x) = x$ pour tout $g \in G$, donc $M_V(x) = x$. □

Considérons l'exemple de $G = \mathbb{Z}/n\mathbb{Z}$. On a :

$$K[G] \simeq K[X]/(X^n - 1) \simeq K[X]/(X - 1) \times K[X]/(1 + X + \cdots + X^{n-1}).$$

L'élément $M = \frac{1}{n}(1 + X + \cdots + X^{n-1})$ est représenté par $(1, 0)$ dans l'algèbre produit de droite.

2.5 L'algèbre $L^2(G)$

Ici $K = \mathbb{C}$. L'algèbre $(\mathbb{C}[G], *)$ peut être munie du produit scalaire hermitien standard :

$$(\varphi, \psi) = \frac{1}{|G|}\sum_{g\in G} \varphi(g)\overline{\psi(g)}.$$

Ce produit est invariant sous G. L'algèbre $(\mathbb{C}[G], *)$ munie de ce produit hermitien est parfois notée $L^2(G)$ par analogie avec la théorie L^2 des fonctions.

2.6 L'algèbre des fonctions $(K[G], \cdot)$

Sur l'espace $K[G]$ qui est aussi l'espace vectoriel $\mathscr{F}(G, K)$ des fonctions $\varphi : G \to K$, existe un autre produit, donné par la multiplication des fonctions sur les valeurs. Le produit $\varphi\psi : G \to K$ est défini par $(\varphi\psi)(g) = \varphi(g)\psi(g)$. Il fait de $K[G]$ une K-algèbre associative et unitaire *commutative*, isomorphe à l'algèbre produit $K \times \cdots \times K$. L'unité multiplicative est la fonction constante égale à 1, c'est-à-dire l'élément $\sum_{g\in G} g$. Nous noterons $(K[G], \cdot)$ la structure d'algèbre ainsi définie pour la distinguer de l'algèbre de groupe $(K[G], *)$.

On notera que la définition de $(K[G], \cdot)$ n'utilise pas la structure de groupe de G. En ce sens, elle peut sembler moins intéressante que $(K[G], *)$. Cependant, dans le cas où G est abélien, elle apparaît de manière cruciale dans la transformation de Fourier qui est un isomorphisme

$$\mathscr{F} : (K[G], *) \xrightarrow{\sim} (K[\widehat{G}], \cdot).$$

Au but, la structure de groupe de G entre en jeu via la définition du groupe dual $\widehat{G}$. Le produit des fonctions sur les valeurs est aussi important dans l'application pour la multiplication rapide de grands polynômes. Ces notions seront développées dans la partie 7 spécifique au cas abélien.

3 Semi-simplicité

On rappelle que G est fini, de cardinal $|G|$ inversible dans K.

3.1 Existence de supplémentaires stables

3.1.1 Théorème. *Soit V une représentation de G. Alors, toute sous-représentation $W \subset V$ admet un supplémentaire stable, c'est-à-dire un supplémentaire en tant que représentation.*

Démonstration : On note $M = \frac{1}{|G|}\sum g$ le moyenniseur. Rappelons qu'il y a une correspondance entre supplémentaires de W et projecteurs sur W, donnée ainsi : à W' on associe le projecteur sur W parallèlement à W', et à p on associe son noyau. On peut voir l'ensemble des projecteurs sur W comme l'ensemble des $p \in \mathrm{Hom}(V, W)$ tels que $p_{|W} = \mathrm{id}_W$. Partons d'un tel projecteur p et notons $p' = Mp$ le moyennisé. D'après 2.4.1, c'est un G-morphisme $V \to W$. De plus comme g, g^{-1} stabilisent W, on peut écrire :

$$p'_{|W} = \frac{1}{|G|}\sum_{g\in G} g_{|W} p_{|W} g^{-1}_{|W} = \frac{1}{|G|}\sum_{g\in G} g_{|W} g^{-1}_{|W} = \mathrm{id}_W\,.$$

Ainsi p' est un projecteur sur W, et $W' = \ker(p')$ est un supplémentaire stable de W. □

3.1.2 Remarque. La preuve ci-dessus est concise (en particulier elle évite le recours aux éléments de V) car elle utilise les propriétés du moyenniseur, établies auparavant. Cependant, comme bien souvent au premier contact, le formalisme peut avoir tendance à masquer ce qu'il se passe concrètement. Il est donc intéressant de donner une rédaction plus directe. Voyons comment procède [Ser98], § 1.3, th. 1, et observons comment le moyenniseur, qui n'est pas nommé, est présent en filigrane. On part d'un projecteur $p : V \to V$ sur W. Définissons une nouvelle application linéaire par :

$$p' = \frac{1}{|G|}\sum_{g\in G} gpg^{-1}.$$

Cette application vérifie les propriétés suivantes :

(i) $p'(V) \subset W$, à cause du fait que W est G-stable,

(ii) $p'_{|W} = \mathrm{id}_W$ car si $x \in W$ on a $p(g^{-1}x) = g^{-1}x$, donc

$$p'(x) = \frac{1}{|G|}\sum_{g\in G} g(p(g^{-1}x)) = \frac{1}{|G|}\sum_{g\in G} g(g^{-1}x) = x.$$

(iii) p' est un G-morphisme, car en faisant le changement d'indices $k = hg$ on a :

$$hph^{-1} = \frac{1}{|G|}\sum_{g\in G} hgpg^{-1}h^{-1} = \frac{1}{|G|}\sum_{k\in G} kpk^{-1} = p.$$

Ainsi p' est un projecteur sur W et un G-morphisme, donc son noyau $W' = \ker(p')$ est un supplémentaire G-stable de W.

3.1.3 Exercice. On peut utiliser une description alternative des supplémentaires d'un sous-espace $W \subset V$ pour donner une deuxième preuve de 3.1.1. On note $\pi : V \to V/W$ le morphisme de quotient. On rappelle qu'une *section* de π est une application linéaire $s : V/W \to V$ telle que $\pi \circ s = \mathrm{id}_{V/W}$.

(1) Montrez que pour tout supplémentaire W' de W, la restriction $\pi_{|W'} : W' \to V/W$ est un isomorphisme puis que $s_{W'} : V/W \simeq W' \hookrightarrow V$ est une section de π. Montrez que les applications $W \mapsto s_{W'}$ et $s \mapsto \mathrm{im}(s)$ sont des bijections réciproques entre l'ensemble des supplémentaires de W dans V et le sous-ensemble de $\mathrm{Hom}(V/W, V)$ composé des sections de π.

(2) Soit V une représentation de G et $W \subset V$ une sous-représentation. On considère l'ensemble $\mathrm{Hom}(V/W, V)$ comme une représentation de G. Montrez que $M = \frac{1}{|G|} \sum g$ stabilise le sous-ensemble des sections de π. Déduisez-en une nouvelle preuve de 3.1.1.

3.1.4 Exercice. Lorsque $K = \mathbb{C}$, on peut donner une troisième preuve de 3.1.1. On munit V d'un produit scalaire hermitien $(-,-)$. On définit une nouvelle forme sesquilinéaire en posant

$$(x, y)' = \frac{1}{|G|} \sum_{g \in G} (g^{-1}x, g^{-1}y).$$

(1) Montrez que c'est un produit scalaire hermitien sur V et qu'il est G-invariant, au sens où $(h^{-1}x, h^{-1}y)' = (x, y)'$ pour tous $x, y \in V$ et $h \in G$. (De la même manière que dans la définition 1.3.4(4), l'ensemble $\mathrm{Sesq}(V)$ des formes sesquilinéaires sur V est une représentation linéaire de G, et le produit scalaire $(-,-)'$ est le moyennisé de $(-,-)$.)

(2) Montrez que pour toute sous-représentation $W \subset V$, le sous-espace W' orthogonal de W pour $(-,-)'$ est un supplémentaire stable.

3.1.5 Remarque. L'élément $M \in K[G]$ s'incarne comme un opérateur dans toutes les représentations linéaires. Nous avons vu qu'il a la propriété remarquable de stabiliser certaines parties naturelles qui *ne* sont pourtant *pas* des sous-espaces vectoriels :

- l'ensemble des projecteurs sur une sous-représentation $W \subset V$, qui est un sous-espace affine de $\mathrm{Hom}(V, W)$ (3.1.1-3.1.2),
- l'ensemble des sections du quotient $V \to V/W$ par une sous-représentation, qui est un sous-espace affine de $\mathrm{Hom}(V/W, V)$ (3.1.3) ;
- l'ensemble des produits scalaires hermitiens sur V, qui est un sous-ensemble de l'espace des formes sesquilinéaires, et un espace homogène sous $\mathrm{GL}(V)$ (3.1.4).

3.2 Représentations irréductibles et théorème de Maschke

3.2.1 Définition. Une représentation V d'un groupe G est dite *irréductible* ou *simple* si elle est non nulle et si ses seules sous-représentations sont 0 et V. Une représentation est dite *semi-simple* si elle est somme directe de sous-représentations simples.

3.2.2 Remarques. (1) Toute représentation de dimension 1 est irréductible.

(2) Pour une représentation de dimension $n > 1$, la condition d'irréductibilité est très forte. Elle implique par exemple les faits suivants :

- pour tout sous-espace $W \neq 0$, on a $\sum_{g \in G} g(W) = V$. En effet, l'espace $\sum_{g \in G} g(W)$ est une sous-représentation non nulle de V.
- pour tout sous-espace $W \neq V$, on a $\cap_{g \in G} g(W) = 0$. En effet, l'espace $\cap_{g \in G} g(W)$ est une sous-représentation stricte de V.

Il n'est donc pas tellement étonnant qu'on ait un résultat aussi contraignant que le lemme de Schur que nous verrons en 4.2.1.

(3) Bien sûr, il y a une analogie avec le concept de simplicité pour les groupes : on cherche à décomposer les représentations en morceaux plus petits. Par ailleurs, il y a un lien direct avec le concept d'endomorphisme semi-simple d'un espace vectoriel : il est équivalent de dire que $u \in \mathrm{End}(V)$ est semi-simple au sens habituel, ou que V est semi-simple comme représentation de l'algèbre $\mathbb{C}[u]$ des polynômes en u, ou encore, que V est semi-simple comme représentation du groupe (infini) $G = \mathbb{C}[u] \cap \mathrm{GL}(V)$.

3.2.3 Théorème. *Toute représentation de dimension finie est semi-simple.*

Démonstration : Soit $V = V_1 \oplus \cdots \oplus V_s$, avec $s \leqslant \dim(V)$, une décomposition maximale (i.e. s maximal) en somme directe de sous-représentations non nulles. Par le théorème 3.1.1, s'il existe un indice i et une sous-représentation non triviale $0 \subsetneq W_i \subsetneq V_i$, celle-ci possède un supplémentaire stable W_i'. On a alors $V_i = W_i \oplus W_i'$ en contradiction avec la maximalité de s. □

Cette décomposition n'est pas unique : par exemple si V est triviale, une décomposition en sous-représentations n'est rien d'autre qu'une décomposition en somme directe de droites et il y a une infinité de façons de faire cela. Mais on verra (théorème 5.1.1) que le nombre des sous-représentations parmi $V_1, \ldots, V_s$ qui sont isomorphes à une représentation irréductible donnée est, lui, unique.

3.2.4 Exercice. Soit K un corps. On note $\rho : \mathbb{Z} \to \mathrm{GL}_2(K)$ l'application définie par $\rho(n) = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$.

(1) Pour $K = \mathbb{C}$, montrez que ρ définit une représentation non semi-simple du groupe $G = \mathbb{Z}$ (donc le théorème est en défaut dans le cas d'un groupe infini).

(2) Pour $K = \mathbb{F}_p$, montrez que ρ induit une représentation non semi-simple du groupe $G = \mathbb{Z}/p\mathbb{Z}$ (donc le théorème est en défaut dans le cas d'un groupe fini d'ordre divisible par $\mathrm{car}(K)$).

4 Caractères

On suppose dans toute la suite du texte que $K = \mathbb{C}$ et que les représentations considérées sont de dimension finie.

4.1 Propriétés élémentaires

4.1.1 Définition. Le *caractère* d'une représentation $\rho : G \to \mathrm{GL}(V)$ est la fonction $\chi_\rho : G \to \mathbb{C}$ définie par $\chi_\rho(g) = \mathrm{tr}(\rho(g))$. On dit qu'un caractère est *irréductible* si la représentation V l'est.

On note parfois χ_V au lieu de χ_ρ. Bien sûr, deux représentations isomorphes ont même caractère. L'intérêt principal des caractères vient du fait remarquable que la réciproque est vraie, comme nous le verrons (corollaire 5.1.3). Voyons maintenant quelques propriétés élémentaires des caractères.

4.1.2 Proposition. *Soit V une représentation linéaire de G et $\chi = \chi_V$. Alors :*

(1) $\chi(1) = \dim(V)$,

(2) $\chi(g^{-1}) = \overline{\chi(g)}$, *le complexe conjugué de* $\chi(g)$,

(3) $\chi(hgh^{-1}) = \chi(g)$.

Tout caractère χ est par définition un élément de $K[G]$. Le point (3) de cette proposition dit que χ est une fonction centrale, i.e. un élement du centre de $K[G]$.

Démonstration : Le point (1) vient de ce que $\chi(1) = \mathrm{tr}(\mathrm{id}_V) = \dim(V)$. Le point (2) vient du fait que si l'on note $d = |G|$, on a $(g_V)^d = \mathrm{id}$. Ainsi g_V est diagonalisable à valeurs propres λ_i racines d-ièmes de l'unité, de sorte que $\lambda_i^{-1} = \overline{\lambda}_i$. Alors $(g_V)^{-1}$ a pour valeurs propres les $\overline{\lambda}_i$, donc

$$\chi(g^{-1}) = \mathrm{tr}((g_V)^{-1}) = \sum \overline{\lambda}_i = \overline{\mathrm{tr}(g_V)} = \overline{\chi(g)}.$$

Enfin (3) est une propriété élémentaire de la trace. □

4.1.3 Exemple. Le caractère d'une représentation triviale $V = V^{\mathrm{triv}}$ est donné par $\chi(g) = \mathrm{tr}(\mathrm{id}_V) = \dim(V)$. Regardons l'exemple de la représentation W de dimension 2 de $\mathfrak{S}_3$ donnée dans 1.3.2, par permutation des coordonnées dans l'hyperplan $x + y + z = 0$ dans K^3. Par la propriété (3) de la proposition ci-dessus, le caractère est invariant sur les classes de conjugaison, donc il suffit de donner ses valeurs sur des représentants de ces classes. Comme dans tout groupe symétrique, les classes de conjugaison sont classifiées par le type de la décomposition en cycles à support disjoint (i.e. la collection des longueurs des cycles). Dans $\mathfrak{S}_3$ on a trois classes de conjugaison, avec pour représentants $a = 1$, $b = (1, 2)$, $c = (1, 2, 3)$. Choisissons la base formée des vecteurs $u_1 = e_1 - e_3$ et $u_2 = e_2 - e_3$ pour notre représentation. L'endomorphisme b_W échange u_1 et u_2 donc sa matrice est $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ qui est de trace nulle. Par ailleurs $c_W(u_1) = u_2 - u_1$ et $c_W(u_2) = -u_1$ donc c_W a pour matrice $\left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ de trace -1. Le caractère χ de W est donc déterminé par $\chi(a) = 2$, $\chi(b) = 0$ et $\chi(c) = -1$.

4.1.4 Proposition. *Soient V_1, V_2 deux représentations de G de caractères χ_1, χ_2.*

(1) *Le caractère de la représentation somme directe $V = V_1 \oplus V_2$ est $\chi = \chi_1 + \chi_2$.*

(2) *Le caractère de la représentation $V = \mathrm{Hom}(V_1, V_2)$ est $\chi = \overline{\chi}_1 \cdot \chi_2$.*

(3) *Le caractère de la représentation duale V^* est $\chi_{V^*} = \overline{\chi}_V$.*

Soulignons le fait que dans (2), il s'agit bien du produit de $\overline{\chi}_1$ et χ_2 sur les valeurs (comme discuté dans 2.6) et non du produit de convolution.

Démonstration : (1) Pour tout $g \in G$ on a $g_V = g_{V_1} \oplus g_{V_2}$. Matriciellement, après choix d'une base adaptée à la décomposition $V_1 \oplus V_2$, cet endomorphisme se représente par une matrice diagonale par blocs. On trouve alors $\chi(g) = \mathrm{tr}(g_V) = \mathrm{tr}(g_{V_1}) + \mathrm{tr}(g_{V_2}) = \chi_1(g) + \chi_2(g)$.

(2) Soit $g \in G$. Soit $\{e_i\}$ une base de V_1 composée de vecteurs propres pour g_{V_1} et λ_i les valeurs propres correspondantes. Soit $\{f_j\}$ une base de V_2 composée de vecteurs propres pour g_{V_2} et μ_j les valeurs propres correspondantes. Notons $\{e_i^*\}$ la base duale de $\{e_i\}$ et $u_{i,j} = e_i^* \otimes f_j \in \mathrm{Hom}(V_1, V_2)$ l'application linéaire définie par $u_{i,j}(x) = e_i^*(x) f_j$. Vérifions que la famille $\{u_{i,j}\}$ est une base de $V = \mathrm{Hom}(V_1, V_2)$. Comme son cardinal est égal à $\dim(V_1)\dim(V_2) = \dim(V)$, il suffit de montrer qu'elle est libre. Or si $\sum_{i,j} a_{i,j} u_{i,j} = 0$, en évaluant sur e_k on trouve $\sum_j a_{k,j} f_j = 0$ donc $a_{k,j} = 0$ pour tous k, j puisque $\{f_j\}$ est une base. Montrons que $u_{i,j}$ est vecteur propre pour g_V de valeur propre $\overline{\lambda}_i \mu_j$. On rappelle que les valeurs propres de $g_{V_1}^{-1}$ sont les $\lambda_k^{-1} = \overline{\lambda}_k$. On calcule :

$$\big[g_V u_{i,j}\big](e_k) = \big[g_{V_2}(u_{i,j}) g_{V_1}^{-1}\big](e_k) = \big[g_{V_2}(u_{i,j})\big](\overline{\lambda}_k e_k) = g_{V_2}(\overline{\lambda}_k \delta_{i,k} f_j) = \delta_{i,k} \overline{\lambda}_k \mu_j f_j = \delta_{i,k} \overline{\lambda}_i \mu_j f_j.$$

Ceci est $[\overline{\lambda}_i \mu_j u_{i,j}](e_k)$, donc $g_V u_{i,j} = \overline{\lambda}_i \mu_j u_{i,j}$. On peut maintenant calculer :

$$\chi_V(g) = \mathrm{tr}(g_V) = \sum_{i,j} \overline{\lambda}_i \mu_j = \sum_i \overline{\lambda}_i \cdot \sum_j \mu_j = \overline{\chi_1(g)} \chi_2(g).$$

(3) C'est le cas particulier de (2) où $V_2 = \mathbb{C}$ est la représentation triviale. □

4.1.5 Exercice. Soit V une représentation de G et χ son caractère. Soit $B = \mathrm{Bilin}(V)$ la représentation des formes bilinéaires sur V, et BS la sous-représentation des formes bilinéaires symétriques. Montrez que $\chi_B(g) = \overline{\chi(g)^2}$ et $\chi_{BS}(g) = \frac{1}{2}(\overline{\chi(g)^2} + \overline{\chi(g^2)})$.

On voit que l'ensemble des caractères est un sous-ensemble de l'espace vectoriel de fonctions $\mathcal{F}(G, \mathbb{C})$ qui est stable par somme, par produit et par passage au conjugué, mais n'est stable ni par passage à l'opposé, ni par multiplication par un scalaire $\lambda \in \mathbb{C}$ (à cause de la propriété $\chi(1) = \dim(V)$ de 4.1.2). Ceci étant dit, la propriété 4.1.2(3) montre que le sous-espace vectoriel engendré par les caractères est inclus dans le sous-espace des fonctions centrales. Nous verrons bientôt qu'il lui est égal et que les caractères irréductibles en forment une base.

4.2 Lemme de Schur

4.2.1 Lemme de Schur. Soient V_1, V_2 deux représentations irréductibles de G. Alors :

$$\mathrm{Hom}_G(V_1, V_2) \simeq \begin{cases} 0 & \text{si } V_1 \not\simeq V_2, \\ \mathbb{C} & \text{si } V_1 \simeq V_2. \end{cases}$$

Démonstration : Soit $f : V_1 \to V_2$ un morphisme de G-représentations. Si $f \neq 0$, alors $\ker(f) \neq V_1$ donc $\ker(f) = 0$ par irréductibilité de V_1. De plus $\mathrm{im}(f) \neq 0$ donc $\mathrm{im}(f) = V_2$ par irréductibilité de V_2. Alors f est un isomorphisme. Par contraposée, ceci donne $\mathrm{Hom}_G(V_1, V_2) = 0$ si $V_1 \not\simeq V_2$.

Si $V_1 \simeq V_2 \simeq V$, alors $f : V \to V$ possède au moins une valeur propre λ. Le morphisme $f - \lambda\,\mathrm{id} : V \to V$ est encore un G-morphisme ; son noyau est non nul par choix de λ, donc égal à V par irréductibilité. Ainsi $f = \lambda\,\mathrm{id}$. □

4.2.2 Corollaire (action de M sur $\mathrm{Hom}(V_1, V_2)$).
(1) Soient V_1, V_2 des représentations irréductibles de G. Pour toute application linéaire $u : V_1 \to V_2$, on pose $Mu = \frac{1}{|G|} \sum_{g \in G} gug^{-1}$. Alors,

$$Mu = \begin{cases} \text{l'application nulle si } V_1 \not\simeq V_2, \\ \text{l'homothétie de rapport } \frac{1}{\dim(V_1)} \mathrm{tr}(u) \text{ si } V_1 = V_2. \end{cases}$$

(2) Soit V une représentation irréductible de G, de caractère χ. Soit $\varphi \in \mathbb{C}[G]$ une fonction centrale sur G. Alors l'endomorphisme $\varphi_V = \sum_g \varphi(g)\, g_V : V \to V$ est l'homothétie de rapport $\frac{|G|}{\dim(V)}(\varphi, \overline{\chi})$.

Démonstration : (1) L'application Mu est un G-morphisme et on peut appliquer le lemme de Schur. Lorsque $V_1 \not\simeq V_2$ on a $Mu = 0$, et lorsque $V_1 = V_2$ il existe $\lambda \in \mathbb{C}$ tel que $Mu = \lambda\,\mathrm{id}$. En prenant la trace, on trouve $\dim(V)\lambda = \mathrm{tr}(Mu) = \mathrm{tr}(\frac{1}{|G|} \sum_{g \in G} gug^{-1}) = \mathrm{tr}(u)$ d'où on déduit la valeur de λ.

(2) Comme φ est dans le centre de $K[G]$, on a $\varphi_V g_V = g_V \varphi_V$ dans $\mathrm{End}(V)$ i.e. φ_V est un G-morphisme. Par le lemme de Schur, c'est une homothétie dont on calcule le rapport λ en prenant la trace :

$$\dim(V)\lambda = \mathrm{tr}(\varphi_V) = \mathrm{tr}(\sum_{g\in G} \varphi(g) g_V) = \sum_{g\in G} \varphi(g)\chi(g) = |G|(\varphi, \overline{\chi}).$$

On en déduit le résultat annoncé. □

4.3 Orthogonalité

On rappelle (*cf* 4.1.1) qu'un caractère irréductible est le caractère d'une représentation irréductible.

4.3.1 Théorème. *Les caractères irréductibles de G forment une base orthonormale de l'espace des fonctions centrales sur G.*

Démonstration : Montrons que la famille des caractères irréductibles est orthonormale. Soient χ_1, χ_2 deux caractères et choisissons deux représentations V_1, V_2 qui leur donnent naissance. Notons χ_V le caractère de $V = \mathrm{Hom}(V_2, V_1)$. On a :

$$(\chi_1, \chi_2) \overset{\text{déf de } (-,-)}{=\!=\!\downarrow} \frac{1}{|G|}\sum_{g\in G} \chi_1(g)\overline{\chi_2(g)} \overset{4.1.4(2)}{=\!=\!\downarrow} \frac{1}{|G|}\sum_{g\in G} \chi_V(g) \overset{\text{déf de } \chi_V}{=\!=\!\downarrow} \frac{1}{|G|}\sum_{g\in G} \mathrm{tr}(g_V) = \mathrm{tr}\left(\frac{1}{|G|}\sum_{g\in G} g_V\right) \overset{\text{déf de } M}{=\!=\!\downarrow} \mathrm{tr}(M_V).$$

Supposons V_1, V_2 irréductibles ; alors l'endomorphisme M_V est décrit par le corollaire 4.2.2. Si $\chi_1 \neq \chi_2$ on a $V_1 \not\simeq V_2$ donc $M_V = 0$ qui est de trace nulle. Si $\chi_1 = \chi_2$ on peut choisir $V_1 = V_2$, et alors M_V est le projecteur sur la droite des homothéties. Il est diagonalisable avec pour valeurs propres $(1, 0, 0, \dots)$, donc sa trace est 1. On a montré que $(\chi_1, \chi_2) = 1$ lorsque $\chi_1 = \chi_2$ et 0 sinon, d'où l'orthonormalité.

Montrons maintenant que la famille est une base. Comme elle est orthogonale, elle est libre. Il suffit donc de montrer que le sous-espace qu'elle engendre a un orthogonal réduit à 0. Soit φ une fonction centrale orthogonale à tout caractère irréductible. On note que $\chi \mapsto \overline{\chi}$ est une involution de l'ensemble des caractères irréductibles, puisque si $\chi = \chi_V$ alors $\overline{\chi} = \chi_{V^*}$, et V^* est irréductible si et seulement si V l'est. D'après 4.2.2(2), on voit alors que l'endomorphisme φ_V est nul pour toute représentation irréductible V. Comme toute représentation est somme directe d'irréductibles, on déduit que φ_V pour toute représentation de dimension finie. En particulier, en regardant la représentation régulière qui est fidèle, on trouve $\varphi = 0$. □

Un point important de la démonstration vaut la peine d'être reformulé : *le produit scalaire (χ_1, χ_2) de deux caractères est égal à la trace de l'opérateur de moyenne sur* $\mathrm{Hom}(V_2, V_1)$.

4.3.2 Corollaire. *Deux représentations irréductibles non isomorphes ont des caractères distincts. L'ensemble* $\mathrm{Irr}(G)$ *des caractères irréductibles est fini, de cardinal égal au nombre de classes de conjugaison de G.*

Démonstration : Soient V_1, V_2 deux représentations irréductibles telles que $\chi_1 = \chi_2$. Posons $V := \mathrm{Hom}(V_2, V_1)$. Compte tenu du commentaire fait juste avant l'énoncé du corollaire, nous avons $\mathrm{tr}(M_V) = (\chi_1, \chi_2) = \|\chi_1\|^2 = 1$. En particulier $M_V \neq 0$ donc son image, qui d'après le lemme 2.4.1

est l'espace des morphismes G-équivariants $\mathrm{Hom}_G(V_1, V_2)$, est non nulle. D'après le lemme de Schur, ceci implique $V_1 \simeq V_2$. Par contraposée, ceci démontre le premier point. Le second découle du fait que la dimension de l'espace des fonctions centrales est égale au nombre de classes de conjugaison de G. □

On notera qu'en dépit de ce résultat, il n'existe en général pas de bijection naturelle entre $\mathrm{Irr}(G)$ et $\mathrm{Conj}(G)$ (voir [Col12], I.2.17).

5 Décomposition des représentations

Dorénavant, pour chaque caractère irréductible $\chi \in \mathrm{Irr}(G)$, on supposera choisie une représentation irréductible notée V_χ de caractère χ. Si V est une représentation, on note $nV = V^{\oplus n} = V \oplus \cdots \oplus V$ la somme directe de n copies de V.

5.1 Décomposition canonique d'une représentation

5.1.1 Théorème. *Soit V une représentation de G, de caractère φ. Soit $V = W_1 \oplus \cdots \oplus W_s$ une décomposition en somme directe de sous-représentations irréductibles, et soit $\chi \in \mathrm{Irr}(G)$.*

(1) *Le nombre des W_i isomorphes à V_χ est égal au produit scalaire (φ, χ). En particulier, il ne dépend pas de la décomposition choisie. Il est appelé* multiplicité *de V_χ (ou de χ) dans V.*

(2) *Soit $W_\chi \subset V$ le sous-espace somme des W_i isomorphes à V_χ.*

(i) *On a une décomposition $V = \oplus_{\chi \in \mathrm{Irr}(G)} W_\chi$ et le projecteur sur W_χ associé à cette décomposition est l'endomorphisme $p_\chi = \frac{\dim(V_\chi)}{|G|} \sum_{g \in G} \overline{\chi}(g)\, g_V$.*

(ii) *Le sous-espace W_χ est isomorphe comme G-représentation à $(\varphi, \chi)V_\chi$ et il ne dépend pas de la décomposition $V = W_1 \oplus \cdots \oplus W_s$ choisie.*

L'espace W_χ est appelé composante isotypique de caractère χ *et la décomposition $V = \oplus W_\chi$ est appelée* décomposition canonique *de V.*

5.1.2 Remarques. (1) Il est remarquable que le projecteur sur W_χ soit l'image par $\widetilde{\rho} : \mathbb{C}[G] \to \mathrm{End}(V)$ d'un élément de $\mathbb{C}[G]$ qui ne dépend pas de V, à savoir $\widetilde{p}_\chi = \frac{\dim(V_\chi)}{|G|}\, \overline{\chi} = \frac{\dim(V_\chi)}{|G|} \sum_{g \in G} \overline{\chi}(g)\, g$.
(2) Une des conséquences de la canonicité est que la décomposition du théorème est préservée par les morphismes de représentations : tout morphisme $f : V \to V'$ de représentations de G envoie la composante isotypique $W_\chi \subset V$ dans la composante isotypique $W'_\chi \subset V'$. En particulier, la décomposition $V = \oplus W_\chi$ est préservée par les endomorphismes linéaires de V qui commutent à l'action de G.

Démonstration : (1) Notons χ_i le caractère de W_i. D'après la proposition 4.1.4, on a $\varphi = \chi_1 + \cdots + \chi_s$ donc $(\varphi, \chi) = (\chi_1, \chi) + \cdots + (\chi_k, \chi)$. D'après le théorème d'orthogonalité, le i-ième terme de cette somme vaut 0 si $W_i \not\simeq V_\chi$ et 1 si $W_i \simeq V_\chi$. Donc le nombre des W_i isomorphes à V_χ est égal à (φ, χ).
(2)(i) La décomposition $V = \oplus_{\chi \in \mathrm{Irr}(G)} W_\chi$ provient de la décomposition $V = W_1 \oplus \cdots \oplus W_s$ en réunissant les W_i isomorphes à une même représentation irréductible V_χ. Maintenant soit ψ un caractère irréductible. Le point (2) du corollaire 4.2.2 montre que la restriction de $\overline{\chi}_V$ à toute sous-représentation irréductible $W \subset V$ isomorphe à V_ψ est l'homothétie de rapport $\frac{|G|}{\dim(V_\psi)}(\overline{\chi}, \overline{\psi})$. Il en

découle que la restriction de $q_\chi := \frac{\dim(V_\chi)}{|G|}\,\overline{\chi}$ à W_ψ est l'identité si $\psi = \chi$ et nulle si $\psi \neq \chi$. Donc q_χ est bien le projecteur sur W_χ associé à la décomposition canonique.

(2)(ii) Le fait que W_χ soit isomorphe à $(\varphi, \chi)\, V_\chi$ est conséquence de (1). Le fait qu'il ne dépende pas de la décomposition choisie découle de (i). □

5.1.3 Corollaire. *Deux représentations de même caractère sont isomorphes.*

Démonstration : En effet, d'après le résultat précédent, elles contiennent le même nombre de fois toute représentation irréductible V_χ donnée. □

On termine par un critère pratique d'irréductibilité.

5.1.4 Théorème. *Si φ est le caractère d'une représentation, alors (φ, φ) est un entier positif, et $(\varphi, \varphi) = 1$ si et seulement si ce caractère est irréductible.*

Démonstration : Soit V une représentation de caractère φ. D'après le théorème 5.1.1, on a $V \simeq \oplus(\varphi, \chi)V_\chi$ où $m_\chi := (\varphi, \chi)$, multiplicité de V_χ, est un entier naturel. On en déduit que $\varphi = \sum m_\chi \chi$ puis, par orthogonalité des caractères :

$$(\varphi, \varphi) = \left(\sum_\chi m_\chi \chi, \sum_{\chi'} m_{\chi'} \chi' \right) = \sum_\chi (m_\chi)^2.$$

C'est un entier positif, qui vaut 1 si et seulement si l'un des m_χ est égal à 1 et les autres sont nuls, si et seulement si V est isomorphe à l'une des V_χ. □

5.2 Décomposition de la représentation régulière

5.2.1 Proposition. *Le caractère r de la représentation régulière de G est donné par $r(1) = |G|$, et $r(g) = 0$ si $g \neq 1$. En d'autres termes, en tant qu'élément de $\mathbb{C}[G]$ on a $r = |G|.1$.*

Démonstration : Notons $V = \mathbb{C}[G]$ l'espace de la représentation régulière. On a $r(1) = \dim(V) = |G|$ d'après 4.1.2. Si $g \neq 1$, l'endomorphisme g_V agit par $g_V(h) = gh$ qui est différent de h, pour tout h. Dans la base de V composée par les éléments de G, la matrice de g_V a donc tous ses termes diagonaux nuls de sorte que $r(g) = \mathrm{tr}(g_V) = 0$. □

5.2.2 Corollaire. *Pour $\chi \in \mathrm{Irr}(G)$, notons d_χ la dimension de la représentation irréductible V_χ.*

(1) *La multiplicité de V_χ dans la représentation régulière est égale à d_χ.*

(2) $\sum_{\chi \in \mathrm{Irr}(G)} (d_\chi)^2 = |G|$.

(3) *Pour tout $g \neq 1$, on a $\sum_{\chi \in \mathrm{Irr}(G)} d_\chi \chi(g) = 0$.*

Ces formules sont très utiles en pratique pour déterminer les tables de caractères de groupes explicites, comme nous le verrons. La formule (2), qui dit en mots que la somme des carrés des dimensions des représentations irréductibles de G est égale à $|G|$, est dûe à Burnside.

Démonstration : D'après le théorème 5.1.1, la multiplicité de V_χ dans $\mathbb{C}[G]$ est égale à

$$(r,\chi) = \frac{1}{|G|}\sum_{g\in G} r(g)\overline{\chi(g)} = \overline{\chi(1)} = d_\chi.$$

On en déduit que $r = \sum_\chi d_\chi\chi$. Compte tenu de la proposition 5.2.1, en évaluant en $g = 1$, on trouve $|G| = \sum_{\chi\in\mathrm{Irr}(G)}(d_\chi)^2$. En évaluant en $g \neq 1$, on trouve $0 = \sum_{\chi\in\mathrm{Irr}(G)} d_\chi\chi(g)$. □

5.3 Transformation de Fourier

Le corollaire 5.2.2 nous donne une décomposition abstraite pour la représentation régulière :

$$\mathbb{C}[G] \simeq \bigoplus_{\chi\in\mathrm{Irr}(G)} d_\chi V_\chi.$$

Il s'agit d'un isomorphisme d'espaces vectoriels avec action de G. La transformation de Fourier permet de raffiner cette décomposition pour prendre également en compte la structure d'anneau de $\mathbb{C}[G]$.

5.3.1 Théorème. *Soient G un groupe fini. Pour chaque $\chi \in \mathrm{Irr}(G)$, on note V_χ une représentation irréductible de caractère χ et $d_\chi = \dim(V_\chi)$. Alors, l'application* transformée de Fourier *:*

$$\mathscr{F} : (\mathbb{C}[G],*) \longrightarrow \prod_{\chi\in\mathrm{Irr}(G)} \mathrm{End}(V_\chi)$$
$$\mathscr{F}(f) = (f_{V_\chi})_\chi \quad \textit{où} \quad f_{V_\chi} = \textstyle\sum_{g\in G} f(g)g_{V_\chi},$$

est un isomorphisme de $\mathbb{C}$-algèbres. Son inverse est la transformée de Fourier inverse *:*

$$\mathscr{F}^{-1} : \prod_{\chi\in\mathrm{Irr}(G)} \mathrm{End}(V_\chi) \longrightarrow (\mathbb{C}[G],*)$$
$$\mathscr{F}^{-1}((f_\chi)_\chi) = f \quad \textit{où} \quad f(g) = \tfrac{1}{|G|}\sum_\chi d_\chi \operatorname{tr}(g_{V_\chi}^{-1} f_\chi).$$

Le but $\prod \mathrm{End}(V_\chi)$ de la transformation de Fourier est muni de sa structure d'anneau produit naturelle (en tant qu'espace vectoriel, le produit est la même chose que la somme directe). La question de savoir si $\mathscr{F}$ est un isomorphisme de représentations est étudiée dans l'exercice 5.3.2.

Démonstration : L'application $\mathscr{F}$ est l'extension à l'algèbre de groupe (comme dans 2.2.3) de l'application $G \to \prod \mathrm{GL}(V_\chi) \subset \prod \mathrm{End}(V_\chi)$ induite par les morphismes $\rho_\chi : G \to \mathrm{GL}(V_\chi)$ qui définissent les structures de représentation. C'est donc un morphisme de $\mathbb{C}$-algèbres. Ce morphisme est injectif car si $f \in \mathbb{C}[G]$ a des incarnations f_{V_χ} nulles pour tout χ, alors l'endomorphisme défini par f est nul sur toutes les représentations irréductibles de G, donc nul sur toutes les représentations par semi-simplicité, donc en particulier nul sur la représentation régulière, donc nul car celle-ci est fidèle. Or d'après la formule de Burnside 5.2.2(2), la dimension de la source et la dimension du but sont égales, donc $\mathscr{F}$ est un isomorphisme. Enfin pour démontrer la formule d'inversion, il suffit de montrer que pour toute fonction $f \in \mathbb{C}[G]$ on a : $f(g) = \frac{1}{|G|}\sum_\chi d_\chi \operatorname{tr}(g_{V_\chi}^{-1} f_{V\chi})$. Cette expression est $\mathbb{C}$-linéaire en f, et il suffit donc de démontrer l'égalité pour les fonctions de base $f = h = \delta_h$, pour $h \in G$. Or d'une part $\delta_h(g) = \delta_{h,g}$ (le symbole de Kronecker), et d'autre part :

$$\frac{1}{|G|}\sum_\chi d_\chi \operatorname{tr}(g_{V_\chi}^{-1} h_{V_\chi}) = \frac{1}{|G|}\sum_\chi d_\chi\chi(g^{-1}h).$$

D'après les formules (2) et (3) de 5.2.2, ceci vaut 1 si $g = h$ et 0 sinon, comme souhaité. □

5.3.2 Exercice (transformation de Fourier et composantes isotypiques).
(1) On note $\mathrm{End}(V_\chi)^*$ l'espace vectoriel $\mathrm{End}(V_\chi)$ muni de la structure de représentation définie par $g.\varphi := g \circ \varphi$, pour $\varphi \in \mathrm{End}(V_\chi)$; c'est la représentation $\mathrm{Hom}(V_\chi^{\mathrm{triv}}, V_\chi)$ au sens de la définition 1.3.4. Démontrez que la composante isotypique de type χ de $\prod \mathrm{End}(V_\chi)^*$ est $\mathrm{End}(V_\chi)^*$ et que la transformation de Fourier induit un isomorphisme de représentations $\mathscr{F}_\chi : \mathbb{C}[G]_\chi \simeq \mathrm{End}(V_\chi)^*$.

(2) On note $\mathrm{End}(V_\chi)$ la représentation $\mathrm{Hom}(V_\chi, V_\chi)$ définie en 1.3.4. En regardant le cas du groupe $G = \mathbb{Z}/n\mathbb{Z}$, montrez que, en général :

(i) le facteur $\mathrm{End}(V_\chi)$ n'est pas la composante isotypique de type χ de $\prod \mathrm{End}(V_\chi)$,

(ii) $\mathscr{F}$ n'est pas un morphisme de représentations,

(iii) $\mathbb{C}[G]_\chi$ et $\mathrm{End}(V_\chi)$ ne sont pas isomorphes comme représentations abstraites.

6 Tables de caractères

6.1 Définition. Soit G un groupe fini et $h = |\mathrm{Conj}(G)|$ le nombre de ses classes de conjugaison. On appelle *table de caractères* de G le tableau carré T_G de format (h, h) tel que :

- les lignes sont indicées par les caractères irréductibles $\chi \in \mathrm{Irr}(G)$;
- les colonnes sont indicées par les classes de conjugaison $\overline{g} \in \mathrm{Conj}(G)$ d'éléments $g \in G$;
- dans la case de position $(\chi, \overline{g})$ figure l'élément $\chi(g)$.

On borde le tableau par une colonne gauche dans laquelle figurent les caractères irréductibles, et une ligne supérieure où figurent les classes de conjugaison. En pratique, on indique une classe de conjugaison C en notant simplement un élément $g \in C$, et on indique en indice le nombre d'éléments de C (nous verrons plus loin pourquoi c'est important).

6.2 Exemple : le groupe symétrique $G = \mathfrak{S}_3$. Il possède 3 classes de conjugaison : l'identité forme une classe, les transpositions $(1,2)$, $(1,3)$, $(2,3)$ forment une deuxième classe, et les 3-cycles $(1,2,3)$, $(1,3,2)$ forment la dernière classe. On sait donc qu'il y a 3 caractères irréductibles. Le caractère trivial noté 1 est le plus simple d'entre eux. Le morphisme signature $\epsilon : \mathfrak{S}_3 \to \{\pm 1\}$ est un autre caractère irréductible. À cause de la formule de Burnside $6 = 1 + 1 + d^2$, le dernier caractère irréductible correspond à une représentation de dimension $d = 2$. Il s'agit de la représentation de $\mathfrak{S}_3 \simeq \mathbb{D}_3$ dans $V = \mathbb{C}^2$ issue de l'action comme groupe d'isométries du triangle équilatéral (voir exercice 2.2.4). Si l'on choisit les générateurs $r = (1,2,3)$ et $s = (1,2)$ pour G, le morphisme $\rho : G \to \mathrm{GL}_2(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{C})$ envoie r sur la matrice de la rotation d'angle $2\pi/3$ et s sur la matrice de la réflexion par rapport à l'axe des abscisses. Le fait que cette représentation est irréductible résulte du fait qu'elle n'a pas de sous-représentation de dimension 1 : les droites propres pour s_V, c'est-à-dire l'axe des abscisses et celui des ordonnées, ne sont pas stables par r_V (prendre garde au fait que r_V n'a pas de valeur propre réelle, mais elle a des valeurs propres complexes et nous travaillons avec la représentation complexe). Notons χ le caractère correspondant ; on calcule donc $\chi(r) = \mathrm{tr}(r_V) = 2\cos(2\pi/3) = -1$ et $\chi(s) = \mathrm{tr}(s_V) = 0$. La table de caractères est donc la suivante.

$\mathfrak{S}_3$	1	$(1,2)_3$	$(1,2,3)_2$
1	1	1	1
ϵ	1	-1	1
χ	2	0	-1

6.3 Proposition (propriétés de la table de caractères T_G). *Soient G un groupe fini, h le nombre de ses classes de conjugaison, et T_G sa table de caractères.*

(1) *Les lignes de T_G sont orthonormées pour le produit scalaire hermitien $(-,-)$, à condition de compter chaque case un nombre de fois égal au cardinal de la classe de conjugaison correspondant à sa colonne.*

(2) *Les colonnes de T_G sont orthogonales deux à deux pour le produit hermitien standard sur $\mathbb{C}^h$ défini par $\langle x, y\rangle = \sum x_i\overline{y}_i$. La norme de la colonne indicée par la classe $C \in \mathrm{Conj}(G)$ est égale à $\frac{|G|}{|C|}$.*

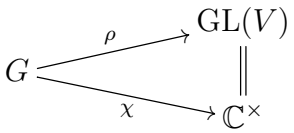
Démonstration : (1) Ce sont les relations d'orthogonalité des caractères. Chaque case d'indice $(\chi, \overline{g})$ doit être pondérée par le cardinal de la classe $\overline{g}$ car la somme qui définit le produit scalaire sur $\mathbb{C}[G]$ porte sur les éléments de G et non les classes de conjugaison.
(2) Ces relations font l'objet de l'exercice 8.5. □

7 Le cas abélien

Dans cette partie, le groupe fini G est abélien. Dans ce cas, pour toute représentation linéaire de dimension finie V de G, les endomorphismes g_V sont diagonalisables (car d'ordre fini donc annulés par un polynôme scindé sur $\mathbb{C}$ à racines distinctes) et donc codiagonalisables (puisqu'ils commutent deux à deux). Ceci démontre que V est somme directe de droites G-stables. En particulier, pour un groupe abélien toutes les représentations irréductibles sont de dimension 1. La réciproque est vraie comme nous le verrons tout de suite.

7.1 Caractères linéaires et groupe dual

La remarque précédente donne une importance particulière aux représentations de dimension 1. Pour une telle représentation V, l'application qui à une homothétie associe son rapport, qui n'est autre que l'application trace, définit un isomorphisme *canonique* $\mathrm{GL}(V) = \mathbb{C}^\times$. À cet isomorphisme près, le morphisme de représentation $\rho : G \to \mathrm{GL}(V)$ peut donc être identifié à son caractère :



Ceci explique la définition suivante.

7.1.1 Définition. Soit G un groupe (non nécessairement fini ni abélien pour cette définition). On appelle *caractère linéaire* de G un morphisme de groupes $\chi : G \to \mathbb{C}^\times$. On appelle *groupe dual* ou *groupe des caractères* l'ensemble $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^\times)$ des caractères linéaires, muni de la multiplication sur les valeurs i.e. $(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$.

Si V est un espace vectoriel de dimension 1, un morphisme $\chi : G \to \mathbb{C}^\times$ comme ci-dessus définit une représentation par la formule $g_V(x) = \chi(g)x$. L'usage du mot *caractère* est un abus dans ce contexte. Comme toute représentation de dimension 1 est irréductible, on a une inclusion $\widehat{G} \hookrightarrow \mathrm{Irr}(G)$. Retrouvons maintenant le fait énoncé en introduction, et surtout sa réciproque, comme un corollaire de la formule de Burnside.

7.1.2 Proposition. *Soit G un groupe fini. Alors G est abélien si et seulement si toutes ses représentations irréductibles sont de dimension 1, si et seulement si $\widehat{G} = \mathrm{Irr}(G)$.*

Démonstration : Le groupe G est abélien si et seulement s'il possède $|G|$ classes de conjugaison, donc aussi $|G|$ caractères irréductibles. Comme les représentations irréductibles sont de dimension $d_\chi \geqslant 1$, d'après la formule de Burnside 5.2.2(2) ceci équivaut à dire que $d_\chi = 1$ pour tout χ. □

La dénomination de groupe dual pour $\widehat{G}$ sous-entend qu'il existe un formalisme de dualité similaire à celui de la dualité des espaces vectoriels de dimension finie. Nous décrivons maintenant deux résultats qui en attestent. Nous noterons $\widehat{\widehat{G}}$ le bidual de G, i.e. le dual de $\widehat{G}$, et

$$\mathrm{ev} : G \to \widehat{\widehat{G}}$$

l'application de bidualité qui envoie g sur le morphisme d'évaluation $\mathrm{ev}_g : \widehat{G} \to \mathbb{C}^\times$, $\chi \mapsto \chi(g)$.

7.1.3 Proposition. *Tout groupe fini abélien est isomorphe à son dual, de manière non canonique.*

Démonstration : La preuve est en 3 étapes.

(1) On suppose d'abord que G est cyclique de cardinal n et on choisit un générateur γ. Dans ce cas un caractère $\chi : G \to \mathbb{C}^\times$ est déterminé par l'image de γ, qui est une racine n-ième de l'unité, et réciproquement tout choix de racine de l'unité $\omega \in \mu_n(\mathbb{C})$ détermine un caractère tel que $\chi(g) = \chi(\gamma^i) = \omega^i$, pour tout $g = \gamma^i \in G$. On a donc un isomorphisme $\widehat{G} = \mu_n(\mathbb{C})$. Or ce dernier groupe est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ par le choix d'une racine primitive n-ième de l'unité. On notera que ces constructions dépendent du choix de générateur g et du choix de racine primitive de l'unité.

(2) On démontre maintenant que si G, H des groupes finis abéliens, on a un isomorphisme $\widehat{G_1 \times G_2} \simeq \widehat{G}_1 \times \widehat{G}_2$. Ceci est à peu près clair : à tout caractère $\chi : G_1 \times G_2 \to \mathbb{C}^\times$ on associe la paire composée de $\chi_1 = \chi_{|G_1 \times \{1\}}$ et $\chi_2 = \chi_{|\{1\} \times G_2}$, et réciproquement à toute paire de caractères (χ_1, χ_2) on associe $\chi : G \to \mathbb{C}^\times$ défini par $\chi(g_1, g_2) = \chi_1(g_1)\chi_2(g_2)$.

(3) D'après le théorème de structure des groupes abéliens de type fini, on dispose d'un isomorphisme $G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ avec $n_1 | n_2 | \ldots | n_r$. Le résultat découle alors de (1) et (2). □

7.1.4 Remarque. Qu'entend-on exactement lorsqu'on dit qu'il n'y a pas d'isomorphisme canonique entre G et son dual ? Le mot canonique est sujet à des interprétations variables selons les mathématiciens, mais tous s'accordent sur le fait qu'un objet canonique ne doit pas dépendre de divers choix faits pour le construire. En algèbre linéaire, ceci se traduit souvent par l'indépendance par rapport aux changements de bases (qui sont des automorphismes particuliers du groupe général linéaire GL). Dans le cas présent, la lectrice pourra vérifier qu'il n'existe pas de choix d'isomorphismes $i_G : G \xrightarrow{\sim} \widehat{G}$ qui soient compatibles avec les morphismes de groupes $f : G \to H$. Si on concentre l'attention sur un groupe G, elle pourra vérifier qu'il n'existe pas d'isomorphisme $i_G : G \xrightarrow{\sim} \widehat{G}$ qui soit compatible avec tous les automorphismes de G... sauf lorsque $G \simeq \mathbb{Z}/2\mathbb{Z}$. En fait la plupart des commentaires de la note :

`https://perso.univ-rennes1.fr/matthieu.romagny/agreg/theme/que_veut_dire_etre_canonique.pdf`

peuvent être formulés à l'identique pour la dualité des groupes finis abéliens.

L'égalité de cardinaux $|G| = |\widehat{G}|$ peut aussi être obtenue à partir des résultats généraux :

$$\begin{array}{ccccc} & \overset{G \text{ abélien}}{\downarrow} & & \overset{4.3.2}{\downarrow} & & \overset{7.1.2}{\downarrow} & \\ |G| & = & |\operatorname{Conj}(G)| & = & |\operatorname{Irr}(G)| & = & |\widehat{G}|. \end{array}$$

7.1.5 Théorème. *L'application de bidualité* $\mathrm{ev} : G \to \widehat{\widehat{G}}$ *est un isomorphisme de groupes.*

Démonstration : Pour montrer que ev est un morphisme de groupes, soient g, h dans G. Soit $\chi \in \widehat{G}$. On a alors $\mathrm{ev}_{gh}(\chi) = \chi(gh) = \chi(g)\chi(h) = \mathrm{ev}_g(\chi)\,\mathrm{ev}_h(\chi) = (\mathrm{ev}_g\,\mathrm{ev}_h)(\chi)$ à cause de la définition de ev, du fait que χ est un morphisme, et de la définition du produit dans $\widehat{G}$. Comme ceci est vrai pour tout χ on voit que $\mathrm{ev}_{gh} = \mathrm{ev}_g\,\mathrm{ev}_h$ comme souhaité. Par ailleurs, on a montré l'égalité des cardinaux de G, son dual, et donc aussi son bidual. Il suffit donc de montrer que ev est injectif. Ceci découlera essentiellement des arguments donnés dans la démonstration de 7.1.3, que nous reprendrons. Soit $g \in G$ avec $g \neq 0$. Si l'on choisit un isomorphisme $G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$, alors g est non nul dans l'un des facteurs $\mathbb{Z}/n_i\mathbb{Z}$. Comme le dual du produit est le produit des duaux, on se ramène à considérer le cas où G est cyclique de cardinal n. Choisissons un générateur γ pour G, une racine *primitive* n-ème de l'unité ω, et notons χ le caractère tel que $\chi(\gamma) = \omega$, comme dans l'étape 1 de la preuve de 7.1.3. Comme $g \neq 0$, on a $g = \gamma^i$ avec i non nul modulo n. On en déduit que $\chi(g) = \chi(\gamma^i) = \omega^i \neq 1$. Ceci montre que $\mathrm{ev}_g(\chi) \neq 0$, donc $\mathrm{ev}_g \neq 0$. □

7.1.6 Remarque. Certains des résultats généraux sur les représentations et les caractères peuvent être obtenus de manière plus simple et directe dans le cas des groupes abéliens. C'est le cas pour les relations d'orthogonalité des caractères. De même, on peut obtenir les résultats ci-dessus concernant le dual $\widehat{G}$ par une approche directe utilisant un lemme de prolongement de caractères. Cette approche est pertinente en particulier dans le cadre de la leçon 110 intitulée *Caractères d'un groupe abélien fini et transformée de Fourier discrète*. Elle est détaillée dans le chapitre 1 du livre [Pey04].

7.2 Transformation de Fourier

Dans le cas abélien, la transformation de Fourier prend une forme particulière qu'il est utile de mettre en évidence. On a $\operatorname{Irr}(G) = \widehat{G}$ et pour tout caractère irréductible χ, on a un choix canonique de représentation associée : on prend $V_\chi = \mathbb{C}$ munie de l'action $g(x) = \chi(g)x$. L'algèbre $\prod \operatorname{End}(V_\chi)$ est simplement l'algèbre $\mathbb{C}[\widehat{G}]$ munie de son produit ponctuel, i.e. $(\mathbb{C}[\widehat{G}], \cdot)$. Nous allons spécialiser dans ce contexte les expressions des transformées de Fourier.

7.2.1 Scholie. *Dans le cas d'un groupe fini abélien G, les notations générales de 5.3 se spécialisent pour donner la forme suivante aux transformées de Fourier :*

$$(\mathbb{C}[G], *) \underset{\mathscr{F}^{-1}}{\overset{\mathscr{F}}{\rightleftarrows}} (\mathbb{C}[\widehat{G}], \cdot)$$

$$\mathscr{F}(f) = \widehat{f} \quad \textit{avec} \quad \widehat{f}(\chi) = \textstyle\sum_{g\in G} f(g)\chi(g) = |G|(f, \overline{\chi})$$

$$\mathscr{F}^{-1}(\widehat{f}) = f \quad \textit{avec} \quad f(g) = \tfrac{1}{|G|} \textstyle\sum_{\chi\in\widehat{G}} \widehat{f}(\chi)\overline{g(\chi)} = (\widehat{f}, g)_{\widehat{G}}$$

où $(-,-)_{\widehat{G}}$ est le produit scalaire canonique de $\mathbb{C}[\widehat{G}]$.

7.2.2 Remarque. Dans un texte mathématique, une scholie est une remarque qui suit un théorème démontré ou un problème résolu, et dont le contenu se situe en marge de la démarche démonstrative. C'est un énoncé qui a valeur de commentaire ou de reformulation.

Précisons comment on passe des notations de 5.3.1 à celles de 7.2.1. Comme les représentations sont ici des caractères linéaires, on note $\chi(g)$ plutôt que g_{V_χ}. L'expression pour la transformée de Fourier devient $\mathscr{F}(f) = \widehat{f}$ avec :

$$\widehat{f}(\chi) = \sum_{g \in G} f(g)\chi(g) = |G|(f, \overline{\chi}).$$

Par ailleurs, dans les notations de 5.3.1 on a $d_\chi = 1$ pour tout χ, et f_χ est remplacé par $\widehat{f}(\chi)$ pour un élément $\widehat{f} \in \mathbb{C}[\widehat{G}]$. On obtient $\mathscr{F}^{-1}(\widehat{f}) = f$ avec :

$$f(g) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(g^{-1})\widehat{f}(\chi).$$

Les expressions pour $\widehat{f}(\chi)$ et $f(g)$ ne montrent leur belle symétrie que lorsqu'on utilise la bidualité. En effet, celle-ci permet d'identifier G au groupe de caractères de $\widehat{G}$ et g au caractère $\mathrm{ev}_g : \widehat{G} \to \mathbb{C}^\times$. On note donc $g(\chi)$ au lieu de $\chi(g) = \mathrm{ev}_g(\chi)$. Ainsi :

$$f(g) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} g(\chi)^{-1}\widehat{f}(\chi) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \overline{g(\chi)}\widehat{f}(\chi) = (\widehat{f}, \overline{g})_{\widehat{G}}.$$

7.2.3 Remarque. Dans [Col12], la transformée de Fourier est définie par $\widehat{f}(\chi) = \overline{(f, \chi)}$. Cette convention diffère de celle choisie ici par le facteur $|G|$ ainsi que par la place du conjugué. Ces différences ne sont pas fondamentales (ce ne sont que des questions de convention). Le choix fait ici présente l'avantage d'être cohérent avec celui fait dans 5.3, et c'est aussi le choix fait dans [Pey04] qui est la source la plus utile pour le versant abélien de la théorie.

$$\therefore$$

Dans les trois prochaines sous-sections 7.3 à 7.5, l'objectif est de présenter la transformation de Fourier discrète dans le langage du traitement du signal qui est le plus adapté, ainsi que l'idée de son implémentation sous la forme de l'algorithme TFR (Transformation de Fourier Rapide) ou en anglais FFT (Fast Fourier Transform), et enfin une application à la multiplication de polynômes de grande taille.

Un point important mérite d'être souligné et pour cela nous citons l'introduction du chapitre III de [Pey04] : *plus qu'un simple cas particulier de la transformation de Fourier sur un groupe fini, la transformation de Fourier discrète possède son propre langage et surtout des algorithmes efficaces nettement moins évidents que les formules limpides du chapitre précédent.* Il convient donc de rester modeste : le temps imparti et les connaissances théoriques en jeu ne vous donnent pas les moyens de donner autre chose que des idées générales sur ces notions.

7.3 Transformation de Fourier discrète

Une référence possible pour cette sous-section est [Pey04], chapitre III, § 1 dont nous conservons les notations. Nous présenterons la transformation de Fourier discrète en partant de la transformation de Fourier du groupe cyclique $G = \mathbb{Z}/N\mathbb{Z}$. Rappelons le calcul du groupe dual, déjà vu dans la démonstration de la proposition 7.1.3.

7.3.1 Lemme. *Soient $G = \mathbb{Z}/N\mathbb{Z}$ et $\omega_N \in \mathbb{C}$ une racine primitive N-ème de l'unité. Pour tout $k \in \mathbb{Z}/N\mathbb{Z}$ soit $\chi_k \in \widehat{G}$ le caractère défini par $\chi_k(s) = \omega_N^{-ks}$. Alors l'application $G \to \widehat{G}$ définie par $k \mapsto \chi_k$ est un isomorphisme.* □

Un *signal temporel à valeurs complexes* est une fonction $\widetilde{f} : \mathbb{R} \to \mathbb{C}$, $t \mapsto \widetilde{f}(t)$. Pour numériser ce signal sur un intervalle $[a, b]$, on y choisit N instants $t_0, \ldots, t_{N-1}$; le plus souvent, on choisit la famille équirépartie $t_n = a + n\frac{b-a}{N}$. On définit alors l'*échantillon de taille N du signal $\widetilde{f}$* par :

$$f \stackrel{\text{def}}{=} \{f[n]\}_{n=0}^{N-1} \quad \text{où} \quad f[n] \stackrel{\text{def}}{=} \widetilde{f}(t_n).$$

Ici, on garde la notation de [Pey04] pour en faciliter la lecture, mais il convient de noter qu'un échantillon est bel et bien un N-uplet, c'est-à-dire un ensemble *ordonné*, et que la notation correcte devrait être $f = (f[n])_{n=0}^{N-1}$. Revenons à l'objet mathématique lui-même ; c'est un vecteur $f \in \mathbb{C}^N$, que l'on peut voir aussi comme une fonction $f_1 : \mathbb{Z}/NZ \to \mathbb{C}$, $n \mapsto f[n]$, ou encore comme un élément de l'algèbre de groupe $\mathbb{C}[\mathbb{Z}/N\mathbb{Z}]$. Si pour simplifier on note $\widehat{f}[k] = \widehat{f_1}(\chi_k)$, on voit que la transformée de Fourier telle qu'exprimée dans 7.2.1 prend la forme qui apparaît dans la définition suivante.

7.3.2 Définition. La *transformation de Fourier discrète* (TFD) de l'échantillon $f = \{f[n]\}_{n=0}^{N-1}$ est le vecteur $\widehat{f} = \{\widehat{f}[k]\}_{n=0}^{N-1}$ défini par

$$\widehat{f}[k] = \sum_{n=0}^{N-1} f[n]\omega_N^{-nk}.$$

On note aussi $\mathscr{F}(f) = \widehat{f}$, d'où une application $\mathscr{F} : \mathbb{C}^N \to \mathbb{C}^N$, $f \mapsto \widehat{f}$.

D'après 7.2.1 encore, on retrouve $\widehat{f}$ à partir de f à l'aide de la transformation de Fourier inverse qui s'exprime par $f[n] = \frac{1}{N}\sum_{k=0}^{N-1} \widehat{f}[k]\omega_N^{nk}$.

7.4 Transformation de Fourier rapide

Une référence possible pour cette sous-section est [Pey04], chapitre III, § 2.1-2.2. Pour un signal f dont on connaît un échantillon $\{f[n]\}_{n=0}^{N-1}$, le calcul direct des N coefficients $\widehat{f}[k] = \sum_{n=0}^{N-1} f[n]\omega_N^{-nk}$ de la TFD nécessite $2N^2$ opérations (additions et multiplications complexes) : pour chaque $\widehat{f}[k]$ on effectue N multiplications puis N additions. L'algorithme FFT historique, dû à Cooley et Tukey, permet de réduire ce temps de calcul en faisant tomber le coût à $\mathrm{O}(N \log N)$.

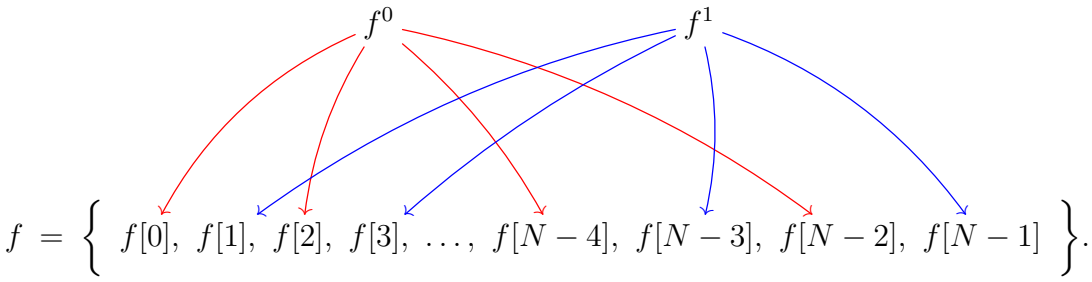
L'algorithme procède par dichotomie pour réordonner les calculs. Pour en présenter l'idée fondamentale, nous supposerons que la longueur de l'échantillon est une puissance de 2, soit $N = 2^p$. On fixe la racine primitive N-ème de l'unité

$$\omega_N = \mathrm{e}^{2i\pi/N}.$$

La clé de l'algorithme sera d'observer que la *partie gauche* et la *partie droite* de $\widehat{f}$:

$$\widehat{f} = \Big\{ \underbrace{\widehat{f}[0], \widehat{f}[1], \widehat{f}[2], \ldots, \widehat{f}[N/2-1]}_{\widehat{f}_g} \,,\, \underbrace{\widehat{f}[N/2], \widehat{f}[N/2+1], \ldots, \widehat{f}[N-1]}_{\widehat{f}_d} \Big\}.$$

s'expriment agréablement en termes des transformées de Fourier discrètes du *vecteur d'indices pairs* et du *vecteur d'indices impairs* de f :



Pour résumer et plus formellement, on pose :

$$\widehat{f}_g = \{\widehat{f}[0], \widehat{f}[1], \ldots, \widehat{f}[N/2-1]\}, \qquad \widehat{f}_d = \{\widehat{f}[N/2], \widehat{f}[N/2+1], \ldots, \widehat{f}[N-1]\},$$

$$f^0 = \{f[0], f[2], \ldots, f[N-2]\}, \qquad f^1 = \{f[1], f[3], \ldots, f[N-1]\}.$$

7.4.1 Lemme. *Pour $k \in \{N/2+1, N/2+2, \ldots, N-1\}$, on pose $k' = k - N/2$.*

(1) *Pour $k \in \{0, 1, 2, 3, \ldots, N/2\}$, on a $\widehat{f}[k] = \widehat{f^0}[k] + \omega_N^{-k} \widehat{f^1}[k]$.*

(2) *Pour $k \in \{\frac{N}{2}+1, \ldots, N-1\}$, on a $\widehat{f}[k] = \widehat{f^0}[k'] - \omega_N^{-k'} \widehat{f^1}[k']$.*

Pour tout $x \in \mathbb{R}$ et $a = \{a_0, \ldots, a_{N-1}\} \in \mathbb{C}^N$, posons $\mathscr{S}_N^x a = \big\{a_j \omega_N^{-xj}\big\}_{j=0}^{N-1} \in \mathbb{C}^N$. Alors :

(3) $\widehat{f}_g = \widehat{f^0} + \mathscr{S}_{N/2}^{1/2} \widehat{f^1}$,

(4) $\widehat{f}_d = \widehat{f^0} - \mathscr{S}_{N/2}^{1/2} \widehat{f^1}$.

Démonstration : En regroupant selon la parité des indices les termes de la somme qui définit $\widehat{f}[k]$, on trouve :

$$\begin{aligned} \widehat{f}[k] &= \sum_{n=0}^{N/2-1} f[2n] \mathrm{e}^{-2ik\pi(2n)/N} + \sum_{n=0}^{N/2-1} f[2n+1] \mathrm{e}^{-2ik\pi(2n+1)/N} \\ &= \sum_{n=0}^{N/2-1} f[2n] \mathrm{e}^{-2ik\pi n/(N/2)} + \omega_N^{-k} \sum_{n=0}^{N/2-1} f[2n+1] \mathrm{e}^{-2ik\pi n/(N/2)}. \end{aligned}$$

Il apparaît une racine primitive $N/2$-ème de l'unité $\omega_{N/2} = \mathrm{e}^{2i\pi/(N/2)}$ qui indique qu'on est en présence de TFD d'échantillons de longueur $N/2$. En tenant compte du fait que $\omega_N^k = -\omega_N^{k'}$, ce calcul donne directement les relations (1) et (2). En réécrivant ces deux égalités à l'aide de l'opérateur $\mathscr{S}_N^x$, on obtient les relations (3) et (4). □

7.4.2 Théorème (algorithme FFT de Cooley-Tukey) *Partant d'un échantillon f, on le sépare en son vecteur pair f^0 et son vecteur impair f^1, qui sont de longueur $N/2$. En appelant une procédure récursive, on calcule les transformées de Fourier discrètes $\widehat{f^0}$ et $\widehat{f^1}$. À l'aide des relations $\widehat{f}_g = \widehat{f^0} + \mathscr{S}^{1/2}_{N/2}\widehat{f^1}$ et $\widehat{f}_d = \widehat{f^0} - \mathscr{S}^{1/2}_{N/2}\widehat{f^1}$ on reconstitue les parties gauche et droite de l'échantillon transformé, puis l'échantillon $\widehat{f}$ lui-même. Le coût de l'algorithme est $\mathrm{O}(N \log N)$.*

L'évaluation du coût $T(N)$ se fait ainsi. La procédure fait deux appels récursifs pour des échantillons de longueur $N/2$, et le réarrangement des termes à l'aide des opérateurs $\mathscr{S}^x_N$ se fait en temps $\mathrm{O}(N)$. On en déduit que $T(N) = 2T(N/2) + \mathrm{O}(N)$. Si on pose $f(N) = T(N)/N$, on a donc $f(N) = f(N/2) + \mathrm{O}(1)$ d'où $f(N) = \mathrm{O}(\log_2(N))$. Voir aussi [Pey04], III, prop. 2.4.

7.5 Application à la multiplication de polynômes

Une référence possible pour cette sous-section est [Pey04], chapitre IV, § 5.1-5.3. Expliquons brièvement l'idée de l'utilisation de la TFD pour la multiplication de polynômes complexes. Tout part de l'observation suivante :

> *La transformation de Fourier d'un groupe cyclique s'identifie avec l'évaluation des polynômes sur les racines de l'unité. La transformation de Fourier inverse s'identifie avec l'interpolation de Lagrange sur les racines de l'unité.*

Nous allons donner un énoncé précis qui explique ces phrases sybillines. Soit G un groupe cyclique de cardinal N. Choisissons un générateur γ pour G, ce qui détermine un isomorphisme :

$$\alpha : (\mathbb{C}[G], *) \xrightarrow{\sim} \mathbb{C}[X]/(X^N - 1)$$

tel que $\alpha(\gamma^n) = X^n$ pour tout $n \in \{0, \dots, N-1\}$, voir 2.2.2. Par ailleurs, choisissons une racine primitive N-ème de l'unité ω, par exemple $\omega = \omega_N = \mathrm{e}^{2i\pi/N}$. Ceci détermine un unique caractère $\chi \in \widehat{G}$ tel que $\chi(\gamma) = \omega$. On a alors $\chi(\gamma^n) = \omega^n$ pour tout n, et χ est un générateur pour $\widehat{G}$ (voir 7.3.1). Introduisons l'isomorphisme :

$$\beta : (\mathbb{C}[\widehat{G}], \cdot) \xrightarrow{\sim} \prod_{k=0}^{N-1} \mathbb{C}$$

défini pour tout élément de $\mathbb{C}[\widehat{G}]$ vu comme une fonction $\varphi : \widehat{G} \to \mathbb{C}$, par :

$$\beta(\varphi) = (\varphi(1), \varphi(\chi), \dots, \varphi(\chi^{N-1})).$$

Enfin rappelons l'isomorphisme classique d'évaluation $\mathbb{C}[X]/(X - a) \xrightarrow{\sim} \mathbb{C}$, $P \mapsto P(a)$, pour tout complexe a, utilisé pour présenter le théorème des restes chinois :

$$\mathrm{TRC} : \frac{\mathbb{C}[X]}{(X^N - 1)} \xrightarrow{\sim} \prod_{k=0}^{N-1} \frac{\mathbb{C}[X]}{(X - \xi_k)} \xrightarrow{\sim} \prod_{k=0}^{N-1} \mathbb{C}.$$

Cette application TRC est définie par $P \mapsto (P(1), P(\omega), \dots, P(\omega^{N-1}))$, c'est l'évaluation en les valeurs $1, \omega, \dots, \omega^{N-1}$. Son inverse est l'interpolation de Lagrange dont on rappelle brièvement la

description. Si $a_0, \dots, a_{N-1}$ sont N nombres complexes donnés, l'interpolation permet de fabriquer un polynôme P tel que $P(\xi_k) = a_k$ pour tout k par la formule $P = \sum_{k=0}^{N-1} a_k L_k$ où

$$L_k = \prod_{\substack{0 \leqslant j \leqslant N-1 \\ j \neq k}} (X - \xi_j) / \prod_{\substack{0 \leqslant j \leqslant N-1 \\ j \neq k}} (\xi_k - \xi_j)$$

est le k-ème polynôme interpolateur de Lagrange.

7.5.1 Lemme. *Avec les notations ci-dessus, les isomorphismes α et β permettent d'identifier la transformation de Fourier $\mathscr{F} : (\mathbb{C}[G], *) \xrightarrow{\sim} (\mathbb{C}[\widehat{G}], \cdot)$ avec l'isomorphisme des restes chinois* TRC. *Plus précisément, on a $\mathscr{F} = \beta^{-1} \circ \mathrm{TRC} \circ \alpha$ c'est-à-dire que le diagramme suivant est commutatif :*

$$\begin{array}{ccc} (\mathbb{C}[G], *) & \xrightarrow{\quad\mathscr{F}\quad} & (\mathbb{C}[\widehat{G}], \cdot) \\ \Big\downarrow{\scriptstyle \alpha} & & \Big\downarrow{\scriptstyle \beta} \\ \dfrac{\mathbb{C}[X]}{(X^N - 1)} & \xrightarrow{\ \mathrm{TRC}\ } & \displaystyle\prod_{k=0}^{N-1} \mathbb{C}. \end{array}$$

Démonstration : Les quatre applications en présence sont des isomorphismes. On doit montrer que $\beta \circ \mathscr{F} = \mathrm{TRC} \circ \alpha$. Soit $f \in \mathbb{C}[G]$, $f = \sum_{n=0}^{N-1} f_n \gamma^n$ où $f_n = f(\gamma^n)$ est la valeur de $f : G \to \mathbb{C}$ sur γ^n. Dans un premier temps calculons $\beta(\mathscr{F}(f))$. Notons $\widehat{f} = \mathscr{F}(f)$ la transformée de Fourier, définie pour $\psi \in \widehat{G}$ par :

$$\widehat{f}(\psi) = \sum_{g \in G} f(g)\psi(g) = \sum_{n=0}^{N-1} f_n \psi(\gamma^n) = \sum_{n=0}^{N-1} f_n \psi(\gamma)^n.$$

L'image de $\widehat{f}$ par β est le uplet dont la k-ème coordonnée vaut $\widehat{f}(\chi^k) = \sum_n f_n \omega^{kn}$, puisque $\chi(\gamma) = \omega$. Dans un second temps calculons $\mathrm{TRC}(\alpha(f))$. Notons $P = \alpha(f) = \sum_n f_n X^n$ modulo $(X^N - 1)$. Son image par TRC est le uplet dont la k-ème coordonnée est $P(\omega^k) = \sum_n f_n \omega^{kn}$. On a obtenu $\beta(\mathscr{F}(f)) = \mathrm{TRC}(\alpha(f))$, comme souhaité. □

Nous allons nous placer dans un anneau $\mathbb{C}[X]/(X^N - 1)$, avec N assez grand, pour calculer le produit de deux polynômes. Lorsqu'on part de deux polynômes P, Q de degré $\leqslant d$, le produit $R = PQ$ est de degré $\leqslant 2d$. Si on veut que les polynômes P, Q, R soient tous trois fidèlement représentés par leur reste modulo $X^N - 1$, il faut donc que $2d \leqslant N - 1$. On choisira un entier $N \geqslant 2d + 1$ qui est une puissance de 2. Considérons l'isomorphisme $\mathscr{F} : \mathbb{C}[X]/(X^N - 1) \xrightarrow{\sim} \prod_{k=0}^{N-1} \mathbb{C}$. Dans l'anneau situé à la source, on représente les polynômes en termes de leurs N coefficients, alors que dans l'anneau situé au but, on les représente en termes de leurs valeurs sur N complexes distincts fixés à l'avance. Lorsqu'il est question d'effectuer le produit de polynômes, cette différence est fondamentale :

- pour deux polynômes donnés par leurs coefficients $P = \sum_{n=0}^{N} P_n X^n$ et $Q = \sum_{n=0}^{N} Q_n X^n$, le calcul direct du coefficient $(PQ)_n = \sum_{k=0}^{n} P_k Q_{n-k}$ coûte $2n + 1$ opérations, si bien que le calcul total du produit PQ coûte N^2 opérations.
- pour deux polynômes donnés par leurs valeurs $(P(\xi_0), \dots, P(\xi_{N-1}))$ et $(Q(\xi_0), \dots, Q(\xi_{N-1}))$, le calcul du produit composante par composante coûte N opérations.

Il est clairement plus avantageux de faire le produit « sur les valeurs ». Ceci donne le résultat suivant.

7.5.2 Théorème (multiplication de polynômes par FFT) *En prenant le chemin du bas dans le schéma suivant, la FFT fournit un algorithme dont le coût est en* $\mathrm{O}(N \log N)$ *pour la multiplication des polynômes de degré inférieur à* N *:*

$$\begin{array}{ccc}
(P_0,\dots,P_{N-1}),(Q_0,\dots,Q_{N-1}) & \xrightarrow[\mathrm{O}(N^2)]{\text{multiplication de polynômes}} & (R_0,\dots,R_{N-1}) \\
\Big\downarrow \text{évaluation } \mathrm{O}(N\log N) & & \Big\uparrow \text{interpolation } \mathrm{O}(N\log N) \\
(P(\xi_0),\dots,P(\xi_{N-1})),(Q(\xi_0),\dots,Q(\xi_{N-1})) & \xrightarrow[\mathrm{O}(N)]{\text{multiplication ponctuelle}} & (R(\xi_0),\dots,R(\xi_{N-1}))
\end{array}$$

7.6 Suggestions de développements

Voici quatre possibilités de développements sur le thème des représentations de groupes finis abéliens (caractères, dualité, transformée de Fourier).

7.6.1 Dualité et bidualité pour un groupe fini abélien. Il s'agit de démontrer que pour G fini abélien, le groupe dual $\widehat{G}$ est isomorphe à G non canoniquement (prop. 7.1.3) et le morphisme de bidualité $\mathrm{ev} : G \to \widehat{\widehat{G}}$ est un isomorphisme (th. 7.1.5). Ce développement peut être préparé à l'aide du chapitre I de [Pey04], qui est spécifique aux groupes abéliens et donne des preuves distinctes de celles données dans ces notes.

7.6.2 TF d'un groupe cyclique et multiplication rapide des polynômes. Pour un groupe fini cyclique, il s'agit de :

(a) démontrer l'orthogonalité des caractères,

(b) en déduire la formule d'inversion de la transformation de Fourier $\mathscr{F}$,

(c) montrer que $\mathscr{F}$ s'identifie au théorème des restes chinois i.e. à l'évaluation (lemme 7.5.1),

(d) expliquer le principe de l'algorithme de multiplication rapide des polynômes (théorème 7.5.2).

Les points (a) à (c) sont des énoncés clairs et précis, avec preuve en bonne et due forme. Pour le point (d) on suppose connue l'existence de l'algorithme FFT et son coût en $\mathrm{O}(N \log N)$; ce point est une simple explication et ne requiert pas vraiment de preuve. Noter qu'on pourrait traiter les points (a) et (b) pour un groupe fini abélien quelconque, mais l'unité du développement se fait autour du cas cyclique, ce qui a le mérite de simplifier un peu les arguments dans (a) et (b). Références : [Pey04], chapitre I (notamment I.2.10, I.2.11, I.4.4) et chapitre IV (notamment IV.5.1). On peut aussi regarder [CLRS04], chapitre 30, ou [GW04], chapitre III.

7.6.3 Théorème de structure des groupes finis abéliens par la dualité. Il s'agit ici de démontrer le théorème de structure des groupes finis abéliens avec la preuve de [Col12], th. I.2.33 (dans le § 5.3 du chapitre I). La preuve utilise la bidualité : il convient donc d'énoncer l'isomorphisme de bidualité ([Col12], prop. I.2.28) et un lemme ([Col12], lemme I.2.32). S'agissant de ces deux résultats préliminaires sur la bidualité, on en démontre ou on en admet ce qu'il faut pour ajuster la durée du développement. Notez que [Col12] s'appuie sur la théorie générale des représentations de groupes pour démontrer ces résultats.

7.6.4 Transformation de Fourier rapide (FFT). Il s'agit de présenter l'algorithme FFT basé sur la dichotomie. Deux références possibles sont [CLRS04], chapitre 30 (précisément 30.2 b) et c)) et [GG13], paragraphe 8.2, notamment 8.14 où est décrit l'algorithme FFT.

8 Exercices

Toutes les représentations sont des $\mathbb{C}$-espaces vectoriels de dimension finie.

8.1 Exercice. Soient G un groupe fini, $\lambda : G \to \mathbb{C}^\times$ un caractère linéaire, et V une représentation. On note $V(\lambda)$ l'espace vectoriel V muni de l'action définie par $g_{V(\lambda)}(x) = \lambda(g)g_V(x)$. Montrez que $V(\lambda)$ est une représentation linéaire de G. Montrez que son caractère est $\chi_{V(\lambda)}(g) = \lambda(g)\chi_V(g)$. Montrez que si λ, μ sont deux caractères linéaires, alors $(V(\lambda))(\mu)$ est isomorphe à $V(\lambda\mu)$.

8.2 Exercice. Soit V une représentation du groupe G. Montrez que la multiplicité de la représentation triviale dans V est égale à la dimension de l'espace des invariants V^G.

8.3 Exercice. Soit X un ensemble fini sur lequel G agit et V la représentation de permutation associée. Calculez le caractère χ_V. Calculez la dimension de l'espace des invariants V^G. Montrez que si X possède au moins deux éléments, alors V n'est pas irréductible.

8.4 Exercice. Soit G un groupe fini et V une représentation irréductible. On note Z le centre de G. Montrez que pour tout $g \in Z$, l'endomorphisme g_V est un G-morphisme. Déduisez-en que c'est une homothétie ; on notera $\omega_V(g)$ le rapport de cette homothétie. Montrez que $\omega_V : Z \to \mathbb{C}^\times$ est un caractère linéaire de Z (on l'appelle le *caractère central* de la représentation irréductible V).

8.5 Exercice. ([Rau00], prop. 5.10) Soit G un groupe fini et T_G sa table de caractères. Pour chaque classe de conjugaison $C \in \mathrm{Conj}(G)$, on note $\delta_C = \sum_{g\in C} g$ la fonction indicatrice de C.

(1) On note $\delta_C = \sum_{\chi\in\mathrm{Irr}(G)} \lambda_\chi(C)\chi$ l'écriture de δ_C sur la base des caractères irréductibles. Donnez une expression pour $\lambda_\chi(C)$.

(2) On considère le produit scalaire hermitien standard $\langle x, y\rangle = \sum x_i\overline{y}_i$ sur $\mathbb{C}^h$ où $h = |\,\mathrm{Conj}(G)|$. En évaluant δ_C sur un élément $k \notin C$, montrez que les colonnes de T_G sont orthogonales deux à deux. En évaluant δ_C sur un élément $k \in C$, montrez que la norme de la colonne d'indice C est égale à $|G|/|C|$. (Voir proposition 6.3.)

8.6 Exercice. Soit $\varphi : G \to H$ un morphisme de groupes (pas nécessairement abéliens ni finis). Démontrez qu'il existe un morphisme naturel $\widehat{\widehat{\varphi}} : \widehat{\widehat{G}} \to \widehat{\widehat{H}}$ tel que $\widehat{\widehat{\varphi}} \circ \mathrm{ev}_G = \mathrm{ev}_H \circ \varphi$.

8.7 Exercice. Soit G un groupe fini et T sa table de caractères, avec en lignes les caractères irréductibles et en colonnes les classes de conjugaison. Supposant que l'on connaît toutes les lignes de T sauf une, expliquez comment compléter la ligne manquante.

8.8 Exercice. Montrez que l'équation $24 = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2$ avec $x_1 = 1$ et $x_2, \ldots, x_5 \geqslant 1$ entiers, n'a qu'une solution. Déduisez-en les dimensions des représentations irréductibles de $\mathfrak{S}_4$.

8.9 Exercice. Soit K un corps. On admet la construction de la K-algèbre $K\{X_1, \ldots, X_n\}$ des *polynômes non commutatifs en* $X_1, \ldots, X_r$. Les règles de calcul y sont les suivantes : les indéterminées X_i ne commutent pas entre elles, mais les scalaires (éléments de K) commutent à chaque X_i. Le polynôme non commutatif $P = 1 + X^2YX + Y^7 + YXYXY^9$ est un exemple d'élément de $K\{X, Y\}$.

(1) Montrez que $K\{X\} = K[X]$.

(2) Soit G un groupe fini engendré par des éléments $g_1, \ldots, g_r$. Montrez que l'algèbre de groupe $K[G]$ est un quotient de $K\{X_1, \ldots, X_n\}$, plus précisément qu'il existe un unique morphisme de K-algèbres $f : K\{X_1, \ldots, X_n\} \to K[G]$ tel que $f(X_i) = g_i$ pour tout i, et que ce morphisme est surjectif. (Compte tenu du fait que la construction précise de $K\{X_1, \ldots, X_n\}$ a été admise, on pourra « se convaincre » plutôt que démontrer...)

(3) Soit $G = \mathbb{D}_n$ le groupe diédral. On considère la présentation par générateurs et relations $G = \langle r, s \,|\, r^n = s^2 = (rs)^2 = 1\rangle$. Démontrez que le morphisme $f : K\{X, Y\} \to K[G]$ déterminé par $f(X) = r$ et $f(Y) = s$, tel que construit dans (2), induit un isomorphisme $K\{X, Y\}/I \xrightarrow{\sim} K[G]$ où I est l'idéal bilatère engendré par les trois polynômes $X^n - 1$, $Y^2 - 1$ et $(XY)^2 - 1$.

8.10 Exercice. Soient G_1, G_2 deux groupes finis. On note $\{V_\chi\}$, resp. $\{W_\psi\}$ une liste de représentants (pour les classes d'isomorphisme) des représentations irréductibles de G_1, resp. de G_2. Montrez que $V_\chi \otimes W_\psi$ est une représentation irréductible de $G_1 \times G_2$. (Nous n'avons pas défini le produit tensoriel $V \otimes V'$ de deux représentations, mais on peut le définir de manière un peu détournée comme $V \otimes V' := \mathrm{Hom}(V^*, V')$.) Montrez que les représentations $V_\chi \otimes W_\psi$ sont toutes non isomorphes deux à deux. En utilisant la relation de Burnside pour $G_1 \times G_2$, vérifiez que l'on obtient ainsi toutes les représentations irréductibles de $G_1 \times G_2$.

Les exercices 8.11 à 8.15 mènent à la table de caractères du groupe symétrique $\mathfrak{S}_4$ en construisant géométriquement chacune des représentations irréductibles, comme dans le livre de Rauch [Rau00]. Une approche plus algébrique est possible, comme dans Peyré [Pey04] ; elle mène à tous les caractères mais ne donne pas autant d'information sur les représentations. Il sera utile de se remémorer les éléments suivants du groupe symétrique $\mathfrak{S}_n$: son sous-groupe dérivé et ses classes de conjugaison.

8.11 Exercice. Soit G un groupe fini. On note G' son sous-groupe dérivé, engendré par les commutateurs, et $G^{\mathrm{ab}} = G/G'$ son abélianisé. Montrez que pour toute représentation V de dimension 1 (ou *caractère linéaire*) du groupe G, le morphisme correspondant $\rho : G \to \mathrm{GL}(V)$ induit un morphisme $\rho^{\mathrm{ab}} : G^{\mathrm{ab}} \to \mathrm{GL}(V)$. Déduisez-en que le groupe symétrique $\mathfrak{S}_n$ possède exactement deux représentations irréductibles de dimension 1.

8.12 Exercice. ([Rau00], p. 46) On rappelle que le groupe des isométries planes d'un polygône régulier à $n \geqslant 3$ côtés est isomorphe au groupe diédral $\mathbb{D}_n$. Le morphisme $\mathbb{D}_n \subset \mathrm{O}_2(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{C})$ définit une représentation complexe V de $\mathbb{D}_n$ de dimension 2, appelée *représentation du n-gone régulier*. On note χ son caractère. Dans la suite, on ne s'intéresse qu'au cas $n = 3$ car on souhaite étudier le groupe symétrique $\mathfrak{S}_3 \simeq \mathbb{D}_3$.

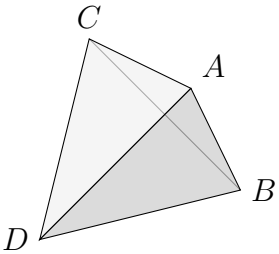
(1) Listez les classes de conjugaison de $\mathbb{D}_3$ et déterminer la valeur de χ sur chaque classe.

(2) Montrez que la représentation V est irréductible, soit directement, soit à l'aide du critère 5.1.4. Dresser la table de caractères de $\mathfrak{S}_3$.

(3) Rappelez comment se décrit l'unique morphisme surjectif $\mathfrak{S}_4 \to \mathfrak{S}_3$ et déduisez de ce qui précède que V définit une représentation de $\mathfrak{S}_4$. Montrez que celle-ci est irréductible.

8.13 Exercice. ([Rau00], p. 40) Soit $T = ABCD$ un tétraède régulier de l'espace affine euclidien $\mathbb{R}^3$. On note G_T le groupe des isométries de $\mathbb{R}^3$ qui laissent T stable.

(1) Montrez que le morphisme de groupes $u : G_T \to \mathfrak{S}_{\{A,B,C,D\}} \simeq \mathfrak{S}_4$ induit par l'action de G_T par permutation des sommets est un isomorphisme. (Pour la surjectivité, exhibez des antécédents par u des transpositions.)

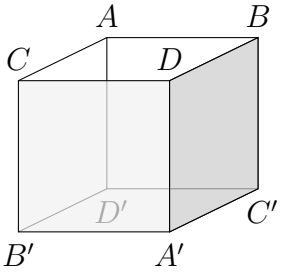


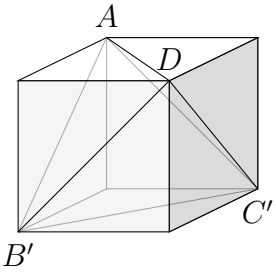
Le morphisme $\mathfrak{S}_4 \simeq G_T \subset \mathrm{O}_3(\mathbb{R}) \subset \mathrm{GL}_3(\mathbb{R}) \subset \mathrm{GL}_3(\mathbb{C})$ définit une représentation complexe $V = V_T$ de $\mathfrak{S}_4$ de dimension 3, appelée *représentation du tétraèdre*. On note χ son caractère.

(2) Donnez un représentant de chacune des classes de conjugaison de $\mathfrak{S}_4$.
   (i) Lorsque g est l'un des éléments $(1,2)$, $(1,2,3)$ ou $(1,2)(3,4)$, décrivez l'isométrie de $\mathbb{R}^3$ qui détermine g_V. Déduisez-en la valeur de $\chi(g)$.
   (ii) Lorsque $g = (1,2,3,4)$, l'isométrie qui détermine g_V est plus difficile à décrire. Montrez que son polynôme caractéristique est diviseur de $X^4 - 1$, à coefficients réels, multiple de $X^2 + 1$, et de terme constant égal à 1. Déduisez-en la valeur de $\chi(g)$.

(3) Montrez que V est une représentation irréductible de $\mathfrak{S}_4$.

8.14 Exercice. ([Rau00], p. 40) Soient C un cube de l'espace affine euclidien $\mathbb{R}^3$, et G_C le groupe des isométries positives (ou déplacements) de $\mathbb{R}^3$ qui laissent C stable.





(1) On note $\mathscr{D} = \{(AA'), (BB'), (CC'), (DD')\}$ l'ensemble des *grandes diagonales* de C, qui joignent un sommet au sommet opposé. Montrez que le morphisme de groupes $u : G_C \to \mathfrak{S}_{\mathscr{D}} \simeq \mathfrak{S}_4$ induit par l'action de G_C par permutation des grandes diagonales est un isomorphisme :
   (i) injectivité : soit $r \in \ker(u)$ avec $r \neq 1$, et Δ son axe. Montrez que pour tout $\delta \in \mathscr{D}$, on a $\Delta = \delta$ ou $\Delta \subset \delta^\perp$. Déduisez-en que Δ est orthogonal à au moins trois des grandes diagonales, ce qui est impossible.
   (ii) surjectivité : exhibez des antécédents par u des transpositions.

Le morphisme $\mathfrak{S}_4 \simeq G_C \subset \mathrm{SO}_3(\mathbb{R}) \subset \mathrm{GL}_3(\mathbb{R}) \subset \mathrm{GL}_3(\mathbb{C})$ définit une représentation complexe $V = V_C$ de $\mathfrak{S}_4$ de dimension 3, appelée *représentation du cube*. On note χ son caractère.

(2) Pour chaque classe de conjugaison de $\mathfrak{S}_4$, et pour un choix de représentant g dans cette classe, donnez la valeur de $\chi(g)$. Pour cela, notez que si la rotation g_V est d'ordre n, alors son angle (qui est bien défini *au signe près*) est égal à $\theta = \pm 2k\pi/n$ avec $\mathrm{pgcd}(k,n) = 1$, et sa trace est égale à $1 + 2\cos(\theta)$. *Commentaire* : il est très intéressant et recommandé de savoir décrire chacune des isométries g_V, mais on voit que ce n'est pas nécessaire pour le calcul du caractère de V_C.

(3) Montrez que V est une représentation irréductible de $\mathfrak{S}_4$.

8.15 Exercice. Utilisez les résultats des trois précédents exercices pour dresser la table des caractères irréductibles de $\mathfrak{S}_4$.

8.16 Exercice. ([Rau00], prop. 6.17) – *exercice à rédiger...*
Le caractère d'une représentation de dimension 1 (i.e. un caractère linéaire) ne s'annule pas. Réciproquement, si le caractère χ d'une représentation V ne s'annule pas, alors V est de dimension 1.

8.17 Exercice. ([Rau00], th. 6.6) – *exercice à rédiger...*
Propriétés d'intégralité. Fait que $\dim(V_\chi)$ divise $|G|$.

La bibliographie ci-dessous contient quelques titres classiques qui peuvent compléter les quatre ouvrages présentés dans le paragraphe 1.2.

Références

[Col12] P. Colmez, *Éléments d'analyse et d'algèbre*, Éditions de l'École Polytechnique, deuxième édition, 2012.

[CLRS04] T. Cormen, C. Leiserson, R. Rivest, C. Stein, *Introduction à l'algorithmique*, deuxième édition, Dunod, 2004.

[GW04] C. Gasquet, P. Witomski, *Analyse de Fourier et applications*, Dunod, 2004.

[GG13] J. von zur Gathen, J. Gerhard, *Modern computer algebra*, Cambridge University Press, third edition, 2013.

[JL03] G. James, M. Liebeck, *Representations and characters of groups*, Cambridge University Press, second edition, 2003.

[Mal81] M.-P. Malliavin, *Les groupes finis et leurs représentations complexes*, Masson, 1981.

[Pey04] G. Peyré, *L'algèbre discrète de la transformée de Fourier*, Ellipses, 2004.

[Rau00] G. Rauch, *Les groupes finis et leurs représentations*, Ellipses, 2000.

[Ren10] D. Renard, *Groupes et représentations*, Ellipses, 2010.

[RWM10] J.-P. Ramis, A. Warusfel, F. Moulin, *Cours de mathématiques pures et appliquées*, volume 1, de Boeck, 2010.

[Ser98] J.-P. Serre, *Représentations linéaires des groupes finis*, Hermann, 1998.