SUR DES MATRICES DE PERMUTATIONS CONJUGUÉES

Daniel Ferrand et Jean-Claude Raoult

Version corrigée et commentée (juin 2006)

Voici trois démonstrations d'un théorème de R. Brauer. Elles sont tout-à-fait dans le programme et dans l'esprit de l'agrégation, et peuvent être proposées comme développement dans plusieurs leçons, en particulier dans :
— dénombrements,
— groupe opérant sur un ensemble,
— groupe symétrique,
— sous-groupes du groupe linéaire,
— matrices semblables,
— déterminant.

THÉORÈME. — *Soit* K *un corps. Pour toute permutation* $\sigma \in \mathfrak{S}_n$ *on note* $P(\sigma) \in \mathbf{GL}_n(K)$ *la matrice associée à la permutation de la base canonique de* K^n. *Pour que deux permutations* σ *et* τ *soient conjuguées dans le groupe symétrique* $\mathfrak{S}_n$ *il faut et il suffit que* $P(\sigma)$ *et* $P(\tau)$ *soient conjuguées dans le groupe linéaire* $\mathbf{GL}_n(K)$*, c'est-à-dire que ces matrices soient semblables (sur* K*).*

Les deux premières démonstrations utilisent des égalités entre des invariants linéaires (trace, déterminant), lesquels sont des éléments du corps de base ; elles ne permettent pas de conclure en caractéristique positive. La dernière, un peu plus détournée, utilise la *dimension* de sous-espaces invariants ; elle est valable en toute caractéristique.

Remarques : 1) Soit k le sous-corps premier de K (ce corps est donc égal à $\mathbf{Q}$ ou à $\mathbf{F}_p$). La matrice de permutation $P(\sigma)$ est dans le sous-groupe $\mathbf{GL}_n(k)$; par suite ses invariants de similitudes sont des polynômes à coefficients dans k. Ainsi, la similitude de $P(\sigma)$ et de $P(\tau)$ dans $\mathbf{GL}_n(K)$ équivaut à leur similitude dans $\mathbf{GL}_n(k)$, puisque l'égalité dans K[X] de polynômes de k[X], entraîne leur égalité dans k[X].

2) La matrice M de changement de base qui assure l'égalité $P(\tau) = M^{-1}P(\sigma)M$ peut très bien ne pas être une matrice de permutation (c'est le but du théorème d'assurer qu'on peut la choisir telle), même si $K = \mathbf{F}_2 = \{0, 1\}$. Si par exemple on note $T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ la matrice de la transposition dans $\mathbf{F}_2^2$ et I la matrice de l'identité, on peut vérifier que dans $\mathbf{GL}_4(\mathbf{F}_2)$ on a

$$\begin{pmatrix} T & 0 \\ 0 & T \end{pmatrix} = \begin{pmatrix} T & T \\ 0 & T \end{pmatrix} \begin{pmatrix} T & 0 \\ 0 & T \end{pmatrix} \begin{pmatrix} T & T \\ 0 & T \end{pmatrix}.$$

Ou dans $\mathbf{GL}_3(\mathbf{Q})$:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Venons maintenant à la démonstration du théorème. La condition est clairement nécessaire. Réciproquement, on suppose qu'il existe une matrice $M \in \mathbf{GL}_n(K)$ telle que

$$P(\tau) = M^{-1}P(\sigma)M\,. \tag{1}$$

Pour que deux permutations soient conjuguées, il faut et il suffit que leurs décompositions en produits de cycles à supports disjoints comportent le même nombre de cycles de chaque longueur : en effet,

étant donné deux cycles $\sigma = (a_1, a_2, \dots, a_k)$ et $\tau = (b_1, b_2, \dots, b_k)$ de longueur k, toute permutation ρ telle que $\rho(b_i) = a_i$ vérifie $\tau = \rho^{-1}\sigma\rho$.

Notant $c_k(\sigma)$ le nombre de cycles de longueur k dans la décomposition de σ, on se ramène ainsi à montrer que pour tout entier $k \geq 1$ on a

$$c_k(\sigma) = c_k(\tau)\ . \tag{2}$$

Il suffit évidemment de considérer les k inférieurs ou égaux à n. Les trois démonstrations suivantes établissent en fait l'égalité de combinaisons linéaires des c_k, à coefficients dans K pour les deux premières et dans $\mathbf{Q}$ (et même dans $\mathbf{Z}$) pour la dernière. L'inversibilité de la matrice des coefficients permet alors de conclure.

Première démonstration via les polynômes caractéristiques (on suppose $car(\mathrm{K}) = 0$).
L'égalité (1) implique que les deux matrices ont le même polynôme caractéristique. On peut numéroter les éléments de la base de sorte que la matrice $\mathrm{P}(\sigma)$ soit le tableau diagonal des matrices des cycles à supports disjoints de la décomposition de σ. Or le polynôme caractéristique d'un cycle de longueur k est $\mathrm{T}^k - 1$. L'hypothèse se traduit donc par l'égalité suivante entre polynômes à coefficients dans K :

$$\prod_k (\mathrm{T}^k - 1)^{c_k(\sigma)} = \prod_k (\mathrm{T}^k - 1)^{c_k(\tau)}. \tag{3}$$

Soit ζ une racine de l'unité d'ordre m (dans une clôture algébrique de K). Comme K est de caractéristique nulle, les racines des polynômes $\mathrm{T}^k - 1$ sont simples et, par suite, la multiplicité de ζ dans $\mathrm{T}^k - 1$ est 1 si $\zeta^k = 1$, c'est-à-dire si m divise k, et 0 sinon. L'égalité (3) entraîne donc la propriété suivante : pour tout $m \geq 1$, on a

$$\sum_{m|k} c_k(\sigma) = \sum_{m|k} c_k(\tau)\ . \tag{4}$$

Les égalités (2) découlent alors du lemme suivant.

Lemme 1. — *Soient* E *un ensemble muni d'un ordre noté* $x \leq y$ *et* $f, g : \mathrm{E} \to \mathbf{Z}$ *deux applications à support fini et vérifiant la propriété suivante : pour tout* $x \in \mathrm{E}$ *on a*

$$\sum_{x \leq y} f(y) = \sum_{x \leq y} g(y)\ . \tag{5}$$

Alors $f = g$.

Comme f et g sont à support fini, l'ensemble $\mathrm{F} \subseteq \mathrm{E}$ des points où f et g diffèrent est fini. S'il n'était pas vide, l'ensemble F possèderait un élément maximal x (puisqu'il est fini) ; mais la condition (5) conduirait alors à une contradiction.

Voici une autre façon de montrer l'égalité des vecteurs colonnes $\mathrm{C} = (c_k)_k$: noter A la matrice définie ainsi :

$$a_{ij} = \begin{cases} 1 & \text{si } j \text{ divise } i, \\ 0 & \text{sinon.} \end{cases}$$

Elle est triangulaire inférieure, parce que si $j > i$, j ne peut diviser i. De plus, on a $a_{ii} = 1$ et $\mathrm{A} = \mathrm{I} + \mathrm{N}$ où N est une matrice triangulaire inférieure à diagonale nulle, donc vérifiant $\mathrm{N}^n = 0$. La matrice A est donc de déterminant 1, et inversible d'inverse $\mathrm{A}^{-1} = \mathrm{I} - \mathrm{N} + \mathrm{N}^2 - \cdots + (-1)^{n-1}\mathrm{N}^{n-1}$, à coefficients entiers (on peut aussi calculer A^{-1} au moyen de la formule d'inversion de Mœbius).

Or les égalités (4) ci-dessus se traduisent, pour $m = 1, \dots, n$ par

$$\mathrm{C}(\sigma)^t \,.\, \mathrm{A} = \mathrm{C}(\tau)^t \,.\, \mathrm{A} \quad \text{d'où} \quad \mathrm{C}(\sigma) = \mathrm{C}(\tau).$$

Deuxième démonstration via les traces (on suppose toujours K de caractéristique nulle).

L'égalité (1) entraîne que pour tout entier m on a

$$P(\tau^m) = M^{-1}P(\sigma^m)M\ , \tag{6}$$

et par suite, que

$$\mathrm{Tr}(P(\tau^m)) = \mathrm{Tr}(P(\sigma^m)).$$

Pour toute permutation s, la trace de la matrice $P(s)$ est la somme de ses éléments diagonaux, lesquels sont égaux à 1 ou à 0 selon que l'élément de la base correspondant est, ou n'est pas, invariant sous s. Par suite, $\mathrm{Tr}(P(\tau^m))$ est égal à l'image dans K du nombre d'éléments invariants sous τ^m. Pour le calculer, on utilise le lemme suivant.

LEMME 2. — *Si ρ est un cycle de longueur k, alors ρ^m est le produit de d cycles à supports disjoints de longueur k/d où $d = \mathrm{pgcd}(k, m)$. En particulier, ρ^m n'a pas de point invariant, sauf si k divise m, et alors tous les points du support sont invariants.*

La conclusion devrait être claire lorsque m divise k. Si elle ne l'est pas, écrire ρ sous la forme $(1, 2, \dots, k)$ et constater que ρ^m est le produit des m cycles

$$(1, m+1, 2m+1, \dots, k-m+1)(2, m+2, \dots, k-m+2)\cdots(m, 2m, \dots, k).$$

Passons à m quelconque : si $d = \mathrm{pgcd}(k, m)$ les permutations ρ^m et ρ^d engendrent le même sous-groupe de $\mathfrak{S}_n$. En effet, comme d divise m, $\rho^m = (\rho^d)^{m/d}$. D'autre part, l'identité de Bezout s'écrit $d = ma + kb$, donc $\rho^d = (\rho^m)^a$. Enfin les orbites, vues comme les parties stables minimales, dépendent du groupe et non du choix d'un système générateur.

Or σ est un produit de cycles ρ_i à supports disjoints ; donc σ^m est le produit des ρ_i^m sur ces mêmes supports. Si le cardinal k d'un support divise m, les k éléments du support sont invariants. Le nombre d'invariants dans la réunion des $c_k(\sigma)$ supports de cardinal k est donc $kc_k(\sigma)$ et pour tous les supports, $\sum_{k|m} kc_k(\sigma)$. Il en va de même pour τ. L'égalité des traces implique donc que pour tout entier $m \geq 1$ on a, dans K :

$$\sum_{k|m} kc_k(\tau) = \sum_{k|m} kc_k(\sigma)\ . \tag{7}$$

Le lemme 1, mais appliqué cette fois-ci à l'ordre opposé à la divisibilité, donne les égalités $kc_k(\tau) = kc_k(\sigma)$. Comme K est de caractéristique nulle, on obtient l'égalité des entiers c_k.

Autre façon de terminer la démonstration : noter $D = (kc_k)_k$ le vecteur colonne des kc_k et constater que les égalités ci-dessus, pour $m = 1, \dots, n$ s'écrivent, avec la matrice A inversible définie plus haut :

$$A\,D(\tau) = A\,D(\sigma) \quad \text{d'où} \quad D(\tau) = D(\sigma)$$

et conclure comme ci-dessus lorsque K est de caractéristique nulle.

Remarque : Sur un ensemble à p éléments avec p premier, un cycle de longueur p et l'application identique ont pour polynômes caractéristiques $T^p - 1$ et $(T-1)^p$ respectivement. Ces polynômes sont égaux en caractéristique p et ne permettent donc pas de distinguer le cycle de l'application identique.

Troisième démonstration via les espaces d'invariants (K quelconque)
Posons $V = K^n$. Un élément $v = (v_1, \dots, v_n) \in V$ est invariant sous une permutation $\rho \in \mathfrak{S}_n$ lorsque ses coordonnées vérifient les relations $v_i = v_{\rho(i)}$ c'est-à-dire si elles sont constantes sur les orbites de ρ ; par suite, $\dim_K(V^\rho)$ est égal au nombre d'orbites de ρ, y compris celles réduites à un point (il s'agit ici d'un entier naturel, un élément de $\mathbf{N}$). De plus, comme $V^\rho = \mathrm{Ker}(P(\rho) - \mathrm{Id})$, la dimension de cet espace est constante sur les classes de similitude.

Dans le cas d'une permutation σ, le nombre d'orbites de σ^m se déduit des $c_k(\sigma)$ au moyen du lemme 2 : chaque cycle de longueur k composant σ se décompose en $\mathrm{pgcd}(k, m)$ cycles dans σ^m. Par

suite, le nombre d'orbites de σ^m est Σ_k pgcd$(k,m)c_k(\sigma)$. Les égalités (6) impliquent donc, pour tout entier $m \in \mathbf{N}$,

$$\sum_k \text{pgcd}(k,m)c_k(\sigma) = \sum_k \text{pgcd}(k,m)c_k(\tau).$$

La conclusion suit de l'inversibilité de la matrice des pgcd. Celle-ci est classique :

LEMME 3 (Déterminant de Smith). — *Soit* S *la matrice* $n \times n$ *dont le terme d'indice* (i,j) *est* pgcd(i,j). *Alors*

$$\det(S) = \varphi(1)\varphi(2)\cdots\varphi(n)$$

où φ *est la fonction indicatrice d'Euler :* $\varphi(n)$ *est le nombre d'entiers inférieurs à n et premiers avec lui.*

Notons Φ la matrice diagonale de termes $(\varphi(1), \varphi(2), \ldots, \varphi(n))$. En utilisant la relation $\Sigma_{d|m}\ \varphi(d) = m$, on vérifie immédiatement l'égalité suivante :

$$A\Phi A^t = S\ ,$$

où A est encore la matrice de la divisibilité définie plus haut ; et on a déjà vu que $\det A = 1$.

Références

La première démonstration figure maintenant dans le livre de BECK, MALICK, PEYRE : *Objectif Agrégation,* H&K (2004). Elle est détaillée dans un exercice (corrigé) page 321.

La troisième démonstration se trouve dans une lettre de Kovacs à Curtis, intitulée : *The permutation lemma of Richard Brauer,* et reproduite dans le Bull. London Math. Soc., 14 (1982), 127-128.

Commentaires

L'interêt mathématique de ce théorème apparaît si on le situe dans son contexte naturel qui est la théorie des représentations des groupes finis, théorie qui va être évoquée *a minima.*

1. Représentations

Les *représentations* d'un groupe G sont les opérations de G sur différents ensembles munis de structures variées, et respectant ces structures, c'est-à-dire les morphismes $G \to \text{Aut}(X)$ de G dans le groupe des automorphismes de X.

Ainsi, une opération d'un groupe G sur un ensemble fini X est la donnée d'un morphisme de groupes $G \to \mathfrak{S}_X$; on dit, selon l'humeur, que X est un G-ensemble, ou bien une *représentation discrète* de G. On note gx l'image de x par g, $X^G \subset\!\!\to X$ l'ensemble des éléments de X invariants sous G, et $X \to X/G$ désigne le passage au quotient qui associe à $x \in X$ son orbite Gx. Le stabilisateur G_x est le sous-groupe de G formé des g tels que $gx = x$, de sorte qu'on dispose d'un isomorphisme de G-ensembles

$$G/G_x \xrightarrow{\sim} Gx.$$

De même, une *représentation linéaire* de G est un morphisme de groupes

$$\rho : G \longrightarrow \mathbf{GL}(V),$$

où V est un espace vectoriel de dimension finie sur un corps K ; pour $g \in G$, on écrira souvent g_V, ou même g pour $\rho(g)$; c'est un automorphisme K-linéaire de V.

Le groupe en cause dans la note ci-dessus est un groupe cyclique. En effet, les relations (6) montrent que les permutations σ et τ ont le même ordre, disons N ; elles définissent donc deux morphismes de groupes

$$\rho,\ \rho' \ : \mathbf{Z}/N\mathbf{Z} \longrightarrow \mathfrak{S}_n, \qquad m \mapsto \sigma^m,\ m \mapsto \tau^m,$$

c'est-à-dire deux opérations du groupe $\mathbf{Z}/N\mathbf{Z}$ sur l'ensemble $X = \{1, 2, \dots, n\}$.

Considérons, comme dans le théorème, l'homomorphisme de groupes

$$P \ : \mathfrak{S}_n \longrightarrow \mathbf{GL}_n(K),$$

qui associe à une permutation s la matrice $P(s)$ caractérisée par la relation $P(s)e_i = e_{si}$, où (e_i) est la base canonique de K^n. On obtient, par composition, deux opérations linéaires $P \circ \rho$ et $P \circ \rho'$ du groupe $\mathbf{Z}/N\mathbf{Z}$ sur l'espace vectoriel K^n :

$$\mathbf{Z}/N\mathbf{Z} \rightrightarrows \mathbf{GL}_n(K), \quad m \mapsto P(\sigma^m),\ m \mapsto P(\tau^m)$$

La matrice M des égalités (6) fournit un automorphisme de K^n compatible à ces opérations au sens où, pour tout m, le carré suivant est commutatif :

$$\begin{array}{ccc} K^n & \overset{P(\tau^m)}{\to} & K^n \\ {\scriptstyle M}\downarrow & & \downarrow{\scriptstyle M} \\ K^n & \underset{P(\sigma^m)}{\to} & K^n \end{array}$$

Autrement dit, ces deux représentations linéaires sont isomorphes. Dans ce langage le théorème s'énonce ainsi :

THÉORÈME. — *Considérons deux représentations discrètes d'un groupe* cyclique. *Si les représentations linéaires associées sont isomorphes, alors les représentations discrètes sont déjà isomorphes.*

2. Du discret au linéaire : contravariance

L'intérêt de ce résultat de Brauer tient à ceci qu'il n'est vrai que pour les groupes cycliques ; l'énoncé est déjà faux pour le groupe « de Klein » à 4 éléments, comme on le verra plus bas. Ce résultat révèle surtout que « permuter les éléments d'une base » est moins anodin qu'il n'y paraît.

Pour le comprendre il faut préciser le passage du discret au linéaire, et d'abord regarder de près comment on associe un espace vectoriel à un ensemble.

Soit donc K un corps et X un ensemble fini. On désigne par $M(X, K)$ le K-espace vectoriel de toutes les applications de X vers K (la lettre M est l'initiale de *map* ; la notation fréquente K^X évoque trop les invariants pour être utilisée ici) ; on peut voir une application $v : X \to K$ comme une famille d'éléments de K indexée par X, ou encore, en numérotant de 1 à n les éléments de X, comme un vecteur de K^n. Une base, dite canonique, est $(e_x)_{x\in X}$ définie par $e_x(x) = 1$, et $e_x(y) = 0$ si $y \neq x$; on a $v = \sum_{x\in X} v(x)e_x$.

Le fait essentiel est que le passage de l'ensemble X à l'espace $M(X, K)$ est *contra*-variant au sens suivant : à une application d'ensembles (finis) $f : X \longrightarrow Y$, cette construction associe une application linéaire *dans l'autre sens*

$$f^* \ : M(Y, K) \longrightarrow M(X, K), \quad v \longmapsto v \circ f$$

Ce renversement du sens des flèches se propage à leur propriétés : on constate que si f est injective, alors f^* est surjective, et que si f est surjective alors f^* est injective.

Si un groupe G opère à gauche sur l'ensemble X, on est donc obligé, pour le faire opérer *à gauche* linéairement sur l'espace vectoriel $\mathsf{M}(X, K)$, de poser

$$(g.v)(x) \;=\; v(g^{-1}x).$$

En termes de la base canonique cela donne bien $g.e_x = e_{gx}$, puisque le scalaire $(g.e_x)(x') = e_x(g^{-1}x')$ est non nul exactement pour les $x' \in X$ tels que $g^{-1}x' = x$, c'est-à-dire pour $x' = gx$.

L'application de passage au quotient $X \to X/G$ conduit à une application $\mathsf{M}(X/G, K) \to \mathsf{M}(X, K)$; la propriété universelle du quotient montre immédiatement que c'est un isomorphisme

$$\mathsf{M}(X/G, K) \xrightarrow{\sim} \mathsf{M}(X, K)^G.$$

Cet isomorphisme a été utilisé au début de la troisième démonstration. Il ne faut pas croire que les choses soient symétriques : pour les éléments invariants, l'inclusion $X^G \hookrightarrow X$ conduit à une application $\mathsf{M}(X, K) \to \mathsf{M}(X^G, K)$ qui est bien surjective, mais dont on ne peut pas identifier le noyau à partir seulement de l'opération de G sur l'espace vectoriel $\mathsf{M}(X, K)$; il faudrait utiliser explicitement la base canonique.

3. Isomorphismes de représentations

Dans le cas des représentations discrètes, on dispose d'un critère d'isomorphisme.

PROPOSITION 3.1. — *Soient* G *un groupe fini, et* X *et* Y *deux* G*-ensembles finis. On suppose que pour tout sous-groupe* H *de* G*, on a* $\mathrm{Card}(X^H) = \mathrm{Card}(Y^H)$. *Alors* X *et* Y *sont* G*-isomorphes, au sens suivant : il existe une bijection* $u : X \to Y$ *compatible aux opérations de* G.

Pour définir u, on raisonne par récurrence sur le cardinal de X, qui est égal au cardinal de Y parce que $\mathrm{Card}(X^{\{1\}}) = \mathrm{Card}(Y^{\{1\}})$. Si $X = \varnothing$ l'assertion est vraie. Sinon, il existe un sous-groupe H de G maximal tel que $X^H \neq \varnothing$; par hypothèse, on a aussi $Y^H \neq \varnothing$. Le stabilisateur d'un point $x \in X^H$ et celui d'un point $y \in Y^H$ contiennent H, donc lui sont égaux, puisque H est choisi maximal. On en tire deux isomorphismes de G-ensembles

$$Gx \xleftarrow{\sim} G/H \xrightarrow{\sim} Gy,$$

ce qui permet de définir u sur l'orbite Gx en posant $u(gx) = gy$, pour tout $g \in G$. Pour prolonger u aux complémentaires $X - Gx$ et $Y - Gy$, on constate d'abord qu'ils sont stables sous G et vérifient l'hypothèse de l'énoncé. L'hypothèse de récurrence entraîne donc l'existence d'un isomorphisme de G-ensembles $X - Gx \to Y - Gy$, qui permet de conclure. C.Q.F.D.

Remarque 3.2. Comme on a $\mathrm{Card}(X^H) = \dim_K \mathsf{M}(X^H, K)$, il est bien naturel de tenter de relier ces entiers à la seule représentation linéaire $\mathsf{M}(X, K)$; mais, comme il a été indiqué plus haut, c'est impossible sans hypothèses supplémentaires. Par contre les entiers $\mathrm{Card}(X/H)$ sont facilement accessibles : $\mathrm{Card}(X/H) = \dim_K \mathsf{M}(X/H, K) = \dim_K \mathsf{M}(X, K)^H$.

Lorsque G est cyclique, de générateur g, un sous-groupe H est engendré par une puissance g^m du générateur, et $\mathrm{Card}(X^H) = \mathrm{Card}(X^{g^m})$; la discussion qui suit le lemme 2 montre que l'hypothèse de la proposition 3.1 correspond aux égalités (7), mais écrites dans $\mathbf{Z}$.

Lorsque G n'est plus cyclique, les égalités $\mathrm{Card}(X^g) = \mathrm{Card}(Y^g)$ pour tout $g \in G$, n'entraînent pas l'isomorphisme des G-ensembles X et Y ; elles impliquent seulement que pour tout sous-groupe H de G, on a $\mathrm{Card}(X/H) = \mathrm{Card}(Y/H)$, en vertu d'une formule due à Cauchy et attribuée à Burnside

$$\mathrm{Card}(H)\mathrm{Card}(X/H) \;=\; \sum_{g \in H} \mathrm{Card}(X^g).$$

On va voir que les égalités $\mathrm{Card}(X^g) = \mathrm{Card}(Y^g)$ impliquent l'isomorphisme des représentations $\mathbf{C}$-linéaires associées $\mathsf{M}(X, \mathbf{C})$ et $\mathsf{M}(Y, \mathbf{C})$.

Dans le cas des représentations linéaires, on dispose également d'un critère d'isomorphisme (pour l'énoncé qui suit voir le livre de J.-P. SERRE, *Représentations linéaires des groupes finis*, p.29). Considérons une représentation linéaire d'un groupe fini G

$$\mathrm{G} \longrightarrow \mathbf{GL}(\mathrm{V}), \qquad g \mapsto g_{\mathrm{V}},$$

où V est un $\mathbf{C}$-espace vectoriel de dimension finie. On lui associe son *caractère* $\chi_{\mathrm{V}} : \mathrm{G} \to \mathbf{C}$ défini par

$$\chi_{\mathrm{V}}(g) = \mathrm{Tr}(g_{\mathrm{V}}).$$

Il caractérise (d'où, sans doute, son nom !) les représentations au sens suivant :

PROPOSITION 3.3. — *Deux représentations de même caractère sont isomorphes.*

Lorsque $\mathrm{V} = \mathsf{M}(\mathrm{X}, \mathbf{C})$ est la représentation linéaire associée à une représentation discrète de G, alors, comme on l'a vu dans la seconde démonstration, $\mathrm{Tr}(g_{\mathrm{V}})$ est la somme des éléments diagonaux de la matrice $\mathrm{P}(g)$, lesquels sont égaux à 1 ou 0 selon que l'élément de la base canonique correspondant est, ou n'est pas, invariant sous g. Bref, on a $\chi(g) = \mathrm{Tr}(g_{\mathrm{V}}) = \mathrm{Card}(\mathrm{X}^g)$.

4. Un contre-exemple

L'exemple qui suit est communiqué par J.-P. Serre.

Le groupe « de Klein » $\mathrm{G} = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ *possède deux représentations discrètes* $\rho, \rho' : \mathrm{G} \to \mathfrak{S}_{\mathrm{X}}$*, où* $\mathrm{X} = \{1, 2, 3, 4, 5, 6\}$*, ayant les propriétés suivantes :*
(i) $\mathrm{Card}(\mathrm{X}^{\rho(\mathrm{G})}) \neq \mathrm{Card}(\mathrm{X}^{\rho'(\mathrm{G})})$*; ces représentations ne sont donc pas isomorphes.*
(ii) Pour tout $g \in \mathrm{G}$*, on a* $\mathrm{Card}(\mathrm{X}^{\rho(g)}) = \mathrm{Card}(\mathrm{X}^{\rho'(g)})$*; les représentations* $\mathbf{C}$*-linéaires associées sont donc isomorphes.*

Les morphismes ρ et ρ' sont définis ainsi sur les générateurs du groupe :

$$\begin{cases} \rho((1,0)) = (12)(34), \\ \rho((0,1)) = (13)(24), \end{cases} \quad \text{et} \quad \begin{cases} \rho'((1,0)) = (12)(34), \\ \rho'((0,1)) = (12)(56). \end{cases}$$

Ces deux représentations ne sont pas isomorphes, puisque X ne contient pas d'élément invariant sous $\rho'(\mathrm{G})$ tandis que 5 et 6 sont invariants sous $\rho(\mathrm{G})$.

Les images par ρ et par ρ' des éléments $\neq \mathrm{id}$ de G sont toutes des produits de deux transpositons à supports disjoints ; elles ont donc chacune 2 points fixes, ce qui montre l'assertion *ii)*.

On peut vérifier directement, i.e. sans utiliser la théorie des caractères, que les représentations linéaires en cause sont isomorphes ; mais même dans le cas de ce groupe à 4 éléments les calculs nécessaires ne sont pas évidents ; cela montre la puissance de la proposition 3.3.

L'idée de ces calculs est que, le groupe étant abélien, on peut trouver une base qui diagonalise les éléments de $\rho(\mathrm{G})$ et une autre ceux de $\rho'(\mathrm{G})$; la répartition des valeurs propres (qui sont égales à 1 ou -1 puisque les éléments non triviaux de G sont d'ordre 2) indique comment envoyer la première base sur la seconde.

Dans la base

$$(b_1, b_2, b_3, b_4, b_5, b_6) = (e_1+e_2+e_3+e_4, e_1-e_2+e_3-e_4, e_1+e_2-e_3-e_4, e_1-e_2-e_3+e_4, e_5-e_6, e_5+e_6)$$

les matrices associées à $(1,0)$ et $(0,1)$ sont diagonales :

$$\rho((1,0)) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad \rho((0,1)) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Et dans la base $(b'_1, b'_2, b'_3, b'_4, b'_5, b'_6) = (e_1 + e_2, e_1 - e_2, e_3 + e_4, e_3 - e_4, e_5 - e_6, e_5 + e_6)$ on a

$$\rho'((1,0)) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad \rho'((0,1)) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

On constate que le changement de base défini par $b_1 \mapsto b'_1,\ b_2 \mapsto b'_4,\ b_4 \mapsto b'_2,\ b_3 \mapsto b'_5,\ b_5 \mapsto b'_3,\ b_6 \mapsto b'_6$ fait correspondre ρ' à ρ.