Théorie des représentations de groupes finis (suite)

Emmanuel di Bernardo

Mardi 6 décembre 2016

Ce document résume la présentation donnée en classe le mardi 6 décembre 2016. Son objectif est de prolonger et d'approfondir les notions de théorie des représentations introduites lors de la séance précédente, puis de les mettre en pratique dans quelques cas concrets, afin notamment de démontrer une propriété importante des représentations de $\mathrm{PSL}_2(q)$.

1 Rappels élémentaires

Il convient avant tout de rappeler les notions les plus importantes introduites lors de la présentation précédente. Avant de s'intéresser aux représentations en tant que telles, nous allons définir l'ensemble suivant, qui se révèlera indispendable par la suite.

Définition 1.1. *Soit X un ensemble fini quelconque, $|X| < \infty$. On définit par $\mathbb{C}X$ l'ensemble de toutes les fonctions de X dans $\mathbb{C}$:*

$$\mathbb{C}X := \{f : X \longmapsto \mathbb{C}\}.$$

Cet espace possède les propriétés importantes suivantes :

- Il s'agit d'un espace vectoriel, de dimension égale à l'ordre de X. On le munira du produit scalaire noté $\langle \cdot, \cdot \rangle_X$ défini par

$$\langle f, g \rangle_X := \frac{1}{|X|} \sum_{x \in X} f(x)\overline{g(x)}.$$

  On peut d'ores et déjà noter que si f et g sont des fonctions à valeurs réelles, le produit scalaire est symétrique.

- Soient $W_0 = \left\{ f \in \mathbb{C}X | \sum_{x \in X} f(x) = 0 \right\}$ et $W_0^{\perp} = \{f \in \mathbb{C}X | f(x) = \textit{constante}\}$. Alors on a $\mathbb{C}X = W_0 \oplus W_0^{\perp}$. En d'autres termes, toute fonction $f \in \mathbb{C}X$ peut s'écrire $f = f_0 + f_1$, avec $f_0 \in W_0$ et $f_1 \in W_0^{\perp}$.

  En effet, prenons f une fonction de $\mathbb{C}X$ et définissons $c_f = \sum_{x \in X} f(x)$. Si $c_f = 0$ on a $f \in W_0$ et l'égalité est vérifiée en posant $f_1 = 0$. Sinon, il suffit de poser $f_0(x) = f(x) - \frac{c_f}{|X|}$ et $f_1(x) = \frac{c_f}{|X|}$ pour tout $x \in X$. Évidemment $f = f_0 + f_1$ et $\sum_{x \in X} f_0(x) = \sum_{x \in X}(f(x) - \frac{c_f}{|X|}) = c_f - |X|\frac{c_f}{|X|} = 0$ et on obtient la décomposition désirée.

Nous allons maintenant définir les représentations et donner les propriétés fondamentales s'y rattachant.

Définition 1.2. *Soit G un groupe fini, V un espace vectoriel de dimension finie et π un homomorphisme tel que :*

$$\pi : G \longmapsto GL(V)$$
$$g \longmapsto \pi(g).$$

Alors on dit que le couple (π, V) est une représentation de G sur V. Pour tout g, l'élément $\pi(g)$ est une matrice qui agit sur les vecteurs de l'espace V.

Si il n'y a pas d'ambigüité sur V, on désignera simplement la représentation par l'homomorphisme qui lui est associé, par exemple ici : π.

Exemple 1.3.

- *La représentation triviale (π, V) de G est donnée par :*

$$\pi : G \longmapsto GL(V)$$

$$g \longmapsto Id_V.$$

Cette représentation est définie sur tout espace V mais ne fournit que peu d'informations sur G.

- *Soit G un groupe fini et X un G-espace fini (c'est à dire qu'il existe une action de G sur X). La représentation régulière (ou représentation à gauche) de G est la représentation $(\lambda_X, \mathbb{C}X)$ donnée par :*

$$\lambda_X : G \longmapsto GL(\mathbb{C}X)$$

$$g \longmapsto \lambda_X(g),$$

avec :

$$(\lambda_X(g)f)(x) := f(g^{-1}x), \quad \forall f \in \mathbb{C}X, x \in X.$$

La représentation régulière possède de nombreuses propriétés très importantes que nous étudierons plus en détail par la suite.

Définition 1.4. *Soit (π, V) une représentation d'un groupe fini G, et soit $V_1 \subset V$. On dit que V_1 est un sous espace invariant de V par π si il satisfait :*

$$\pi(g)(V_1) \subseteq V_1, \quad \forall g \in G.$$

Définition 1.5. *Soit (π, V) une représentation d'un groupe fini G, et soit $V_1 \subset V$ un sous-espace invariant. On dit que V_1 est un sous-espace irreductible si ses seuls sous-espaces invariants sont V_1 et l'espace nul. Dans ce cas, on dira que la restriction $\pi|_{V_1}$ est une représentation irréductible.*

Définition 1.6. *Soient (π, V) et (ρ, W) deux représentations d'un même groupe fini G. Si il existe une application linéaire (que l'on peut voir comme une matrice) $T : V \longmapsto W$ vérifiant :*

$$T\pi = \rho T$$

alors on dit que ρ et π sont entrelacées, et on dit que T entrelace π et ρ. Si de plus T est une matrice inversible, alors on a

$$\pi = T^{-1}\rho T$$

et on dit que π et ρ sont équivalentes. On dénote par $Hom_G(\pi, \rho)$ l'espace de toutes les matrices qui entrelacent π et ρ.

Pour toute représentation (π, V) d'un groupe fini G avec V de dimension finie, on peut toujours décomposer π comme une somme directe finie de représentations irréductibles. Cette décomposition est unique, à équivalence près. En effet, deux représentations équivalentes livrent exactement la même information sur G, simplement dans des espaces différents.

Définition 1.7. *Soir G un groupe fini et (π, V) une représentation de G. Le caractère de π noté χ_π est l'application définie par :*

$$\chi_\pi(g) := Tr(\pi(g)).$$

Il s'agit d'une fonction de $\mathbb{C}G$. Bien que cette définition puisse sembler arbitraire, le caractère est un outil puissant qui contient beaucoup d'informations sur la représentation. Nous rappellons ici succintement quelques-unes de ses propriétés les plus remarquables.

Proposition 1.8. *Soit G un groupe fini et (π, V) une représentation de G. Alors π est irreductible si et seulement si*

$$\langle \chi_\pi, \chi_\pi \rangle_G = 1.$$

Cette affirmation découle du résultat important suivant[1] :

Théorème 1.9. ***(Lemme de Schur)*** *Soit G un groupe fini et (π, V), (ρ, W) deux représentations irréductibles de G. Alors :*

$$\langle \chi_\pi, \chi_\rho \rangle_G = dim_{\mathbb{C}}(Hom(\pi, \rho)) = \begin{cases} 1 \text{ si } \pi \text{ et } \rho \text{ sont équivalents} \\ 0 \text{ sinon} \end{cases}.$$

Autrement dit, l'espace des matrices qui entrelacent π et ρ a au plus une dimension égale à 1.

Pour conclure cette section, nous énoncerons sans preuve la formule suivante[2] :

Proposition 1.10. ***(Formule du degré)*** *Soit $(\pi_1, V_1), ..., (\pi_h, V_h)$ la liste des représentations irréductibles d'un groupe fini G, à équivalence près. Soit $n_i = dim(V_i)$ le degré de π_i. Alors :*

$$\sum_{i=1}^{h} n_i^2 = |G|.$$

Notons que le nombre de représentations irréductibles non-équivalentes de G est fini si $|G| < \infty$. En effet, d'après le lemme de Schur, les caractères des représentations irréductibles non-équivalentes de G sont orthonormaux dans $\mathbb{C}G$. Mais une liste de fonctions orthonormales entre elles dans $\mathbb{C}G$ ne peut pas contenir plus de $|\mathbb{C}G| = |G|$ éléments, c'est à dire qu'il ne peut y avoir qu'au plus $|G|$ représentations irréductibles non-équivalentes de $|G|$.

2 Application dans un cas concret : le groupe abélien

2.1 Préambule

Essayons à présent de mettre en application ces différentes notions dans un cas concret. Par exemple, si G est un groupe fini abélien, alors les représentations de G auront des propriétés particulières, et si en plus G est cyclique, alors toutes ses représentations peuvent directement être explicitées. Nous aurons besoin du résultat suivant :

Proposition 2.1. *Soit G un groupe fini et (π, V) une représentation irréductible de G. Alors*

$$Hom_G(\pi, \pi) = \{T \in GL(V) \mid T = \lambda \cdot Id, \lambda \in \mathbb{C}\},$$

où Id est la matrice identité.

Démonstration : Bien évidemment, π est équivalente à elle-même. Par application directe du lemme de Schur, puisque π est irréductible, on doit donc avoir $dim_{\mathbb{C}}(Hom_G(\pi, \pi)) = 1$. Si $T \in Hom_G(\pi, \pi)$, alors T commute avec la matrice π :

$$T\pi = \pi T.$$

[1] Cf. Corollaire 3.4.21 dans le livre
[2] Cf. Corollaire 3.4.24

On sait que les matrices scalaires de la forme $T = \lambda \cdot Id$ commutent avec toutes les matrices (la vérification est immédiate), elles sont donc solutions du problème :

$$\{T = \lambda \cdot Id, \lambda \in \mathbb{C}\} \subseteq Hom_G(\pi, \pi).$$

L'ensemble des matrices scalaires est isomorphe à $\mathbb{C}$ et forme un espace de dimension 1. D'après le lemme de Schur, il ne peut pas y en avoir d'autres : nous avons donc trouvé toutes les matrices qui entrelacent π avec elle-même. □

2.2 Le groupe abélien

Le résultat précédent est un résultat général, valable pour tout groupe G fini. Appliqué au cas particulier d'un groupe abélien, il permet de démontrer la proposition suivante.

Proposition 2.2. *Soit G un groupe fini abélien et soit $n = |G|$. Alors G possède exactement n représentations irréductibles non-équivalentes de degré 1.*

Démonstration : Soit (π, V) une représentation irréductible de G. Puisque G est abélien, on a

$$\pi(gh) = \pi(hg), \quad \forall\ g, h \in G.$$

Mais π est un homomorphisme. Donc

$$\pi(g)\pi(h) = \pi(h)\pi(g), \quad \forall\ g, h \in G.$$

En d'autres termes, la matrice $\pi(g)$ entrelace π avec elle même pour tout $g \in G$. D'après la proposition précédente, cela implique que $\pi(g) = \lambda_g \cdot Id, \lambda_g \in \mathbb{C}$.
Pour tout élément $v \in V$, on a $\pi(g)(v) = \lambda_g \cdot Id \cdot v = \lambda_g \cdot v \in \mathbb{C} \cdot v$ d'où $\pi(g)(\mathbb{C} \cdot v) \subseteq \mathbb{C} \cdot v$.
$\mathbb{C} \cdot v$ est donc un sous-espace invariant, isomorphe à $\mathbb{C}$ et donc de dimension 1, quel que soit v.
Autrement dit, tout sous-espace $V_1 \in V$ de dimension supérieure à 1 peut être décomposé le long de ses vecteurs de base en autant de sous-espaces invariants de dimension 1.
Soient maintenant $(\pi_1, V_1), ..., (\pi_h, V_h)$ la liste de toutes les représentations irréductibles de G, à équivalence près. Puisqu'elles ont toutes degré 1, on obtient en appliquant la formule du degré :

$$\sum_{i=1}^{h} n_i^2 = |G| \Rightarrow \sum_{i=1}^{h} 1 = n \Rightarrow h = n.$$

G possède donc bien n représentations irréductibles non-équivalentes de degré 1. □

2.3 Le groupe cyclique

Si G n'est pas seulement abélien, mais cyclique, alors ses représentations peuvent être données explicitement. Soit à nouveau $n = |G|$. Notons que si G est cyclique, on a $G = \mathbb{Z}/n\mathbb{Z}$
à isomorphisme près. Il suffit donc d'étudier les propriétés de $\mathbb{Z}/n\mathbb{Z}$ pour caractériser entièrement G.

Proposition 2.3. *Soit $G = \mathbb{Z}/n\mathbb{Z}$. Alors G possède n représentations $(\chi_1, \mathbb{C}), ..., (\chi_n, \mathbb{C})$ de la forme $\chi_i(z) = \omega^{a_i z}$, avec $a_i \in \{0, ..., n-1\}$ et $\omega = e^{\frac{2i\pi}{n}}$.*

Démonstration : Puisque G est abélien, on a n représentations irréductibles non-équivalentes $(\pi_1, V_1), ..., (\pi_n, V_n)$ de G avec $dim(V_i) = 1$. Soit χ_i le caractère de π_i. Puisque le degré de π_i vaut 1, $V_i = \mathbb{C}$ et $\pi_i : G \longmapsto \mathbb{C}$ est une fonction de $\mathbb{C}G$. En particulier, une matrice de taille 1 est égale à sa trace, ce qui permet d'affirmer que la représentation π_i est égale à son caractère χ_i. Alors χ_i est un homomorphisme de groupes, c'est à dire $\chi_i(z_1 z_2) = \chi_i(z_1)\chi_i(z_2)$ pour tous $z_1, z_2 \in G$ et $\chi_i(1) = 1$. D'autre part, puisque G est cyclique, on a $z^n = 1, \forall z \in G$. En combinant ces résultats, on obtient :

$$1 = \chi_i(1) = \chi_i(z^n) = \chi_i(z)^n, \qquad \forall z \in G$$

Les solutions pour $\chi_i(z)$ sont les n racines de l'unité dans $\mathbb{C}$:

$$\chi_i(z) = e^{\frac{2i\pi a_i z}{n}}, \qquad a_i \in \{0, ..., n-1\}$$

ou, pour adopter une écriture plus compacte en posant $\omega = e^{\frac{2i\pi}{n}}$:

$$\chi_i(z) = \omega^{a_i z}.$$

□

3 Représentations de $PSL_2(q)$

L'objectif de cette présentation sera de montrer le résultat fondamental suivant :

Théorème 3.1. *Soit q un nombre premier, $q \geqslant 5$. Alors toute représentation irréductible non-triviale de $PSL_2(q)$ a au moins degré $\frac{q-1}{2}$.*

Pour ce faire, nous commencerons par démontrer quelques propriétés importantes de la représentation régulière λ_X. En les appliquant ensuite au cas particulier de $PSL_2(q)$, on obtiendra la preuve du théorème.

3.1 La représentation λ_X^0

Nous avions vu dans la section 1 que, pour G un groupe fini et X un G-espace fini, on définit la représentation régulière λ_X de G par :

$$\lambda_X : G \longmapsto GL(\mathbb{C}X),$$

$$\lambda_X(g)(f(x)) = f(g^{-1}x).$$

Notons que $\lambda_X(g)$ ne modifie pas directement f, elle se contente de permuter ses arguments. Soit $x_1, ..., x_l$ la liste de ces éléments et $\delta_{x_1}, ..., \delta_{x_l}$ les fonction de $\mathbb{C}X$ définies par :

$$\delta_{x_i}(y) = \begin{cases} 1 \text{ si } y = x_i \\ 0 \text{ sinon.} \end{cases}$$

Ces fonctions forment une base de $\mathbb{C}X$. Toute fonction $f \in \mathbb{C}X$ peut être exprimée comme un vecteur dans cette base, et l'action de $\lambda_X(g)$ sur f est une permutation des composantes. On en déduit que la matrice $\lambda_X(g)$ est une *matrice de permutation* pour tout g : toutes ses entrées sont donc soit 0, soit 1. Ce constat nous sera d'une grande utilité par la suite.

Proposition 3.2. *Soit G un groupe fini et X un G-espace fini, avec $\mathbb{C}X = W_0 \oplus W_0^\perp$ la décomposition de $\mathbb{C}X$ vue en section 1. Alors W_0 et $W_0^\perp$ sont des espaces invariants pour λ_X.*

Démonstration : Soit $f \in W_0^\perp$. Alors f est constante et $(\lambda_X(g)f)(x) = f(g^{-1}x) = f(x)$ quels que soient x et g. Donc non seulement $W_0^\perp$ est invariant par λ_X, mais en plus la restriction $\lambda_X|_{W_0^\perp}$ est l'application identité sur $W_0^\perp$.

Soit maintenant $f \in W_0$. On a donc $\sum_{x \in X} f(x) = 0$. Montrons que $\lambda_X(g)f \in W_0$:

$$\sum_{x \in X} \lambda_X(g)f(x) = \sum_{x \in X} f(g^{-1}x) = \sum_{x \in X} f(x) = 0.$$

La deuxième égalité provient du fait que $g^{-1}X = X$ car X est un G-espace. Les deux sommes contiennent donc les mêmes termes, simplement pas dans le même ordre : elles sont égales car X est fini. Ainsi $(\lambda_X(g)f)(x) \in W_0$ et W_0 est invariant par λ_X. □

En définissant $\lambda_X^0 = \lambda_X|_{W_0}$, cette proposition livre la décomposition suivante pour λ_X sur $\mathbb{C}X$:

$$\lambda_X = \lambda_X^0 \oplus Id,$$

où Id est la matrice triviale de dimension 1 car $W_0^\perp$ a dimension 1.

Définition 3.3. ***(2-transitivité)*** *Soit G un groupe fini et X un G-espace. On dit que l'action de G sur X est 2-transitive si pour tous (x_1, x_2) et $(y_1, y_2) \in X \times X$ avec $x_1 \neq x_2$ et $y_1 \neq y_2$ on peut trouver un élément $g \in G$ tel que $gx_1 = y_1$ et $gx_2 = y_2$.*

Nous disposons maintenant de tous les éléments pour montrer la proposition suivante. Il faudra parfois utiliser certains éléments de la présentation donnée la semaine précédente, qui seront systématiquement rappelés.

Proposition 3.4. *Soit G un groupe fini et X un G-espace fini. Alors si l'action de G sur X est 2-transitive, λ_X^0 est une représentation irréductible.*

Démontration : Considérons l'action de G sur $X \times X$ donnée par $g(x, y) = (gx, gy)$, pour tous $x, y \in X, g \in G$. Soit $Diag = \{(x, x) \in X \times X \mid x \in X\}$. Nous allons montrer que l'action de G sur $X \times X$ possède exactement deux orbites : $Diag$ et $X \times X - Diag$. En effet, par définition de la 2-transitivité de l'action de G sur X, pour tous (x_1, x_2) et $(y_1, y_2) \in X \times X - Diag$, on peut trouver $g \in G$ tel que $g(x_1, x_2) = (y_1, y_2)$. Tous ces éléments appartiennent bien à la même orbite. En revanche, il n'existe pas g tel que $g(x_1, x_2) = (y, y)$ pour $(y, y) \in Diag$, car cela impliquerait $gx_1 = gx_2$ et donc g n'est pas une permutation de X, ce qui contredit les hypothèses. Donc $X \times X - Diag$ est une orbite sur $X \times X$.

D'autre part, il est évident que si X est 2-transitif, il est aussi transitif : pour tout $x, y \in X$, il existe $g \in G$ avec $gx = y$. En particulier, pour $(x, x), (y, y) \in Diag$, il existe $g \in G$ avec $g(x, x) = (y, y)$. $Diag$ est alors une autre orbite de l'action de G et il y a 2 orbites sur $X \times X$.

Lors de la séance précédente, nous avions vu que si G agit sur Y (finis), alors si n est le nombre d'orbites sur Y, on a la relation suivante :

$$n = \frac{1}{|G|} \sum_{g \in G} \chi_{\lambda_Y}(g).$$

Dans notre cas, puisque nous considérons l'action sur $X \times X$ et que nous avons 2 orbites, l'équation devient :

$$2 = \frac{1}{|G|} \sum_{g \in G} \chi_{\lambda_{X \times X}}(g).$$

Il nous faut maintenant déterminer $\chi_{\lambda_{X \times X}}$. Pour ce faire, construisons l'application

$$\phi : \mathbb{C}X \otimes \mathbb{C}X \longmapsto \mathbb{C}(X \times X)$$

$$\phi(f_1 \otimes f_2)(x, y) := f_1(x) f_2(y).$$

Une vérification directe montre que cette application est un isomorphisme entre $\mathbb{C}X \otimes \mathbb{C}X$ et $\mathbb{C}(X \times X)$. Lors de la présentation précédente, nous avions vu deux résultats importants sur les caractères de représentations régulières. Premièrement, si X et X' sont deux G-espaces isomoprphes, alors $\chi_{\lambda_X} = \chi_{\lambda_{X'}}$. Deuxièmement, $\lambda_{X \otimes X} = \lambda_X^2$. En mettant ces deux résultats ensembles nous obtenons

$$2 = \frac{1}{|G|} \sum_{g \in G} \chi_{\lambda_X}(g)^2.$$

On reconnaît ici la formule du produit scalaire sur $\mathbb{C}G$:

$$2 = \langle \chi_{\lambda_X}, \chi_{\lambda_X} \rangle_G.$$

Rappellons que $\lambda_X = \lambda_X^0 \oplus Id$. Puisque le caractère d'une représentation est la trace de sa matrice, $\chi_{\lambda_X} = \chi_{\lambda_X^0} + \chi_{Id} = \chi_{\lambda_X^0} + 1$ car Id est la matrice identité de dimension 1. En substituant dans le produit scalaire et en appliquant la distributivité, on obtient

$$2 = \langle \chi_{\lambda_X^0}, \chi_{\lambda_X^0} \rangle_G + \langle \chi_{\lambda_X^0}, 1 \rangle_G + \langle 1, \chi_{\lambda_X^0} \rangle_G + \langle 1, 1 \rangle_G.$$

Puisque λ_X et donc λ_{X^0} est une matrice de permutation (donc à coefficients dans $\mathbb{N}$), sa trace est aussi dans $\mathbb{N}$. Il n'y a donc aucun nombre complexe dans cette équation et les produits scalaires commutent. De plus, toutes les valeurs de ces produits scalaires sont des entiers naturels, en particulier une application directe de la définition donne $\langle 1, 1 \rangle_G = 1$. L'équation devient alors

$$1 = \langle \chi_{\lambda_X^0}, \chi_{\lambda_X^0} \rangle_G + 2\langle 1, \chi_{\lambda_X^0} \rangle_G.$$

Mais puisque ces produits scalaires sont des nombres naturels, la seule solution possible est $\langle 1, \chi_{\lambda_X^0} \rangle_G = 0$ et $\langle \chi_{\lambda_X^0}, \chi_{\lambda_X^0} \rangle_G = 1$. Cette dernière égalité implique que λ_X^0 est irréductible (en vertu de Prop. 7) ce qui conclut la preuve. □

3.2 Degré des représentations de $PSL_2(q)$

Rappel : Soit q un nombre premier, $q \geqslant 5$. L'application de Möbius ϕ a été définie précédemment par :

$$\phi : A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \phi_A(z) = \frac{az+b}{cz+d}, \qquad z \in \mathbb{F}_q.$$

On avait montré que $PSL_2(q)$ est isomorphe $\phi(SL_2(q))$.

Nous allons maintenant utiliser la théorie des représentations développée jusqu'ici pour montrer le Théorème 13. Pour ce faire, commençons par définir B comme étant le groupe des transformations affines de $\mathbb{F}_q$:

$$B = \left\{ z \mapsto az + b \mid a \in \mathbb{F}_q^*, b \in \mathbb{F}_q \right\}.$$

$\mathbb{F}_q$ peut donc être vu comme un B-espace fini. Comme précédemment, on définit $W_0 = \left\{ f \in \mathbb{C}\mathbb{F}_q | \sum_{z \in \mathbb{F}_q} f(x) = 0 \right\}$ et on obtient la représentation régulière $\lambda_{\mathbb{F}_q} : B \longmapsto GL(\mathbb{C}\mathbb{F}_q)$, ainsi que sa restriction $\lambda^0_{\mathbb{F}_q}$ sur W_0.

Lemme 3.5. *$\lambda^0_{\mathbb{F}_q}$ est une représentation irréductible de B, de degré $q-1$.*

Démonstration : D'après la Proposition 3.4, il nous suffit de montrer que l'action de B sur $\mathbb{F}_q$ est 2-transitive. En d'autre termes, si (x_1, x_2) et (y_1, y_2) sont des couples d'éléments dans $\mathbb{F}_q$ avec $x_1 \neq x_2$ et $y_1 \neq y_2$, il faut montrer qu'il existe une transformation affine $g(z) = az + b$ dans B avec :

$$\begin{cases} ax_1 + b = y_1 \\ ax_2 + b = y_2 \end{cases}.$$

Cela revient à résoudre l'équation d'une droite passant par les points (x_1, y_1) et (x_2, y_2). La solution d'un tel problème est de la forme :

$$g(z) = \frac{y_2 - y_1}{x_2 - x_1}(z - x_1) + y_1$$

(la vérification est immédiate par substitution). Il s'agit bien d'un élément de B, $\mathbb{F}_q$ est donc 2-transitif et la représentation $\lambda^0_{\mathbb{F}_q}$ est une représentation irréductible. De plus, puisque $dim(W_0) = dim(\mathbb{C}\mathbb{F}_q) - 1 = q - 1$, alors $\lambda^0_{\mathbb{F}_q}$ a degré $q-1$. □

Nous allons maintenant introduire le sous-ensemble B_0 défini par

$$B_0 := \phi \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{F}_q^*, b \in \mathbb{F}_q \right\}.$$

B_0 est donc un sous-groupe de B, et ses éléments sont les transformations de la forme $g(z) = \frac{az+b}{a^{-1}}$ ou, plus simplement :

$$g(z) = a^2 z + b, \qquad a \in \mathbb{F}_q^*, b \in \mathbb{F}_q.$$

De plus, en définissant par $\mathbb{F}_q^{*2}$ l'ensemble des carrés de $\mathbb{F}_q$ et en définissant l'homomorphisme $\alpha : B \longmapsto \mathbb{F}_q^*$ par :

$$\alpha(z \longmapsto az + b) = a,$$

on a $B_0 = \alpha^{-1}(\mathbb{F}_q^{*2})$.

Théorème 3.6. *Soit q un nombre premier. Alors B_0 admet $\frac{q+3}{2}$ représentations irréductibles à équivalence près, dont :*

- *$\frac{q-1}{2}$ homomorphismes de groupe $\chi_1, ..., \chi_{\frac{q-1}{2}} : B_0 \longmapsto \mathbb{C}^*$*
- *2 représentations non-équivalentes de degré $\frac{q-1}{2}$, notées ρ^+ et ρ^-.*

Démonstration : Il est aisé de montrer que le groupe $\mathbb{F}_q^{*2}$ est un groupe abélien : soient $a^2, b^2 \in \mathbb{F}_q^{*2}$, alors $a^2b^2 = (ab)^2 \in \mathbb{F}_q^{*2}$. En vertu de la Proposition 2.2, $\mathbb{F}_q^{*2}$ doit donc admettre $\frac{q-1}{2}$ représentations non-équivalentes $\pi_1, ..., \pi_{\frac{q-1}{2}} : \mathbb{F}_q^{*2} \longmapsto \mathbb{C}^*$, toutes de degré 1. En composant par l'homomorphisme$\alpha|_{B_0}$ et en posant $\chi_i = \pi_i \circ \alpha|_{B_0}$, on obtient $\frac{q-1}{2}$ représentations $\chi_1, ..., \chi_{\frac{q-1}{2}} : B_0 \longmapsto \mathbb{C}^*$, toutes de degré 1.

Considérons maintenant la restriction de $\lambda^0_{\mathbb{F}_q}$ à B_0. Nous allons montrer qu'elle se décompose en deux représentations irréductibles de degré $\frac{q-1}{2}$. Définissons pour tout $c \in \mathbb{F}_q$ les fonctions $e_c : \mathbb{F}_q \longmapsto \mathbb{C}$ données par :

$$e_c(z) = \omega^{cz}, \qquad \omega = e^{\frac{2\pi i}{q}}.$$

De telles fonctions étaient déjà intervenues dans la Section 2.3. Ces fonctions forment une base de $\mathbb{C}\mathbb{F}_q$, en effet pour $c, c' \in \mathbb{F}_q$ on a :

$$\langle e_c, e_{c'} \rangle_{\mathbb{F}_q} = \frac{1}{q} \sum_{z=0}^{q-1} \omega^{(c-c')z} = \begin{cases} 1 \text{ si } c = c' \\ 0 \text{ sinon.} \end{cases}$$

Cette égalité provient du fait que, pour $c \neq c'$, il s'agit d'une somme sur les q racines q-ièmes de l'unité, et cette somme est toujours nulle. En revanche, si $c = c'$, tous les termes de la somme valent 1. Nous avons donc q fonctions différentes qui engendrent un espace de dimension q : elles en forment une base. En fait, on pourrait même montrer que les e_c avec $c \in \mathbb{F}_q^*$ engendrent W_0 et e_0 engendre $W_0^\perp$ (cela découle directement de propriétés de ces fonctions).
Rappellons que pour $g \in B_0$ et $z \in \mathbb{F}_q$ l'action de B_0 sur $\mathbb{F}_q$ est donnée par $gz = az + b$, avec $a \in \mathbb{F}_q^{*2}$ et $b \in \mathbb{F}_q$ des coefficients dépendant de g. La transformation inverse est alors donnée par $g^{-1}z = \frac{z-b}{a}$. Ainsi :

$$(\lambda^0_{\mathbb{F}_q}(g)e_c)(z) = e_c(g^{-1}z) = e_c(\frac{z-b}{a}) = \omega^{c\frac{z-b}{a}} = \omega^{-\frac{cb}{a}} e_{c/a}(z).$$

Dénotons par W^+ le sous-espace de W_0 engendré par les e_c avec $c \in \mathbb{F}_q^{*2}$, et W^- son complémentaire dans W_0 :

$$W^+ = \text{span}\langle e_c : c \in \mathbb{F}_q^{*2} \rangle$$
$$W^- = \text{span}\langle e_c : c \in \mathbb{F}_q^* - \mathbb{F}_q^{*2} \rangle.$$

Si $e_c \in W^+$, alors $c \in \mathbb{F}_q^{*2}$ et $\lambda^0_{\mathbb{F}_q}(g)e_c = \omega^{-\frac{cb}{a}} e_{c/a}$. Mais a est un carré, donc $\frac{c}{a} \in \mathbb{F}_q^{*2}$ et $\lambda^0_{\mathbb{F}_q}(g)e_c \in W^+$ pour tout $g \in B_0$. Inversement, par le même raisonnement on montre que si $e_c \in W^-$, alors $\lambda^0_{\mathbb{F}_q}(g)e_c \in W^-$ pour tout $g \in B_0$. Ces deux espaces sont donc des sous-espaces invariants par $\lambda^0_{\mathbb{F}_q}$: notons ρ_+ et ρ_- les restrictions de $\lambda^0_{\mathbb{F}_q}|_{B_0}$ à W^+ et W^- respectivement. Notons que pour tout $a \in \mathbb{F}_q^*$, $a^2 = (-a)^2$. On a donc $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$ ce qui implique $|\mathbb{F}_q^* - \mathbb{F}_q^{*2}| = \frac{q-1}{2}$. Il en suit :

$$dim_{\mathbb{C}} W^+ = dim_{\mathbb{C}} W^- = \frac{q-1}{2}$$

et les degrés pour B_0 de ρ_+ et ρ_- valent $\frac{q-1}{2}$. Il faut à présent montrer que ces deux représentations sont irréductibles. Pour ce faire, constatons que si g est un élément de $B - B_0$, c'est à dire g est de la forme $g(z) = az + b$ avec $a \in \mathbb{F}_q^* - \mathbb{F}_q^{*2}$, alors $\lambda_{\mathbb{F}_q^0}(g)$ intervertit W^+ et W^-. En effet, si e_c est un élément de la base de W^+, alors c est un carré, mais si a n'en est pas un, alors $e_{c/a} \in W^-$. L'autre sens découle de la surjectivité de $\lambda_{\mathbb{F}_q}$. Ainsi, la décomposition de $\lambda_{\mathbb{F}_q}$ sur $W_0 = W^+ \oplus W^-$ s'écrit explicitement :

$$\lambda^0_{\mathbb{F}_q}(g) = \begin{cases} \begin{pmatrix} \rho_+(g) & 0 \\ 0 & \rho_-(g) \end{pmatrix} & \text{si } g \in B_0 \\ \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix} & \text{si } g \in B - B_0. \end{cases}$$

Ce qui donne pour les caractères :

$$\chi^0_{\lambda_{\mathbb{F}_q}}(g) = \begin{cases} \chi_{\rho_+}(g) + \chi_{\rho_-}(g) \text{ si } g \in B_0 \\ 0 \qquad\qquad\quad \text{si } g \in B - B_0 \end{cases}.$$

Nous avons montré dans le Lemme 3.5 que $\lambda^0_{\mathbb{F}_q}$ est une représentation irréductible sur B. On a donc :

$$1 = \left\langle \chi_{\lambda^0_{\mathbb{F}_q}}, \chi_{\lambda^0_{\mathbb{F}_q}} \right\rangle_B = \frac{1}{|B|} \sum_{g \in B} |\chi_{\lambda^0_{\mathbb{F}_q}}(g)|^2$$

par la définition du produit scalaire. Remarquons que $|B| = |\mathbb{F}_q^*| \cdot |\mathbb{F}_q| = q(q-1)$, et $|B_0| = |\mathbb{F}_q^{*2}| \cdot |\mathbb{F}_q| = \frac{q(q-1)}{2}$. En particulier $|B| = 2|B_0|$. En substituant dans l'équation et en développant la somme, on obtient :

$$1 = \frac{1}{2|B_0|} \left(\sum_{g \in B_0} |\chi_{\lambda^0_{\mathbb{F}_q}}(g)|^2 + \sum_{g \in B - B_0} |\chi_{\lambda^0_{\mathbb{F}_q}}(g)|^2 \right).$$

La deuxième somme est nulle en vertu de ce qui précède, l'équation devient alors :

$$1 = \frac{1}{2|B_0|} \sum_{g \in B_0} |\chi_{\lambda^0_{\mathbb{F}_q}}(g)|^2$$

$$1 = \frac{1}{2|B_0|} \sum_{g \in B_0} |\chi_{\rho_+}(g) + \chi_{\rho_-}(g)|^2$$

$$1 = \frac{1}{2} \langle \chi_{\rho_+} + \chi_{\rho_-}, \chi_{\rho_+} + \chi_{\rho_-} \rangle_{B_0}.$$

On peut procéder ici comme dans la preuve de la Proposition 3.4 : puisque ρ_+ et ρ_- sont des restrictions de $\lambda^0_{\mathbb{F}_q}$, ce sont aussi des matrices à coefficients dans $\mathbb{N}$, et il en va de même pour leur caractère. Alors le produit scalaire commute, et on obtient après développement :

$$1 = \frac{1}{2}(\langle \chi_{\rho_+}, \chi_{\rho_+} \rangle_{B_0} + 2\langle \chi_{\rho_+}, \chi_{\rho_-} \rangle_{B_0} + \langle \chi_{\rho_-}, \chi_{\rho_-} \rangle_{B_0}).$$

Encore une fois, tous ces produits scalaires sont à valeurs dans $\mathbb{N}$, avec $\langle \chi_{\rho_+}, \chi_{\rho_+} \rangle_{B_0} \neq 0$ car on aurait sinon $\chi_{\rho_+}(g) = 0$ pour tout g dans B_0. Or ρ_+ est un homomorphisme, on sait donc au moins que $\rho_+(e) = Id$ est une matrice à trace non-nulle. Il y a donc au moins un terme dans l'expression

$$\langle \chi_{\rho_+}, \chi_{\rho_+} \rangle_{B_0} = \frac{1}{\frac{|q-1|}{2}} \sum_{g \in B_0} \chi^2_{\rho_+}(g)$$

qui est non nul, et puisque tous les termes sont des carrés de nombres réels (donc positifs), elle est non-nulle. La seule solution possible à cette équation est donc :

$$\chi^0_{\lambda^0_{\mathbb{F}_q}}(g) = \begin{cases} \langle \chi_{\rho_+}, \chi_{\rho_+} \rangle_{B_0} = \langle \chi_{\rho_-}, \chi_{\rho_-} \rangle_{B_0} = 1 \\ \langle \chi_{\rho_+}, \chi_{\rho_-} \rangle_{B_0} = 0 \end{cases}.$$

La première équation implique que ρ_+ et ρ_- sont irréductibles. La seconde implique que ces deux représentations ne sont pas équivalentes.

Nous avons donc trouvé toutes les représentations prévues par le Théorème, il faut toutefois certifier qu'il n'en existe pas d'autres. Utilisons pour cela la formule du degré : nous avons vu $|B_0| = \frac{q(q-1)}{2}$. La somme des carrés des degrés de toutes les représentations trouvées jusqu'à maintenant vaut :

$$\frac{q-1}{2} 1^2 + 2 \cdot \left(\frac{q-1}{2} \right)^2 = \frac{q(q-1)}{2} = |B_0|.$$

Nous avons donc trouvé toutes les représentations de B_0 et prouvé le théorème.□

À présent, nous sommes en mesure de donner la preuve du théorème 13, le théorème principal de cette présentation.

Preuve du théorème 3.1 : Soit π une représentation non-triviale quelconque de $PSL_2(q)$ sur $\mathbb{C}^n$. Considérons sa restriction $\pi|_{B_0}$. Elle peut se décomposer en une somme directe de représentations irréductibles de B_0, dont la liste exhaustive est spécifiée par le Théorème 18. Il a été montré précédemment que, pour $q \geqslant 5$, $PSL_2(q)$ est un groupe simple. Ainsi, la représentation $\pi|_{B_0}$ est

injective, c'est à dire $\pi_{B_0}(g) \neq Id$ pour $g \neq e$, où e est l'élément neutre de B_0. En effet, si tel n'était pas le cas, $Ker(\pi)$ serait un sous-groupe normal non-trivial dans $PSL_2(q)$, ce qui contredirait la simplicité.
Le Théorème 18 affirme que les représentations de degré 1 de B_0 sont obtenues en composant des représentations de degré 1 de $\mathbb{F}_q^{*2}$ avec l'homomorphisme $\alpha|_{B_0} : B_0 \mapsto \mathbb{F}_q^{*2}$. Remarquons maintenant que le groupe commutateur $[B_0, B_0] = \left\{aba^{-1}b^{-1} | a, b \in B_0\right\}$ est envoyé sur l'élément neutre $1 \in \mathbb{F}_q^{*2}$ par $\alpha|_{B_0}$. En effet, puisque $\alpha|_{B_0}$ est un homomorphisme, il vérifie :

$$\alpha(aba^{-1}b^{-1}) = \alpha(a)\alpha(b)\alpha(a)^{-1}\alpha(b)^{-1} = 1$$

puisque $\mathbb{F}_q^{*2}$ est un groupe abélien. Ainsi toutes les représentations de degré 1 de B_0, qui sont obtenues par composition avec $\alpha|_{B_0}$, doivent être triviales sur le commutateur de B_0. Il ne reste alors plus que les deux représentations ρ^+ et ρ^- qui soient non-triviales. Puisque π est non-triviale, au moins une des représentations ρ_+ ou ρ_- doit apparaître dans sa décomposition, ce qui implique $n \geqslant \frac{q-1}{2}$.

Références

[1] Giuliana Davidoff, Peter Sarnak, and Alain Valette, *Elementary Number Theory, Group Theory and Ramanujan Graphs*, Cambridge University Press, Cambridge, 2003.