Groupes linéaires finis permutant deux fois transitivement un ensemble de droites

Lucas Vienne

Groupes linéaires finis permutant deux fois transitivement un ensemble de droites

Lucas Vienne

Departement de mathématiques. Université d'Angers. France

Résumé

Let $n \geq 2$ be a positive integer, and G a doubly transitive subgroup of the symmetric group on $X = \{1, \ldots, n\}$. In this paper we find all linear group representations ρ of G on an euclidean vector space V which contains a set of equiangular vector lines $\mathcal{G} = \{\langle v_1 \rangle, \ldots, \langle v_n \rangle\}$ such that :

(1) V is generated by $v_1, \ldots, v_n$,

(2) for all i in X and all σ in G, $\langle \rho_\sigma(v_i) \rangle = \langle v_{\sigma(i)} \rangle$.

Then we illustrate our construction when $G = SL_d(q)$, q odd and $d \geq 2$.

Key words: groupe, permutation group, groupe de permutations, groupe doublement transitif, Paley graphs, equiangular lines

1 Introduction

Un entier $n \geq 2$ est donné ainsi qu'un groupe de permutations G sur l'ensemble $X = \{1, \ldots, n\}$. Nous dirons (par abus) qu'une représentation linéaire γ de G dans un espace vectoriel V est deux fois transitive s'il existe une gerbe de droites vectorielles $\mathcal{G} = \{\langle v_1 \rangle, \ldots, \langle v_n \rangle\}$ de V telle que :

(1) L'espace V est engendré par les vecteurs $v_1, \ldots, v_n$.

(2) Pour tout indice i dans X et tout σ dans G on a $\langle \gamma_\sigma(v_i) \rangle = \langle v_{\sigma(i)} \rangle$.

Notations

1. Lorsque le contexte est sans ambiguïté sur l'action γ d'un groupe G sur un ensemble Y, on utilise, pour σ dans G et y dans Y, la notation simplifiée $\gamma_\sigma(y) = \sigma(y)$. Par exemple, la relation (2) précédente s'écrit plus simplement

$$\sigma\langle v_i \rangle = \langle \sigma(v_i) \rangle = \langle v_{\sigma(i)} \rangle.$$

Email address: `lucas.vienne@univ-angers.fr` (Lucas Vienne).

2. Le groupe G étant fini, son image $\gamma(G)$ est contenue dans le groupe orthogonal d'un produit scalaire sur V qui sera noté $\varphi = (.|.)$ dans la suite.

Quelques remarques

Choisissons des générateurs $v_1, \ldots, v_n$ de même norme pour les droites de la gerbe $\mathcal{G}$. La double transitivité de G nous montre qu'il existe des scalaires ω, c (où $\omega \neq 0$) et des coefficients $\varepsilon_{i,j}$ ($i \neq j$, dans X), tous dans $\{-1, +1\}$ tels que

$$(R1) \qquad \forall i, j \in X, \quad (v_i|v_j) = \begin{cases} \omega & \text{si } i = j \\ \varepsilon_{i,j}.c & \text{si } i \neq j \end{cases}.$$

De plus, pour chaque élément σ dans G, il existe une liste de coefficients $\nu^\sigma = (\nu_1^\sigma, \ldots, \nu_n^\sigma)$ tous pris dans $\{-1, +1\}$ tels que

$$(R2) \qquad \forall j \in X, \quad \sigma(v_j) = \nu_j^\sigma . v_{\sigma(j)}.$$

Utilisant la relation $(R2)$, il vient pour $i \neq j$,

$$\varepsilon_{i,j}.c = (v_i|v_j) = (\sigma(v_i)|\sigma(v_j)) = (\nu_i^\sigma.v_{\sigma(i)}|\nu_j^\sigma.v_{\sigma(j)}) = \nu_i^\sigma.\nu_j^\sigma.\varepsilon_{\sigma(i),\sigma(j)}.c,$$

$$(R3) \text{ donc, si } c \neq 0, \qquad \varepsilon_{\sigma(i),\sigma(j)} = \nu_i^\sigma.\nu_j^\sigma.\varepsilon_{i,j}.$$

La double transitivité de G nous montre que les coefficients $\varepsilon_{i,j}$ sont déterminés par la connaissance de l'un d'eux et des coefficients ν_j^σ introduits en $(R2)$. Notant $\mathcal{E} = (\varepsilon_{i,j})$ la matrice dont la diagonale principale est nulle ($\varepsilon_{i,i} = 0$) et les autres coefficients sont les $\varepsilon_{i,j}$, désignant par I_n , la matrice de Gram du système de vecteurs $(v_1, \ldots, v_n)$ est donc de la forme

$$(R4) \qquad \mathrm{Gram}(v_1, \ldots, v_n) = S_{\mathcal{E}}(\omega, c) = \omega.I_n + c.\mathcal{E}.$$

Dans cet article nous déterminons quels choix des systèmes de coefficients

$$(3) \qquad \nu^\sigma = (\nu_1^\sigma, \ldots, \nu_n^\sigma),$$

satisfaisant aux relations $(R2)$ définissent une représentation linéaire de G sur V, puis nous étudions la nature, irréductible ou non, de ces représentations. Pour énoncer nos résultats, introduisons le groupe multiplicatif produit

$$\Pi^n = \{\nu = (\nu_1, \ldots, \nu_n) \mid \forall j, \ \nu_j = \pm 1\},$$

sur lequel on fait agir G ; pour tout $\nu = (\nu_1, \ldots, \nu_n)$ dans Π^n et toute permutation σ de X notons $\nu_\sigma = (\nu_{\sigma(1)}, \ldots, \nu_{\sigma(n)})$, puis posons

$$(4) \qquad \forall (\sigma, \nu) \in G \times \Pi^n, \quad \theta_\sigma(\nu) = \nu_{\sigma^{-1}}.$$

La relation immédiate $(\nu.\nu')_\sigma = \nu_\sigma.\nu'_\sigma$ nous montre que θ_σ est un morphisme. Noter que dans la définition (4), l'exposant (-1) est là pour s'assurer que θ un morphisme et non un anti-morphisme ($\theta_{\sigma.\sigma'} = \theta_\sigma.\theta_{\sigma'}$). Notons $G \ltimes \Pi^n$ le produit semi-direct de G par Π^n sous cette action.

Les théorèmes 1 et 2 donnent nos principaux résultats. Nous les ferons suivre par quelques exemples.

Théorème 1
Soit G un groupe de permutation 2-transitif sur l'ensemble $X = \{1, \dots, n\}$, $(e_1, \dots, e_n)$ une base orthonormée d'un espace vectoriel E et $\mathcal{J} : G \to G \ltimes \Pi^n$ un morphisme de groupes de la forme

$$(5) \qquad \forall \sigma \in G, \quad \mathcal{J}(\sigma) = (\sigma, \nu^\sigma)$$

1. *Il existe une unique représentation linéaire $\rho : G \to GL(E)$ dite* associée *au morphisme $\mathcal{J}$, satisfaisant aux relations $(R2)$:*

$$\forall j \in X, \quad \rho_\sigma(e_j) = \nu_j^\sigma . e_{\sigma(j)}.$$

2. *Le nombre de matrices $\mathcal{E} = (\varepsilon_{i,j})$, symétriques, à coefficients dans $\{\pm 1\}$ et de diagonale principale nulle satisfaisant aux relations $(R3)$*

$$\forall \sigma \in G, \forall i, j \in X, \quad \varepsilon_{\sigma(i),\sigma(j)} = \nu_i^\sigma . \nu_j^\sigma . \varepsilon_{i,j}$$

est 0 ou 2. Si $\mathcal{E}$ est l'une d'elles l'autre est $-\mathcal{E}$.
3. *Si la représentation $\rho : G \to GL(E)$ n'est pas irréductible, alors :*
   a. Il existe une matrice $\mathcal{E}$ satisfaisant aux conditions $(R3)$.
   b. Cette matrice possède exactement deux valeurs propres λ_1 et λ_2.
   c. Les sous-espaces propres E_1 et E_2 associés sont des sous-G-modules irréductibles de E sur lesquels le groupe G induit des représentations doublement transitives.

Théorème 2
Soit G un groupe de permutation de l'ensemble $X = \{1, \dots, n\}$, et une représentation linéaire $\gamma : G \to GL(V)$ doublement transitive de (G, X) sur un espace vectoriel euclidien V de dimension finie.
Il existe un morphisme $\mathcal{J} : G \to G \ltimes \Pi^n$ de la forme (5) tel que :
1. *Si $\dim(V) = n$, la représentation γ est semblable à la représentation ρ associée au morphisme $\mathcal{J}$.*
2. *Si $\dim(V) < n$, la représentation γ est semblable à l'une des deux composantes irréductibles de ρ décrites dans la partie 3 du théorème 1.*

Nous appliquerons ensuite ces théorèmes aux sous groupes G de $GL_d(q)$ contenant $SL_d(q)$, agissant deux fois transitivement sur l'espace projectif $\mathbb{P}_{d-1}(q)$.

2 Preuves

2.1 Résultats préliminaires

Proposition 1
Soit E un espace euclidien réel muni d'une base orthonormée $(e) = (e_1, \dots, e_n)$, S une matrice symétrique réelle de type $n \times n$, et pour tout couple de scalaires (ω, c), posons $S(\omega, c) = \omega . I_n + c.S$. Notons $\psi_{k,c}$ et $\widetilde{\psi}_{k,c}$ la forme bilinéaire et l'endomorphisme symétrique associés à la matrice $S(\omega, c)$ dans la base (e).

On suppose $c \neq 0$.
1.*a. L'application affine $\alpha : \lambda \to \omega + c.\lambda$ établit une bijection entre les valeurs propres de $S = S(0,1)$ et celles de $S(\omega, c)$.*
1.*b. Les sous-espaces propres de $\widetilde{\psi}_{k,c}$ sont indépendants du couple (ω, c). Plus précisément, si $E_{k,c}(\mu)$ désigne le sous-espace propre de $\widetilde{\psi}_{\omega,c}$ associé à la valeur propre μ on a :*

$$E_{\omega,c}(\omega + c.\lambda) = E_{0,1}(\lambda)$$

2. *Soit $E = E_1 \oplus \ldots \oplus E_s$ la décomposition de E en somme des sous-espaces propres de S associés aux valeurs propres $\lambda_1, \ldots, \lambda_s$ qu'on suppose rangées en fonction de leurs multiplicités croissantes $m_1 \leq \ldots \leq m_s$. Le noyau de $\widetilde{\psi}_{\omega,c}$ est (0) ou l'un des E_i $(1 \leq i \leq s)$.*
3. *Le rang de $\widetilde{\psi}_{\omega,c}$ est toujours supérieur ou égal à $n - m_s$.*

Démonstration. Simple, on la laisse au lecteur. □

On se place dans la situation décrite dans l'introduction : le groupe G opère deux fois transitivement sur l'ensemble $X = \{1, \ldots, n\}$. La représentation linéaire $\gamma : G \to GL(V)$ est doublement transitive dans un espace vectoriel euclidien V et il existe des générateurs $v_1, \ldots, v_n$ de V et des scalaires ν_i^σ (pour $(\sigma, i) \in G \times X$) tels que les relations $(R2)$ soient satisfaites. Le lemme suivant nous informe sur les sous-modules de V.

Lemme 1
Supposons que U est un sous-G-module de V distinct de V.
1. *Il existe un projecteur p_U de V sur U qui commute aux opérations de G :*

$$\forall \sigma \in G, \quad p \circ \sigma = \sigma \circ p.$$

2. *Notant, pour tout indice $i \in X$, $u_i = p(v_i)$, alors*

$$\forall \sigma \in G, \ \sigma(u_i) = \nu_i^\sigma u_{\sigma(i)}.$$

3. *Il existe une matrice $\mathcal{E} = (\varepsilon_{i,j})$ de diagonale principale nulle, dont les coefficients, pour $i \neq j$, sont dans $\{-1, +1\}$ et satisfont aux relations $(R3)$*

$$\forall \sigma \in G, \forall i, j \in X, \quad \varepsilon_{\sigma(i),\sigma(j)} = \nu_i^\sigma . \nu_j^\sigma . \varepsilon_{i,j}$$

4. *Pour des constantes non nulles convenablement choisies ω_U et c_U on a*

$$\mathrm{Gram}(u_1, \ldots, u_n) = S_{\mathcal{E}}(\omega_U, c_U) = \omega_U I_n + c_U \mathcal{E}$$

Démonstration. La première affirmation vient d'un résultat classique : tout sous-G-module U de V admet un supplémentaire W qui est aussi un G-module. Alors les projecteurs p_U et p_W associés à la décomposition $V = U \oplus W$ commutent aux opérations de G. La deuxième affirmation en découle directement puisque pour tout indice $i \in X$, l'égalité $\sigma(v_i) = \nu_i^\sigma v_{\sigma(i)}$ conduit à

$$\sigma(u_i) = \sigma \circ p(v_i) = p \circ \sigma(v_i) = p(\nu_i^\sigma v_{\sigma(i)}) = \nu_i^\sigma p(v_{\sigma(i)}) = \nu_i^\sigma u_{\sigma(i)}.$$

On en déduit que les vecteurs u_i sont tous de même norme et de la double transitivité de G sur X, on déduit l'existence des constantes ω_U et c_U telles que le système de vecteurs $(u_1, \ldots, u_n)$ satisfasse aux relations $(R1)$. Mais le coefficient ω_U est non nul puisque c'est le carré des vecteurs non nuls u_i, et le coefficient c_U est aussi non nul puisque le rang de la matrice $\mathrm{Gram}(u_1,\ldots,u_n)$ étant inférieur à la dimension du module U, il est strictement inférieur à n. Finalement la matrice $\mathcal{E}=(\varepsilon_{i,j})$ satisfait aux relations $(R3)$, si bien que $\mathrm{Gram}_\psi(u_1,\ldots,u_n)=S_\mathcal{E}(\omega_U,c_U)$ comme voulu. □

2.2 Preuve du théorème 1

On adopte les hypothèses et notations de ce théorème .
1. Pour chaque élément σ de G la relation $(R2)$:

$$\forall j\in X,\quad \rho_\sigma(e_j)=\nu_j^\sigma.e_{\sigma(j)}$$

définit une fonction ρ_σ envoyant la base orthonormée $(e)=(e_1,\ldots,e_n)$ sur une base orthonormée de E, qui s'étend donc en une isométrie linéaire de E. Ceci montre bien sûr l'unicité de ρ, mais il nous reste à vérifier que ρ est un morphisme. Or, comme $\mathcal{J}$ est un morphisme on a

$$\mathcal{J}(\sigma.\delta)=\sigma\delta.\nu^{\sigma\delta}=\mathcal{J}(\sigma).\mathcal{J}(\delta)=\sigma\nu^\sigma.\delta\nu^\delta=\sigma\delta.\nu_\delta^\sigma\nu^\delta,$$

donc $$\nu^{\sigma\delta}=\nu_\delta^\sigma\nu^\delta.$$

Par ailleurs : $\rho_{\sigma\delta}(e_i)=\nu_i^{\sigma.\delta}e_{\sigma.\delta(i)}$ et $\rho_\sigma.\rho_\delta(e_i)=\rho_\sigma(\nu_i^\delta.e_{\delta(i)})=\nu_i^\delta.\nu_{\delta(i)}^\sigma e_{\sigma.\delta(i)}$,

D'où l'égalité recherchée, $\rho_{\sigma\delta}(e_i)=\rho_\sigma.\rho_\delta(e_i)$.

2. Le groupe G opérant deux fois transitivement sur l'ensemble X, il est clair, d'après la relation $(R3)$, que la connaissance d'un des coefficients $\varepsilon_{i,j}$ détermine tous les autres. Par ailleurs si $\mathcal{E}$ est une matrice satisfaisant aux relations $(R3)$ il en est bien sûr de même de $-\mathcal{E}$, ce qui prouve l'assertion 2.

3.a. Pour tout sous-G-module U de E, distinct de E, le lemme 1 nous montre qu'il existe une matrice $\mathcal{E}$ satisfaisant aux relations $(R3)$, ce qui prouve a. Dans la suite, si $(u_1,\ldots,u_n)$ est l'image de la base orthonormée $(e_1,\ldots,e_n)$ par la projection orthogonale $p_U:E\to U$ sa matrice de Gram sera simplement notée $\mathrm{Gram}_U=\mathrm{Gram}(u_1,\ldots,u_n)$.
Toujours d'après le lemme 1, la matrice Gram_U est de la forme

$$\mathrm{Gram}_U=S(\omega,c)=\omega I_n+c.\mathcal{E}$$

pour des constantes non nulles ω et c. L'endomorphisme symétrique $\widetilde{\psi}_{\omega,c}$ de matrice $S(\omega,c)$ dans la base $(e)=(e_1,\ldots,e_n)$ se diagonalise sur E et ses sous-espaces propres sont clairement des sous-G-modules de E, or d'après la proposition 1, ce sont les mêmes que ceux de la matrice $\mathcal{E}=S(0,1)$. Soient $\lambda_1,\ldots,\lambda_s$ les valeurs propres de $\mathcal{E}$, rangées dans l'ordre de leur multiplicités croissantes $m_1\le\cdots\le m_s$, et $E_1,\ldots,E_s$ les sous-espaces propres associés. Remarquons que $\mathcal{E}$ n'étant pas une homothétie, on a $s\ge 2$. Comme les E_u sont des sous-G-modules de E, le projecteur orthogonal p_u de E sur E_u $(1\le u\le s)$ commute avec l'action de G donc, toujours d'après le lemme 1, la matrice Gram_{E_u} est de la forme $\mathrm{Gram}(u_1,\ldots,u_n)=S_\mathcal{E}(\omega_u,c_u)$ pour des constantes non nulles ω_u et c_u. D'après la proposition 1, le noyau de $S_\mathcal{E}(\omega_u,c_u)$ est l'un des espaces propres E_t $(1 \leq t \leq s)$ de $\mathcal{E}$ et son rang est supérieur ou égal à $n - m_s$. Or ce rang est aussi inférieur ou égal à la dimension m_u de E_u. Donc

$$n - m_s \leq m_u \quad \text{soit} \quad n \leq m_u + m_s.$$

Mais comme $s \geq 2$ on peut choisir $u \neq s$ et il vient alors

$$n \leq m_u + m_s \leq n,$$

donc $n = m_u + m_s$, ce qui implique $s = 2, u = 1$, et prouve b.

Le module E est donc la somme directe orthogonale des sous-espaces propres E_1 et E_2 de la matrice $\mathcal{E}$ de dimensions respectives m_1 et m_2 (où $m_1 \leq m_2$) qui sont des sous-G-modules de E. Pour achever la démonstration du théorème 1, il nous faut montrer que les sous-modules E_1 et E_2 sont irréductibles.
Soit W un sous-module irréductible de E. D'après le lemme 1, sa matrice de Gram est de la forme

$$\mathrm{Gram}_W = S(\omega_W, c_W) = \omega_W I_n + c_W \mathcal{E},$$

et, n'étant pas de rang n, elle est liée à G_{E_1} ou G_{E_2}. Son rang $m = \dim(W)$ est donc égal à m_1 ou m_2, ce qui prouve déjà que E_1 est irréductible. Raisonnant par l'absurde, si E_2 ne l'est pas, il se décompose en somme orthogonale de sous-modules $E_2 = E_2^1 \oplus \cdots \oplus E_2^k$ qui sont tous de dimension m_1 et admettent des matrices de Gram de rang m_1, donc liées à la matrice Gram_{E_1} de E_1. L'espace E étant somme orthogonale de E_1 et des E_2^j $(1 \leq j \leq k)$, il est facile de vérifier que sa matrice de Gram, qui n'est autre que l'identité, est la somme des matrices de Gram de chacun des termes de la somme directe. Or cette somme bien sûr une matrice liée à Gram_{E_1} qui ne peut pas être l'identité. Ceci prouve, par l'absurde, que E_2 n'est pas réductible et achève la démonstration du théorème 1. $\square$

2.3 Preuve du théorème 2

D'après l'introduction, on peut choisir des vecteurs $v_1, \ldots, v_n$ dans V tels que :
 * $V = \langle v_1, \ldots, v_n \rangle$.
 * Le groupe G opère 2-transitivement la gerbe de droites $\mathcal{G} = \{\langle v_1 \rangle, \ldots, \langle v_n \rangle\}$.
 * Les relations $(R2)$, $(R3)$ et $(R4)$ sont satisfaites, pour des constantes ω, c et une matrice $\mathcal{E} = (\varepsilon_{i,j})$ convenablement choisies.

Reprenant un raisonnement fait plus haut on voit que pour tout indice $i \in X$,

$$\gamma_{\sigma\delta}(v_i) = \nu_i^{\sigma.\delta} v_{\sigma.\delta(i)} \qquad \text{et} \qquad \gamma_\sigma.\gamma_\delta(v_i) = \gamma_\sigma(\nu_i^\delta.v_{\delta(i)}) = \nu_i^\delta.\nu_{\delta(i)}^\sigma v_{\sigma.\delta(i)},$$

d'où l'on déduit que $\nu^{\sigma\delta} = \nu_\delta^\sigma \nu^\delta$, puis que l'application $\mathcal{J} : \sigma \to \sigma.\nu^\sigma$ est un morphisme de G dans le produit semi-direct $G \ltimes \Pi^n$ puisque

$$\mathcal{J}(\sigma.\delta) = \sigma\delta.\nu^{\sigma\delta} \qquad \text{et} \qquad \mathcal{J}(\sigma).\mathcal{J}(\delta) = \sigma\nu^\sigma.\delta\nu^\delta = \sigma\delta.\nu_\delta^\sigma\nu^\delta.$$

Soit $\rho : G \to GL(E)$ la représentation associée au morphisme $\mathcal{J}$ (cf. thm 1). L'espace E est donc euclidien, muni d'une base orthonormée $e_1, \ldots, e_n$ telle que la représentation ρ satisfasse aux relations $(R2)$:

$$\forall j \in X, \quad \rho_\sigma(e_j) = \nu_j^\sigma.e_{\rho_\sigma(j)}.$$

Comme la représentation γ satisfait aux mêmes relations, l'application $\pi : e_j \to v_j$ (pour $j \in X$) se prolonge en un morphisme du G-module E sur le G-module V.
1. Si $\dim V = n$, π est un isomorphisme.
2. Sinon le noyau de π est un sous-module de E qui ne peut qu'être E ou l'un des deux sous-modules E_1 et E_2 de E décrits dans le théorème 1. Son image est donc aussi soit nulle, soit isomorphe à l'un de ces deux modules. $\square$

3 Quelques exemples

Exemple 1

Voici un exemple de représentation linéaire $\gamma : G \to GL(E)$, associée à un morphisme $\mathcal{J} : G \to G \ltimes \Pi^n$, qui est doublement transitive et irréductible.
Nous utiliserons le résultat classique suivant (voir par exemple [1]) :

Lemme 2
Soit G un groupe de permutation de $Y = \{1, \ldots, m\}$ et ρ la représentation linéaire de G sur $\mathbb{R}^m$ associée qui, pour une base orthonormée $(e_1, \ldots, e_m)$ s'écrit :

$$\forall \sigma \in G, \forall i \in Y, \quad \rho_\sigma(e_i) = e_{\sigma(i)}.$$

Notons χ le caractère de la représentation ρ, $\chi_1, \ldots, \chi_k$, les caractères irréductibles du groupe G, et pour pour chaque indice j ($1 \leq j \leq k$), soit $\mu_j = (\chi|\chi_j)$ la multiplicité du caractère χ_j dans la représentation ρ.
Alors la somme $\sum_j \mu_j^2$ est égale au nombre d'orbites de G dans son action naturelle sur $Y \times Y$.

Appliquons ce résultat dans la situation suivante :
Soit $\mathbb{F}_3$ le corps à trois éléments, V l'espace vectoriel $\mathbb{F}_3^3$, et G le groupe $SL(V)$ agissant naturellement sur l'ensemble $Y = V^*$ des 26 vecteurs non nuls de V.
Il est facile de vérifier que le groupe G possède trois orbites dans son action naturelle sur $Y \times Y$ qui sont :
* L'ensemble des couples de vecteurs (v, v) pour $v \in V^*$.
* L'ensemble des couples de vecteurs $(v, -v)$ pour $v \in V^*$.
* L'ensemble des couples de vecteurs (v, w) pour $v, w \in V^*$, non colinéaires.
Choisissons un système de représentants $v_1, \ldots v_{13}$ des droites vectorielles de V et notons $\overline{v}_1, \ldots \overline{v}_{13}$ leurs opposés. La représentation linéaire $\gamma : G \to GL(\mathbb{R}^{26})$ associée à l'action de naturelle de G sur $Y = V^* = \{v_1, \ldots v_{13}, \overline{v}_1, \ldots \overline{v}_{13}\}$ permute la base Y de $\mathbb{R}^{26}$. D'après le lemme 2, cette représentation γ se décompose en une somme de représentations irréductibles γ_j intervenant avec des multiplicités μ_j telles que $3 = \sum_j \mu_j^2$. On en déduit immédiatement que γ est une somme de trois représentations irréductibles non semblables. Or il n'est pas difficile de les décrire car la représentation γ admet clairement comme sous-représentation l'espace U engendré par les vecteurs de la forme

$v_i + \overline{v}_i$, dans lequel la droite vectorielle $\sum_i v_i + \sum_i \overline{v}_i$ $(1 \leq i \leq 13)$ est elle même un sous espace stable par G. Il s'ensuit que l'orthogonal E de U dans V est lui-même un sous espace stable par G et irréductible, puisque V est somme d'exactement trois sous G-modules irréductibles. Regardons comment G agit sur E. Comme $E = U^{\perp}$, il admet pour base l'ensemble des 13 vecteurs de la forme $e_i = v_i - \overline{v}_i$, et l'action de G sur E est donnée par des relations

$$\forall \sigma \in G, \quad \sigma(e_i) = \sigma(v_i - \overline{v}_i) = \nu_i^{\sigma}(v_{\sigma(i)} - \overline{v}_{\sigma(i)}) = \nu_i^{\sigma}.e_{\sigma(i)},$$

où les coefficients ν_i^{σ} valent tous ± 1. Donc la représentation de $G = SL_3(3)$ sur E donnée par ces relations est irréductible et associée au morphisme $\mathcal{J} : G \to G \ltimes \Pi^n$ donné par $\mathcal{J}(\sigma) = \sigma.\nu^{\sigma}$.

Exemple 2

Généralisons maintenant l'idée utilisée dans l'exemple 1.

Soit $\mathbb{F}_q$ un corps fini à q éléments, de caractéristique impaire, C l'ensemble de ses carrés non nuls et $\overline{C}$ l'ensemble de ses non-carrés. Choisissons un entier $d \geq 2$, notons V l'espace vectoriel F_q^d, n le nombre de droites vectorielles de V, chacune d'elle étant engendrée par un vecteur v_i $(i \in X = \{1, \ldots, n\})$. Soit enfin G un sous-groupe de $GL(V)$ contenant le groupe spécial linéaire $SL(V)$. L'action naturelle de $SL(V)$ sur l'espace projectif $\mathbb{P}(V)$ étant doublement transitive, il en de même de celle de G. Elle se transmet aussi à X en notant $\sigma(i)$, pour tout indice i dans X et tout σ dans G, l'unique indice tel que

$$\sigma(\langle v_i \rangle) = \langle v_{\sigma(i)} \rangle.$$

Plus précisément, il existe un scalaire non nul λ_i tel que

$$\sigma(v_i) = \lambda_i.v_{\sigma(i)}.$$

On définit alors une représentation γ de G comme groupe de permutations de l'ensemble $Y = \{v_1, -v_1, \ldots, v_n, -v_n\}$ en posant

$$(6) \qquad \begin{aligned} &* \ \gamma_\sigma(v_i) = \nu_i^{\sigma}.v_{\sigma(i)} \qquad \text{ou} \qquad \nu_i^{\sigma} = \begin{cases} 1 & \text{si} \quad \lambda_i \in C \\ -1 & \text{si} \quad \lambda_i \in \overline{C} \end{cases}, \\ &* \ \gamma_\sigma(-v_i) = -\gamma_\sigma(v_i). \end{aligned}$$

Pour éviter toute confusion posons maintenant pour chaque indice i, $\overline{v_i} = -v_i$, notons encore γ la représentation linéaire du groupe G sur l'espace $\mathbb{R}^{2n}$ associée à l'action du groupe G sur Y et soit χ son caractère. D'après le lemme 2, le nombre ω d'orbites de G dans son action naturelle sur $Y \times Y$ vaut

$$\omega = \sum_j \mu_j^2, \quad \text{où} \quad \mu_j = (\chi | \chi_j)$$

représente la multiplicité du caractère irréductible χ_j dans la représentation γ. Regardons comment G agit sur $\mathbb{R}^{2n}$.
L'égalité $\{\gamma_\sigma(v_i), \gamma_\sigma(\overline{v}_i)\} = \{v_{\sigma(i)}, \overline{v}_{\sigma(i)}\}$ valable pour tout σ dans G nous montre que le sous-espace U engendré par les vecteurs $u_i = v_i + \overline{v}_i$ $\ (i \in X)$

est stable par l'action de G, ainsi que la droite vectorielle D engendrée par le vecteur $\sum_i u_i$, et son orthogonal dans U, $D^{\perp} \cap U$. L'orthogonal E de U dans $\mathbb{R}^{2n}$ est lui-même stable par G, engendré par les n vecteurs $e_i = v_i - \overline{v}_i$, et l'action de G sur E est donnée par les relations

$$(7) \qquad \forall \sigma \in G, \quad \gamma_\sigma(e_i) = \gamma_\sigma(v_i - \overline{v}_i) = \nu_i^\sigma(v_{\sigma(i)} - \overline{v}_{\sigma(i)}) = \nu_i^\sigma.e_{\sigma(i)}$$

Donc la représentation de G sur E donnée par ces relations est associée au morphisme $\mathcal{J} : G \to G \ltimes \Pi^n$ donné par $\mathcal{J}(\sigma) = \sigma.\nu^\sigma$. Le théorème suivant décrit, suivant les différentes situations, la décomposition de γ en somme de représentations irréductibles.

Théorème 3
Sous les hypothèses précédentes, soit $\gamma : G \to GL(E)$ la représentation de G donnée par les relations (7)

$$\forall i \in X, \forall \sigma \in G, \quad \gamma_\sigma(e_i) = \nu_i^\sigma.e_{\sigma(i)}$$

− *Si $d \geq 3$ la représentation γ est irréductible.*
− *Supposons $d = 2$ et notons $GL_2^+(q)$ le sous-groupe de $GL_2(q)$ formé des automorphismes dont le déterminant est un carré dans F_q.*
  (*a*) *Si $G \not\subset GL_2^+(q)$, la représentation γ est irréductible.*
  (*b*) *Si $G \subset GL_2^+(q)$, la représentation γ est réductible.*
Dans le cas (b) le G-module E se décompose en somme directe $E = E_1 \oplus E_2$ de deux sous-modules irréductibles de même dimension, échangés par l'action sur E du groupe $GL_2(q)$. De plus,
∗ *si $q \not\equiv 1 \mod 4$, le module E reste irréductible sur $\mathbb{R}$,*
∗ *si $q \equiv 1 \mod 4$, la décomposition à lieu sur $\mathbb{R}$ et les représentations de G sur E_1 et E_2 sont associées aux graphes de Paley $\mathcal{P}(q)$ (voir* [5]*).*

Démonstration. Sous les hypothèses générales du théorème 3, l'action de G sur X étant doublement transitive, le théorème 1 nous dit que la représentation γ de G sur E est soit irréductible sur $\mathbb{R}$, soit somme directe de deux représentations irréductibles, non semblables. Mais d'après le lemme 2, dans le premier cas le groupe G possède trois orbites sur $Y \times Y$ tandis que dans le second il en possède quatre. Or l'action de G sur $Y \times Y$ possède au moins trois parties stables qui sont :
* L'ensemble Δ des couples de vecteurs (v, v) pour $v \in Y$.
* L'ensemble Δ' des couples de vecteurs $(v, -v)$ pour $v \in Y$.
* L'ensemble ∇ des couples de vecteurs (v, w) pour $v, w \in Y$, non colinéaires.
De plus l'action γ de G sur Y est nécessairement transitive sinon Δ et Δ' seraient formées d'au moins deux orbites, si bien que l'action $\gamma \times \gamma$ de G sur $Y \times Y$ aurait au moins cinq orbites, ce qui est impossible. Donc seule la partie ∇ peut être formée d'une ou deux orbites sous l'action $\gamma \times \gamma$ de G.
Discutons suivant les valeurs de la dimension d de l'espace V.

− *Supposons $d \geq 3$.*

L'action naturelle du groupe $SL_d(q)$ sur l'ensemble des couples (v, w) de vecteurs non liés dans V est transitive, tout comme celle de G, donc l'action $\gamma \times \gamma$ de G sur ∇ est transitive. Le lemme 2 nous montre que dans ce cas la représentation γ de G sur E est irréductible.

– *Supposons* $d = 2$.

Lemme 3
Le nombre θ d'orbites du groupe G, agissant sur l'ensemble ∇ des couples de vecteurs (v, w) pour v, w dans Y non colinéaires est
* $\theta = 2$, *si* $G \subset GL_2^+(q)$,
* $\theta = 1$, *si* $G \not\subset GL_2^+(q)$.

Démonstration. On sait déjà que G possède une ou deux orbites dans son action $\gamma \times \gamma$ sur ∇. De plus comme G opère transitivement sur les couples de droites $(\langle v_i \rangle, \langle v_j \rangle)$ distinctes, il opère transitivement sur ∇ si et seulement si l'orbite de (v_i, v_j) sous l'action de G par $\gamma \times \gamma$ contient $(v_i, -v_j)$, $(-v_i, v_j)$ et $(-v_i, -v_j)$, ce qui revient à dire que G contient un élément σ tel que $\sigma(v_i) = v_i$ et $\sigma(v_j) = \lambda.v_j$ où le scalaire λ n'est pas un carré (d'après la définition (5) de l'action γ). Mais comme G contient le groupe $SL_2(q)$, ceci signifie aussi que G contient un élément dont le déterminant n'est pas un carré, ce qui prouve le lemme. $\square$

Pour achever la preuve du théorème 3, on se place maintenant dans le cas (b) de ce théorème pour lequel $d = 2$ et $G \subset GL_2^+(q)$.
D'après le lemme 2, l'action γ de G sur E est réductible, et plus précisément E est somme de deux sous-G-modules irréductibles E_1 et E_2. Mais, toujours, d'après le lemme 2, l'action $\gamma \times \gamma$ du groupe linéaire $GL_2(q)$ étant transitive sur l'ensemble ∇, la représentation de $GL_2(q)$ sur E est irréductible. Or le sous-groupe G est invariant dans $GL_2(q)$ puisqu'il contient $SL_2(q)$, donc $GL_2(q)$ permute les deux sous-espaces E_1 et E_2. Distinguons deux cas :

Premier cas : $q \not\equiv 1 \mod 4$.
L'automorphisme σ qui envoie la base (v_1, v_2) de V sur $(v_2, -v_1)$ est dans $SL_2(q)$ donc dans G, et comme -1 n'est pas un carré dans $\mathbb{F}_q$ les relations (6) et (7) nous conduisent à $\gamma_\sigma(v_1) = v_2$, $\gamma_\sigma(v_2) = -v_1$ puis

$$\gamma_\sigma(e_1) = e_2 = \nu_1^\sigma e_2 \quad \text{et} \quad \gamma_\sigma(e_2) = -e_1 = \nu_2^\sigma.$$

S'il existait une matrice $\mathcal{E} = (\varepsilon_{i,j})$ satisfaisant aux relations $(R4)$ du théorème 1, on devrait avoir

$$\varepsilon_{\sigma(1),\sigma(2)} = \varepsilon_{2,1} = \varepsilon_{1,2} = \nu_1^\sigma \nu_2^\sigma.\varepsilon_{1,2} = -\varepsilon_{1,2},$$

ce qui est faux. Donc $\mathcal{E}$ n'existe pas et d'après le théorème 1 la représentation γ de G sur E est irréductible sur $\mathbb{R}$. Sa décomposition en somme directe $E = E_1 \oplus E_2$ a donc lieu sur le corps $\mathbb{C}$ des complexes.

Deuxième cas : $q \equiv 1 \mod 4$.
La décomposition $E = E_1 \oplus E_2$ a maintenant lieu sur le corps des réels et les représentations de G sur E_1 et E_2 sont associées à des familles équiangulaires de droites liées aux graphes de Paley $\mathcal{P}(q)$ (voir [5] pour une construction de ces familles de droites). $\square$

4 Bibliographie

Articles

[1] Dominique de Caen, *Large equiangular sets of lines in Euclidean spaces.* The electronic journal of comninatorics. November 9, 2000.

[2] L. Nguyen Van The, *On a problem of Specker about Euclidean representations of finite graphs.*, (2008)
http ://arxiv.org/abs/0810.2359

[3] Aidan Roy , *Minimal Euclidean representations of graphs.* (2008)
http ://arxiv.org/abs/0812.3707

[4] L. Vienne, *Représentations linéaires des graphes finis.* (2009)
http ://arxiv.org/abs/0902.1874.

[5] L. Vienne, *Groupes d'isométries permutant doublement transitivement un ensemble de droites vectorielles (1).* (2009)
http ://fr.arxiv.org/abs/0903.0912.

[6] Brouwer, A. E. ; Cohen, A. M. ; and Neumaier, A. *Conference Matrices and Paley Graphs.* In Distance Regular Graphs. New York : Springer-Verlag.

Livres

[7] Godsil, Chris, and Royle, *Algebraic Graph Theory.* New York : Springer. (2001)

[8] Gérard Rauch, *Les groupes finis et leurs représentations.* Ellipses. (2001)

[9] Norman Biggs. *Finite groups of automorphisms.* London Mathematical Society. (1970)

[10] Norman Biggs. *Algebraic Graph Theory.* Cambridge University Press, (1993)

[11] P. J. Cameron and J.H.Van Lint. *Designs, graphs,codes and their links, vol 22 of London Mathematical Society Student Texts,* Cambridge University Press, Cambridge, (1991).