



**HAL**  
open science

## Groupes linéaires finis permutant deux fois transitivement un ensemble de droites

Lucas Vienne

► **To cite this version:**

Lucas Vienne. Groupes linéaires finis permutant deux fois transitivement un ensemble de droites. 2009. hal-00422673v1

**HAL Id: hal-00422673**

**<https://hal.science/hal-00422673v1>**

Preprint submitted on 8 Oct 2009 (v1), last revised 13 Dec 2009 (v2)

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Groupes linéaires finis permutant deux fois transitivement un ensemble de droites

Lucas Vienne

*Departement de mathématiques. Université d'Angers. France*

---

## Résumé

Un entier  $n$  étant donné ainsi qu'un groupe  $G$  de permutation de  $X = \{1, \dots, n\}$ , dans cet article, on détermine les représentations linéaires  $\rho$  de  $G$  permutant doublement transitivement un système équiangulaire de  $n$  droites vectorielles  $\langle v_1 \rangle, \dots, \langle v_n \rangle$  dans un espace euclidien  $V$  tout en respectant l'action de  $G$  sur  $X$ , c'est-à-dire que pour tout indice  $i$  entre 1 et  $n$  et tout  $\sigma$  dans  $G$ ,

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

On applique ensuite ces résultats aux groupes  $SL_d(q)$ , pour  $q$  impair et  $d \geq 2$ .

*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  $X = \{1, \dots, n\}$ . Nous dirons (abusivement) qu'une représentation linéaire  $\rho$  de  $G$  dans un espace vectoriel  $V$  est une représentation deux fois transitive de  $(G, X)$  sur  $V$  s'il existe une gerbe de droites vectorielles  $\mathcal{G} = \{\langle v_1 \rangle, \dots, \langle v_n \rangle\}$  de  $V$  telle que :

- (1) L'espace  $V$  est engendré par les vecteurs  $v_1, \dots, v_n$ .
- (2) La gerbe  $\mathcal{G}$  est invariante sous l'action de  $G$  et, la restriction à  $\mathcal{G}$  de cette action est doublement transitive.
- (3) Pour tout indice  $i$  dans  $X$  et tout  $\sigma$  dans  $G$  on a  $\langle \rho_\sigma(v_i) \rangle = \langle v_{\sigma(i)} \rangle$ .

### *Notations et remarques*

1. Lorsque le contexte est sans ambiguïté sur l'action  $\gamma$  d'un groupe  $G$  sur

---

*Email address:* [lucas.vienne@univ-angers.fr](mailto:lucas.vienne@univ-angers.fr) (Lucas Vienne).

un ensemble  $\Omega$ , on utilise, pour  $\sigma$  dans  $G$  et  $\omega$  dans  $\Omega$ , la notation simplifiée  $\gamma_\sigma(\omega) = \sigma(\omega)$ . Par exemple, la relation (3) précédente s'écrit plus simplement

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

2. Le groupe  $G$  étant fini, son image  $\rho(G)$  est contenue dans le groupe orthogonal d'un produit scalaire  $\psi$  sur  $V$  convenablement choisi qu'on notera plus simplement  $\psi = (\ | )$  dans la suite.

3. Si nous choisissons pour les droites de la gerbe  $\mathcal{G}$ , des générateurs  $v_1, \dots, v_n$  de même norme, alors pour tout élément  $\sigma$  du groupe  $G$  il existe une liste de coefficients  $\nu^\sigma = (\nu_1^\sigma, \dots, \nu_n^\sigma)$  tous pris dans  $\{\pm 1\}$  tels que

$$(4) \quad \forall j \in X, \quad \sigma(v_j) = \nu_j^\sigma \cdot v_{\sigma(j)}.$$

Par ailleurs la double transitivité du groupe  $G$  sur la gerbe  $\mathcal{G}$  nous montre qu'il existe des nombres  $k, c$  et des coefficients  $\varepsilon_{i,j}$  ( $i \neq j$ , pris dans  $X$ ) tous dans  $\{\pm 1\}$  tels que

$$(5) \quad \forall i, j \in X, \quad (v_i | v_j) = \begin{cases} k & \text{si } i = j \\ \varepsilon_{i,j} \cdot c & \text{si } i \neq j \end{cases}.$$

Utilisant la relation (4), il vient pour  $i \neq j$ ,

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

$$(6) \quad \text{donc, si } c \neq 0, \quad \varepsilon_{\sigma(i), \sigma(j)} = \nu_i^\sigma \cdot \nu_j^\sigma \cdot \varepsilon_{i,j}.$$

La double transitivité de  $G$  agissant sur la gerbe  $\mathcal{G}$  nous montre aussi que tous les coefficients  $\varepsilon_{i,j}$  sont déterminés par la connaissance de l'un d'eux et des coefficients  $\nu_j^\sigma$  introduits dans la relation (4) qui retiendront donc particulièrement notre attention.

On note  $S_{\mathcal{E}}(k, c) = k \cdot I_n + c \cdot \mathcal{E}$  la matrice de Gram du système  $(v_1, \dots, v_n)$ , où  $I_n$  est la matrice identique et  $\mathcal{E}$  la matrice des  $(\varepsilon_{i,j})$  dont la diagonale principale est nulle (pour tout  $j \in X$ ,  $\varepsilon_{j,j} = 0$ ).

Dans cet article nous déterminons quels choix des systèmes de coefficients  $\nu^\sigma = (\nu_1^\sigma, \dots, \nu_n^\sigma)$  satisfaisant aux relations (4) définissent une représentation linéaire de  $G$  sur  $V$ , puis nous étudions la nature, irréductible ou non, de ces représentations. Pour énoncer clairement nos résultats introduisons le groupe multiplicatif produit

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

sur lequel on fait agir  $G$ ; pour tout  $\nu = (\nu_1, \dots, \nu_n)$  dans  $\Pi^n$  et toute permutation  $\sigma$  de  $X$  on note  $\nu_\sigma = (\nu_{\sigma(1)}, \dots, \nu_{\sigma(n)})$ , puis on pose

$$(7) \quad \forall (\sigma, \nu) \in G \times \Pi^n, \quad \varphi_\sigma(\nu) = \nu_{\sigma^{-1}}.$$

La relation immédiate  $(\nu \cdot \nu')_\sigma = \nu_\sigma \cdot \nu'_\sigma$  nous montre que  $\varphi_\sigma$  est un morphisme. Noter que dans la définition (7), l'exposant  $(-1)$  est là pour s'assurer que  $\varphi$  un morphisme et non un anti-morphisme ( $\varphi_{\sigma \cdot \sigma'} = \varphi_\sigma \cdot \varphi_{\sigma'}$ ). Notons  $G \ltimes \Pi^n$  le produit semi-direct de  $G$  par  $\Pi^n$  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  $\mathcal{J} : G \rightarrow G \times \Pi^n$  un morphisme de groupes de la forme

$$(8) \quad \forall \sigma \in G, \quad \mathcal{J}(\sigma) = (\sigma, \nu^\sigma)$$

1. Il existe une unique représentation linéaire  $\rho : G \rightarrow GL(E)$  dite associée au morphisme  $\mathcal{J}$ , satisfaisant aux relations (4) :

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

2.a. Le nombre de matrices  $\mathcal{E} = (\varepsilon_{i,j})$ , symétriques, à coefficients dans  $\{\pm 1\}$  et de diagonale principale nulle satisfaisant aux relations (6)

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

est 0 ou 2. Si  $\mathcal{E}$  est l'une d'elles l'autre est  $-\mathcal{E}$ .

2.b. Si ce nombre est 0 la représentation  $\rho$  est irréductible sur  $\mathbb{R}$ . Sinon la matrice  $\mathcal{E}$  possède exactement deux sous-espaces propres  $E_1$  et  $E_2$ . L'espace  $E$  est somme directe orthogonale de  $E_1$  et  $E_2$  sur lesquels le groupe  $G$  induit, par restriction, des représentations  $\rho_1$  et  $\rho_2$  doublement transitives et irréductibles.

### **Théorème 2**

Soit  $G$  un groupe de permutation de  $X = \{1, \dots, n\}$ , et  $\gamma : G \rightarrow GL(V)$  une représentation linéaire doublement transitive de  $(G, X)$  sur un espace vectoriel  $V$  de dimension finie.

Il existe un morphisme  $\mathcal{J} : G \rightarrow G \times \Pi^n$  de la forme (8) tel que :

1. Si  $\dim(V) = n$ , la représentation  $\gamma$  est semblable à la représentation  $\rho$  associée au morphisme  $\mathcal{J}$ .
2. Sinon la représentation  $\gamma$  est semblable à l'une des deux représentations de  $G$  sur les espaces  $E_1$  ou  $E_2$  décrites dans le théorème 1.

Nous donnerons plus loin quelques exemples. Le premier est un exemple de représentation associée à un morphisme  $\mathcal{J}$  de la forme (8) qui est irréductible. Nous le généraliserons ensuite aux sous-groupes de  $GL_d(q)$  contenant  $SL_d(q)$ .

## **2 Preuves**

### **2.1 Un résultat préliminaire**

#### **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

$(k, c)$ , posons  $S(k, c) = k.I_n + c.S$ . Notons  $\beta_{k,c}$  et  $\phi_{k,c}$  la forme bilinéaire et l'endomorphisme symétrique associés à la matrice  $S(k, c)$  dans la base  $(e)$ .

On suppose  $c \neq 0$ .

1.a. L'application affine  $\alpha : \lambda \rightarrow k + c.\lambda$  établit une bijection entre les valeurs propres de  $S = S(0, 1)$  et celles de  $S(k, c)$ .

1.b. Les sous-espaces propres de  $\phi_{k,c}$  sont indépendants du couple  $(k, c)$ . Plus précisément, si  $E_{k,c}(\mu)$  désigne le sous-espace propre de  $\phi_{k,c}$  associé à la valeur propre  $\mu$  on a :

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

2. Soient  $E = E_1 \oplus \dots \oplus E_s$  la décomposition de  $E$  en somme des sous-espaces propres de  $S$  associés aux valeurs propres  $\lambda_1, \dots, \lambda_s$  qu'on suppose rangées en fonction de leurs multiplicités croissantes  $m_1 \leq \dots \leq m_s$ . Le noyau de  $\phi_{k,c}$  est  $(0)$  ou l'un des  $E_i$ , son image est  $E$  ou la somme des  $E_j$  pour  $j \neq i$ .

3. Le rang de  $\phi_{k,c}$  est toujours supérieur ou égal à  $n - m_s$ .

*Démonstration.* Simple, on la laisse au lecteur. □

## 2.2 Preuve du théorème 1

On adopte les hypothèses et notations du théorème 1.

1. L'unicité de  $\rho$  est claire.

Pour chaque élément  $\sigma$  de  $G$  la relation (4) :

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

définit une fonction  $\rho_\sigma$  envoyant la base orthonormée  $(e) = (e_1, \dots, e_n)$  sur une base orthonormée de  $E$ , qui s'étend donc en une isométrie linéaire de  $E$ . Il nous reste à vérifier que pour  $\sigma$  et  $\delta$  dans  $G$  on a  $\rho_\sigma \cdot \rho_\delta = \rho_{\sigma\delta}$ , ce qui découle simplement du fait que  $\mathcal{J}$  est un morphisme car :

$$\rho_{\sigma\delta}(e_i) = \nu_i^{\sigma\delta} e_{\sigma\delta(i)} \quad \text{et} \quad \rho_\sigma \cdot \rho_\delta(e_i) = \rho_\sigma(\nu_i^\delta \cdot e_{\delta(i)}) = \nu_i^\delta \cdot \nu_{\delta(i)}^\sigma e_{\sigma\delta(i)},$$

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

$$\nu^{\sigma\delta} = \nu_\delta^\sigma\nu^\delta,$$

ce qui montre que pour tout indice  $i$  dans  $X$ , on a  $\rho_{\sigma\delta}(e_i) = \rho_\sigma \cdot \rho_\delta(e_i)$ , et prouve donc 1.

2.a. Le groupe  $G$  opérant deux fois transitivement sur l'ensemble  $X$ , il est clair, d'après la relation (6), 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 (6) il en est bien sûr de même de  $-\mathcal{E}$ , ce qui prouve l'assertion.

2.b. Nous utiliserons le

### Lemme 1

Toute matrice symétrique réelle  $\mathcal{E} = (\varepsilon_{i,j})_{1 \leq i,j \leq n}$  qui remplit les conditions (6) a exactement deux valeurs propres.

*Démonstration.* Soit  $\lambda_1, \dots, \lambda_s$  les valeurs propres de  $\mathcal{E}$ , rangées dans l'ordre de leur multiplicités croissantes  $m_1 \leq \dots \leq m_s$ , et  $E_1, \dots, E_s$  les sous-espaces propres associés. Remarquons déjà que  $\mathcal{E}$  n'étant pas une homothétie on a  $s \geq 2$ . Les relations (6) signifient que tout élément du groupe  $G$  est dans le groupe orthogonal de la forme bilinéaire  $\beta$  de matrice  $\mathcal{E}$ . Donc les sous-espaces propres de  $\beta$  sont stables sous l'action de  $G$ . Par suite, pour tout indice  $t$  entre 1 et  $s$ , le projecteur orthogonal  $p_t$  de  $E$  sur  $E_t$  commute avec l'action de  $G$  :

$$\forall \sigma \in G, \quad \rho_\sigma \circ p_t = p_t \circ \rho_\sigma,$$

donc si l'on note  $x_1, \dots, x_n$  les projections de  $e_1, \dots, e_n$  sur  $E_t$  par  $p_t$ , il vient pour tout indice  $j \in X$  et tout  $\sigma \in G$ ,

$$\rho_\sigma \circ p_t(e_i) = p_t \circ \rho_\sigma(e_i) = \nu_i^\sigma \cdot p_t(e_{\sigma(i)}),$$

soit encore

$$\rho_\sigma(x_i) = \nu_i^\sigma \cdot x_{\sigma(i)}.$$

Le groupe  $G$  opère donc aussi deux fois transitivement sur la gerbe de droites  $\{\langle x_1 \rangle, \dots, \langle x_n \rangle\}$  de  $E_t$ . D'après les remarques faites dans l'introduction, il existe des constantes  $k_t, c_t$  telles que

$$\forall i, j \in X, \quad (x_i | x_i) = k_t \quad \text{et pour } i \neq j, \quad (x_i | x_j) = c_t \cdot \varepsilon_{i,j}$$

La matrice de Gram du système de vecteurs  $(x_1, \dots, x_n)$  est donc  $S_{\mathcal{E}}(k_t, c_t)$  où  $c_t \neq 0$  puisque ces vecteurs sont liés. D'après la proposition 1, son rang  $r_t$  vaut  $r_t = n - m_i$  pour un indice  $i$  compris entre 1 et  $s$ , mais ce rang est aussi inférieur ou égal à la dimension  $m_t$  de  $E_t$ . Comme  $m_1 \leq \dots \leq m_s$ , il vient

$$n - m_s \leq n - m_i = r_t \leq m_t,$$

d'où l'on tire  $n \leq m_t + m_s$ . Choisisant  $t \neq s$ , il vient

$$n \leq m_t + m_s \leq n, \quad \text{puis} \quad m_t + m_s = n.$$

Comme bien sûr  $m_1 + \dots + m_s = n$ , on a  $s = 2$  et  $t = 1$ . Donc  $S_{\mathcal{E}}(k_t, c_t)$  ne possède que deux valeurs propres ainsi que  $\mathcal{E}$  d'après la proposition 1.  $\square$

On peut maintenant achever la preuve du théorème 1.

Soit  $V$  un sous- $G$ -module de  $E$  et  $p$  la projection orthogonale sur  $V$ . Les projections respectives  $v_1, \dots, v_n$  des vecteurs  $e_1, \dots, e_n$  sur  $V$  engendrent une gerbe de droites  $\{\langle v_1 \rangle, \dots, \langle v_n \rangle\}$  de  $V$  qui est permutée deux fois transitivement par le groupe  $G$ . Donc, comme précédemment on voit que la matrice de Gram du système de vecteurs  $v_1, \dots, v_n$  doit être de la forme  $S_{\mathcal{E}}(k, c) = kI_n + c\mathcal{E}$  où  $\mathcal{E}$  est une matrice satisfaisant aux relations (6).

S'il n'existe aucune matrice  $\mathcal{E}$  satisfaisant aux relations (6), le coefficient  $c$  est nul et la matrice de Gram de  $v_1, \dots, v_n$  est  $kI_n$ . Par suite  $v_1, \dots, v_n$  est une base orthogonale de  $V$  et donc aussi de  $E$ . Ceci prouve que  $E$  est irréductible.

Si le coefficient  $c$  n'est pas nul, il existe une matrice  $\mathcal{E}$  satisfaisant aux conditions (6). Notons  $\beta$  la forme bilinéaire de matrice  $\mathcal{E}$  dans la base  $e_1, \dots, e_n$ . Pour deux indices  $i, j$  quelconques et  $\sigma$  dans  $G$  on a

$$\beta(\sigma(e_i), \sigma(e_j)) = \beta(\nu_i^\sigma e_{\sigma(i)}, \nu_j^\sigma e_{\sigma(j)}) = \nu_1^\sigma \nu_j^\sigma \varepsilon_{\sigma(i), \sigma(j)} = \varepsilon_{i,j} = \beta(e_i, e_j).$$

Donc le groupe  $G$  est contenu dans le groupe orthogonal de la forme  $\beta$ . D'après le lemme 1,  $\beta$  possède deux valeurs propres  $\lambda_1$  et  $\lambda_2$  associées à une

décomposition de  $E$  en somme orthogonale  $E = E_1 \oplus E_2$  des sous-espaces propres correspondants, qui sont aussi stables sous l'action de  $G$ . Il ne reste qu'à montrer l'irréductibilité des  $G$ -modules  $E_1$  et  $E_2$ . Soit  $W$  un sous- $G$ -module de  $E$  distinct de  $E$ ,  $p_W$  la projection orthogonale de  $E$  sur  $W$  et  $w_1, \dots, w_n$  les images de  $e_1, \dots, e_n$  par cette projection. Comme précédemment on voit que la matrice de Gram du système de vecteurs  $w_1, \dots, w_n$  est de la forme  $S_{\mathcal{E}}(k, c)$  où  $c \neq 0$  puisque ces vecteurs sont liés. Mais on sait que le rang de cette matrice égal à la dimension  $m_1$  ou  $m_2$  d'un des espaces  $E_1$  et  $E_2$ . Ceci montre déjà que si  $m_1 \leq m_2$ , le  $G$  module  $E_1$  est irréductible et si  $E_2$  ne l'est pas, il est la somme directe de deux sous-modules isomorphe à  $E_1$ . Si c'est le cas on peut décomposer  $E$  en somme orthogonale  $E = E_1 \oplus E'_1 \oplus E''_1$  de trois modules isomorphes. Décomposons chaque  $e_i$  en une somme  $e_i = x_i + x'_i + x''_i$ . Les systèmes de vecteurs  $(x_i)$ ,  $(x'_i)$  et  $(x''_i)$  ayant des matrices de Gram proportionnelles, il existe des  $G$ -isomorphismes qui envoient chaque  $x_i$  sur  $x'_i$  ou chaque  $x_i$  sur  $x''_i$ . Mais alors il est clair qu'il doit exister un morphisme qui envoie chaque  $x_i$  sur  $e_i = x_i + x'_i + x''_i$ . Or ceci est clairement impossible puisque  $m_1 < n$ . Donc  $E_2$  est irréductible, ce qui termine la preuve du théorème 1.  $\square$

### 2.3 Preuve du théorème 2

D'après l'introduction, on peut choisir des vecteurs  $v_1, \dots, v_n$  dans  $V$  tels que :

\*  $V = \langle v_1, \dots, v_n \rangle$ .

\* Le groupe  $G$  opère 2-transitivement la gerbe de droites  $\mathcal{G} = \{\langle v_1 \rangle, \dots, \langle v_n \rangle\}$ .

\* Les relations (4), (5) et (6) sont satisfaites, pour des constantes  $k, c$  et une matrice  $\mathcal{E} = (\varepsilon_{i,j})$  convenablement choisies.

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

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

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

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

Soit  $\rho : G \rightarrow GL(E)$  la représentation associée au morphisme  $\mathcal{J}$ . L'espace  $E$  est donc euclidien, muni d'une base orthonormée  $e_1, \dots, e_n$  telle que la représentation  $\rho$  satisfasse aux relations (4) :

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

Comme la représentation  $\gamma$  satisfait aux mêmes relations, l'application  $\theta : e_j \rightarrow v_j$  (pour  $j \in X$ ) se prolonge en un morphisme du  $G$ -module  $E$  sur le  $G$ -module  $V$ .

1. Si  $\dim V = n$ ,  $\theta$  est un isomorphisme.

2. Sinon le noyau de  $\theta$  est un sous-module de  $E$  qui ne peut qu'être  $E$  ou l'un des deux sous-modules 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  $\gamma : G \rightarrow GL(E)$ , associée à un morphisme  $\mathcal{J} : G \rightarrow G \times \Pi^n$ , qui est doublement transitive et irréductible. Nous utiliserons le résultat classique suivant (voir par exemple [9]) :

#### Lemme 2

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

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

Notons  $\chi$  le caractère de la représentation  $\rho$ ,  $\chi_1, \dots, \chi_k$ , les caractères irréductibles du groupe  $G$ , et pour chaque indice  $j$  ( $1 \leq j \leq k$ ), soit  $\mu_j = (\chi | \chi_j)$  la multiplicité du caractère  $\chi_j$  dans la représentation  $\rho$ .

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  $v_1, \dots, v_{13}$  des droites vectorielles de  $V$  et notons  $\bar{v}_1, \dots, \bar{v}_{13}$  leurs opposés. La représentation linéaire  $\gamma : G \rightarrow GL(\mathbb{R}^{26})$  associée à l'action de naturelle de  $G$  sur  $Y = V^* = \{v_1, \dots, v_{13}, \bar{v}_1, \dots, \bar{v}_{13}\}$  permute la base  $Y$  de  $\mathbb{R}^{26}$ . D'après le lemme 2, cette représentation  $\gamma$  se décompose en une somme de représentations irréductibles  $\gamma_j$  intervenant avec des multiplicités  $\mu_j$  telles que  $3 = \sum_j \mu_j^2$ . On en déduit immédiatement que  $\gamma$  est une somme de trois représentations irréductibles non semblables. Or il n'est pas difficile de les décrire car la représentation  $\gamma$  admet clairement comme sous-représentation l'espace  $U$  engendré par les vecteurs de la forme  $v_i + \bar{v}_i$ , dans lequel la droite vectorielle  $\sum_i v_i + \sum_i \bar{v}_i$  ( $1 \leq i \leq 13$ ) 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'exactly 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  $e_i = v_i - \bar{v}_i$ , et l'action de  $G$  sur  $E$  est donnée par des relations

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



où les coefficients  $\nu_i^\sigma$  valent tous  $\pm 1$ . Donc la représentation de  $G = SL_3(3)$  sur  $E$  donnée par ces relations est irréductible et associée au morphisme  $\mathcal{J} : G \rightarrow G \times \Pi^n$  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  $v_i$  ( $i \in X = \{1, \dots, n\}$ ). 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 est de même de celle de  $G$ . Elle se transmet aussi à  $X$  en notant  $\sigma(i)$ , pour tout indice  $i$  dans  $X$  et tout  $\sigma$  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  $\lambda_i$  tel que

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

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

$$(9) \quad \begin{aligned} * \gamma_\sigma(v_i) &= \nu_i^\sigma \cdot v_{\sigma(i)} & \text{ou} & \quad \nu_i^\sigma = \begin{cases} 1 & \text{si } \lambda_i \in C \\ -1 & \text{si } \lambda_i \in \overline{C} \end{cases}, \\ * \gamma_\sigma(-v_i) &= -\gamma_\sigma(v_i). \end{aligned}$$

Pour éviter toute confusion posons maintenant pour chaque indice  $i$ ,  $\overline{v}_i = -v_i$ , notons encore  $\gamma$  la représentation linéaire du groupe  $G$  sur l'espace  $\mathbb{R}^{2n}$  associée à l'action du groupe  $G$  sur  $Y$  et soit  $\chi$  son caractère. D'après le lemme 2, le nombre  $\omega$  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  $\chi_j$  dans la représentation  $\gamma$ . 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  $\sigma$  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

$$(10) \quad \forall \sigma \in G, \quad \gamma_\sigma(e_i) = \gamma_\sigma(v_i - \overline{v}_i) = \nu_i^\sigma (v_{\sigma(i)} - \overline{v}_{\sigma(i)}) = \nu_i^\sigma \cdot e_{\sigma(i)}$$

Donc la représentation de  $G$  sur  $E$  donnée par ces relations est associée au morphisme  $\mathcal{J} : G \rightarrow G \times \Pi^n$  donné par  $\mathcal{J}(\sigma) = \sigma.\nu^\sigma$ . Le théorème suivant

décrit, suivant les différentes situations, la décomposition de  $\gamma$  en somme de représentations irréductibles.

### **Théorème 3**

*Sous les hypothèses précédentes, soit  $\gamma : G \rightarrow GL(E)$  la représentation de  $G$  donnée par les relations (10)*

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

- Si  $d \geq 3$  la représentation  $\gamma$  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  $\gamma$  est irréductible.

(b) Si  $G \subset GL_2^+(q)$ , la représentation  $\gamma$  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  $q \not\equiv 1 \pmod{4}$ , le module  $E$  reste irréductible sur  $\mathbb{R}$ ,

\* si  $q \equiv 1 \pmod{4}$ , 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  $\gamma$  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  $\Delta$  des couples de vecteurs  $(v, v)$  pour  $v \in Y$ .

\* L'ensemble  $\Delta'$  des couples de vecteurs  $(v, -v)$  pour  $v \in Y$ .

\* L'ensemble  $\nabla$  des couples de vecteurs  $(v, w)$  pour  $v, w \in Y$ , non colinéaires.

De plus l'action  $\gamma$  de  $G$  sur  $Y$  est nécessairement transitive sinon  $\Delta$  et  $\Delta'$  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  $\nabla$  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  $\nabla$  est transitive. Le lemme 2 nous montre que dans ce cas la représentation  $\gamma$  de  $G$  sur  $E$  est irréductible.

- Supposons  $d = 2$ .

**Lemme 3**

Le nombre  $\theta$  d'orbites du groupe  $G$ , agissant sur l'ensemble  $\nabla$  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  $\nabla$ . De plus comme  $G$  opère transitivement sur les couples de droites  $(\langle v_i \rangle, \langle v_j \rangle)$  distinctes, il opère transitivement sur  $\nabla$  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  $\sigma$  tel que  $\sigma(v_i) = v_i$  et  $\sigma(v_j) = \lambda.v_j$  où le scalaire  $\lambda$  n'est pas un carré (d'après la définition (9) de l'action  $\gamma$ ). 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  $\gamma$  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  $\nabla$ , 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 :  $q \not\equiv 1 \pmod{4}$ .*

L'automorphisme  $\sigma$  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 (9) et (10) 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 (6) 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  $\gamma$  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 :  $q \equiv 1 \pmod{4}$ .*

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 combinatorics. 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] Blokhuis, A. *On Subsets of  $GF(q^2)$  with Square Differences.* Indag. Math. 46, 369-372, (1984).
- [7] Brouwer, A. E. ; Cohen, A. M. ; and Neumaier, A. *Conference Matrices and Paley Graphs.* In Distance Regular Graphs. New York : Springer-Verlag.

### *Livres*

- [8] Godsil, Chris, and Royle, *Algebraic Graph Theory.* New York : Springer. (2001)
- [9] Gérard Rauch, *Les groupes finis et leurs représentations.* Ellipses. (2001)
- [10] Norman Biggs. *Finite groups of automorphisms.* London Mathematical Society. (1970)
- [11] Norman Biggs. *Algebraic Graph Theory.* Cambridge University Press, (1993)
- [12] 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).