GROUPE DES PERMUTATIONS D'UN ENSEMBLE FINI - APPLICATIONS

SOMMAIRE

Rappels :

L'ensemble S_n des bijections de $[\![1, n]\!]$ dans lui même est un groupe pour la loi de composition des applications :

$$S_n = \mathrm{Bij}[\![1, n]\!] \text{ et } |S_n| = n!$$

Soit $X = \{x_1 ; x_2 ; ... ; x_n\}$ un ensemble de cardinal n. L'ensemble Bij(X) des bijections de X dans lui même est aussi un groupe pour la loi de composition des applications qui est appelé groupe des permutations de X.
Ce groupe Bij(X) est isomorphe au groupe symétrique S_n.
Par la suite, on travaillera donc avec S_n.

Soit $\sigma \in S_n$, on note $\sigma(x)$ l'image de $x \in [\![1, n]\!]$.

Une permutation σ est entièrement déterminée par la donnée des $\sigma(x)$ pour tout $x \in [\![1, n]\!]$.

On présente souvent une permutation sous la notation suivante : $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$

Le groupe S_n est non commutatif dès que $n \geqslant 3$. (Par exemple $(1, 2)(2, 3) = (1, 2, 3)$ et $(2, 3)(1, 2) = (1, 3, 2)$)

1. Orbites et cycles

1.1. Propriété - Définition

Soit $\sigma \in S_n$.

La relation R_σ définie sur $[\![1, n]\!]^2$ par : $x \, R_\sigma \, y \iff \exists n \in \mathbb{Z},\ y = \sigma^n(x)$

est une relation d'équivalence.

Ses classes d'équivalences sont appelées les orbites suivant σ ou σ-orbites.

On note $\text{Orb}_{<\sigma>}(x) = \{\sigma^n(x), n \in \mathbb{Z}\}$ la σ-orbite de x (i.e. la classe d'équivalence de x pour la relation R_σ)

Démonstration de la propriété :

- La réflexivité découle de la propriété $\sigma^0 = Id$.
- La symétrie provient du fait que σ^n est une bijection d'inverse σ^{-n}.
- Le transitivité est une conséquence des règles de composition des applications.

1.2. Remarques sur les orbites :

- x et $\sigma(x)$ sont dans la même σ-orbite.
- si x et y sont dans des σ-orbites différentes, alors il n'existe pas d'entier n tel que $y = \sigma^n(x)$.
- les σ-orbites étant des classes d'équivalences, elles forment donc une partition de $[\![1, n]\!]$.
- Deux permutations σ et σ' différentes peuvent avoir les mêmes orbites ! Considérer, par exemple, dans S_3 :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ et } \sigma' = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

  pour lesquelles il n'y a qu'une seule orbite, à savoir $\{1 ; 2 ; 3\}$

- Une orbite réduite à un élément est dite "triviale". Il y a autant d'orbites triviales que de points fixes par σ.

  En effet, si x est fixe par σ, alors $\text{Orb}_{<\sigma>}(x) = \{\sigma^n(x), n \in \mathbb{Z}\} = \{x\}$.

1.3. Définition **Cycle**

On dit qu'une permutation $\sigma \in S_n$ est un cycle s'il existe **une seule σ-orbite O non triviale** (i.e. card $O > 1$)

S'il en est ainsi, le cardinal de O s'appelle la longueur du cycle σ et O en est le support.

Exemples :

Dans S_5 :

- Considérons : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix}$

  On a : $\text{Orb}_{<\sigma>}(1) = \{1 ; 2 ; 5\}$, $\text{Orb}_{<\sigma>}(3) = \{3\}$, $\text{Orb}_{<\sigma>}(4) = \{4\}$. σ est donc un cycle.

  Comme card $O = 3$, on dit que σ est un 3-cycle et on le note $\sigma = (1, 2, 5)$.

  Le support de σ est : $\text{Supp}(\sigma) = \{1 ; 2 ; 5\}$

- Considérons : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$

  On a :

  $\text{Orb}_{<\sigma>}(1) = \{1 ; 2\}$, $\text{Orb}_{<\sigma>}(3) = \{3 ; 4 ; 5\}$. σ n'est pas un cycle. (On verra que $\sigma = (1, 2)(3, 4, 5)$)

1.4. Remarques sur les cycles :

- Chaque r-cycle s'écrit de r façons différentes.
- Un r-cycle c est d'ordre r (c'est-à-dire $c^r = Id$)
- Un 2-cycle s'appelle une transposition et un n-cycle une permutation circulaire.

1.5. Remarques sur le support :

- Le support d'un r-cycle $(\alpha_1, \alpha_2, \dots, \alpha_r)$ est l'ensemble $\{\alpha_1 ; \alpha_2 ; \dots ; \alpha_r\} \subset [\![1 ; n]\!]$.
- Plus généralement, on peut définir le support pour toute permutation $\sigma \in S_n$ par :

$$\text{Supp } \sigma = \{x \in [\![1 ; n]\!] \text{ tels que } \sigma(x) \neq x\}$$

(Ensemble des éléments dérangés par σ)

On remarquera que : $x \in \text{Supp } \sigma \Rightarrow \sigma(x) \in \text{Supp } \sigma$.

(σ est injective donc $\sigma(x) \neq x$ entraîne $\sigma(\sigma(x)) \neq \sigma(x)$)

Dans le cas d'un cycle, le support coïncide avec l'unique orbite non triviale.

1.6. Proposition

Deux cycles σ et σ' à supports disjoints commutent.

Démonstration :

Notons S le support de σ et S' le support de σ'.

- Si $x \in [\![1 ; n]\!] \setminus S \cup S'$ alors $\sigma(\sigma'(x)) = \sigma'(\sigma(x)) = x$.
- Si $x \in S$ alors $\sigma(x) \in S$ et comme S et S' sont disjoints, $x, \sigma(x) \notin S'$ d'où $\sigma(\sigma'(x)) = \sigma(x)$ et $\sigma'(\sigma(x)) = \sigma(x)$.
- Le cas où $x \in S'$ est analogue.

Dans tous les cas σ et σ' commutent.

1.7. Proposition

Toute permutation $\sigma \in S_n \setminus Id$ s'écrit de façon unique (à l'ordre près des facteurs) $\sigma = c_1 c_2 \dots c_p$ où les c_i sont des cycles à supports disjoints (deux à deux).

Démonstration :

L'idée générale est que l'ensemble des σ-orbites est une partition de S_n et que chaque σ-orbite (non triviale) définit un cycle.

Formalisons :

Soit $\sigma \in S_n \setminus Id$.

Existence :

Notons $A_1, A_2, \dots A_r$ les σ-orbites. On a donc :

$$[\![1, n]\!] = A_1 \cup A_2 \cup \ldots \cup A_r \text{ (union disjointe)}$$

Pour tout $i \in [\![1, r]\!]$, définissons c_i par : $\qquad c_i(x) = \begin{cases} \sigma(x) \text{ si } x \in A_i \\ x \text{ si } x \notin A_i \end{cases}$

Alors c_i est soit l'identité, soit un cycle car :

$$x \notin A_i \Rightarrow \text{Orb}_{<c_i>}(x) = \{x\} \text{ (car } x \text{ est fixe par } c_i)$$

$$x \in A_i \Rightarrow \text{Orb}_{<c_i>}(x) = \{ c_i^k(x), k \in \mathbb{Z}\} = \{\sigma^k(x), k \in \mathbb{Z}\} = \text{Orb}_{<\sigma>}(x) = A_i$$

(Car, si $x \in A_i$ alors $\sigma(x) \in A_i$, donc $c_i^2(x) = c_i(\sigma(x)) = \sigma^2(x)$, donc par récurrence facile : $c_i^k(x) = \sigma^k(x)$)

Donc il y a au plus une c_i-orbite non réduite à un élément, ce qui prouve bien que c_i est l'identité ou un cycle.

Enfin, posons : $\qquad s = c_1 c_2 \ldots c_r$

Montrons que $s = \sigma$. Soit $x \in [\![1, n]\!]$. Notons i l'unique indice tel que $x \in A_i$.

On a alors : $\qquad \forall j \neq i, c_j(x) = x$ et $c_i(x) = \sigma(x)$

En outre : $\qquad \forall j \neq i, c_j(\sigma(x)) = \sigma(x)$ car $\sigma(x) \in A_i$

D'où $\qquad s(x) = \sigma(x)$

C'est-à-dire : $\qquad s = \sigma$

Enfin, on retire du produit les éventuels c_i qui sont l'identité pour obtenir après réindexation :

$$\sigma = c_1 \ldots c_p$$

<u>Unicité</u> :

Supposons que $d_1, \ldots, d_q$ sont des cycles à supports disjoints tels que :

$$\sigma = d_1 \ldots d_q$$

Soit $j \in [\![1, q]\!]$. Soit x un élément du support B_j de d_j.

Comme les supports de $d_1, \ldots, d_q$ sont disjoints deux à deux, seul d_j a un effet sur x :

$$\sigma(x) = d_j(x)$$

Donc, par récurrence : $\qquad \forall k \in \mathbb{Z}, \sigma^k(x) = d_j^k(x)$

C'est-à-dire : $\qquad \text{Orb}_{<\sigma>}(x) = \text{Orb}_{<d_j>}(x) = B_j$

Donc $B_1, \ldots, B_q$ sont les σ-orbites, donc $q = p$ et pour tout $i \in [\![1, p]\!]$ on a, via une réindexation :

$$B_i = A_i$$

Donc : $\qquad d_i = c_i$

Ce qui prouve l'unicité.

<u>Exemple</u> :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} = (1, 2)(3, 4, 5)$$

1.8. Corollaire

Soit $n \in \mathbb{N}$, $n \geqslant 2$.

1) S_n est engendré par les transpositions.
2) S_n est engendré par les $n - 1$ transpositions :

$$(1, i) \text{ où } i \in [\![2, n]\!]$$

3) S_n est engendré par les $n - 1$ transpositions :

$$(i, i + 1) \text{ où } i \in [\![1, n - 1]\!]$$

Note : on a plus l'unicité et les transpositions ne sont pas forcément à supports disjoints. **Cependant le nombre de transpositions est à parité fixe.**

Démonstration :

1) Il suffit de le démontrer pour un cycle. Par récurrence immédiate sur la longueur r.

Retenir qu'un r-cycle peut s'écrire comme un produit de $r - 1$ transpositions.

On considère la propriété :

$$H_r : \text{tout } r\text{-cycle } (\alpha_1, \alpha_2, \dots , \alpha_r) \text{ s'écrit } \tau_1\tau_2 \dots \tau_{r-1}$$
$$\text{où les } \tau_i \ (1 \leqslant i \leqslant r - 1) \text{ sont des transpositions}$$

On a H_2 car un 2-cycle est une transposition.

Supposons : H_r pour un certain entier r.

Soit $c = (\beta_1, \beta_2, \dots, \beta_{r+1})$ un cycle de longueur $r + 1$.

On remarque : $$c = (\beta_1, \beta_{r+1})(\beta_1, \beta_2, \dots , \beta_r).$$

Or, $(\beta_1, \beta_2, \dots , \beta_r)$ est un cycle de longueur r, donc peut (par hypothèse de récurrence) s'écrire $\tau_1\tau_2 \dots \tau_r$.

Posons $\tau = (\beta_1, \beta_{r+1})$. On a donc $c = \tau\, \tau_1\tau_2 \dots \tau_r$, ce qui est H_{r+1}.

D'où 1).

2) Il suffit de remarquer que toute transposition (i, j) peut s'écrire :

$$(i, j) = (1, j)(1, i)(1, j)$$

3) Par récurrence. Soit (i, j) une transposition.

On considère la propriété :

$$\wp(k) : \text{toute transposition } (p, q) \text{ avec } |p - q| \leqslant k \text{ s'écrit comme un}$$
$$\text{produit de transpositions du type } (i, i + 1) \text{ où } i \in [\![1, n - 1]\!]$$

On a $\wp(1)$. (La transposition $(p, p + 1)$ est déjà du type souhaité)

Montrons que, pour tout $k \in [\![1, n - 2]\!]$, on a : $\wp(k) \Rightarrow \wp(k + 1)$

Soit (p, q) une transposition telle que $|p - q| \leqslant k + 1$.

On remarque que : $$(p, q) = (p, q - 1)(q - 1, q)(p, q - 1)$$

Or, par hypothèse de récurrence, la transposition $(p, q - 1)$ s'écrit comme un produit de transpositions du type $(i, i + 1)$ où $i \in [\![1, n - 1]\!]$.

Il en est donc de même pour la transposition (p, q). D'où $\wp(k + 1)$.

D'après le principe de raisonnement par récurrence, on en déduit 3).

Exemple :

Dans S_7 :

$$(3, 7) = (1, 7)(1, 3)(1, 7)$$

$$(3, 7) = (3, 6)(6, 7)(3, 6) = (3, 5)(5, 6)(3, 5)(6, 7)(3, 5)(5, 6)(3, 5) = (3, 5)(5, 6)(6, 7)(5, 6)(3, 5)$$

$$(3,7) = (3, 4)(4, 5)(3, 4)(5, 6)(6, 7)(5, 6)(3, 4)(4, 5)(3, 4) = (3, 4)(4, 5)(5, 6)(6, 7)(5, 6)(4, 5)(3, 4)$$

2. Signature d'une permutation. Groupe alterné

2.1. Définition Signature d'une permutation

Soit $\sigma \in S_n$. On appelle signature de σ l'entier noté $\mathrm{sgn}(\sigma)$ et défini par :

$$\mathrm{sgn}(\sigma) = (-1)^k \text{ où } k \text{ est la parité du nombre de transpositions dans la décomposition de } \sigma.$$

Exemple : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$. On a $\sigma = (1, 2)(3, 4, 5) = (1, 2)(3, 5)(3, 4)$. Donc $\mathrm{sgn}(\sigma) = (-1)^3 = -1$.

2.2. Remarques sur la signature :

- La signature d'une transposition est toujours égale à (-1).
- La signature d'un r-cycle est toujours égale à $(-1)^{r-1}$. (Car, d'après la récurrence vu ci-dessus (1.8.1)), un r-cycle peut se décomposer en $r - 1$ transpositions)

2.3. Théorème

La signature d'une permutation est un morphisme surjectif du groupe $(S_n, \circ)$ sur $(\{-1 ; 1\}, \times)$.

Démonstration :

En effet, pour toutes permutations σ et σ' : $\mathrm{sgn}(\sigma\sigma') = (-1)^{k+k'} = (-1)^k \times (-1)^{k'} = \mathrm{sgn}(\sigma) \times \mathrm{sgn}(\sigma')$.

Donc sgn est un morphisme de $(S_n, \circ)$ sur $(\{-1 ; 1\}, \times)$.

Il est évidemment surjectif, car $\mathrm{sgn}(Id) = 1$ et $\mathrm{sgn}((1, 2)) = -1$

2.4. Théorème

Si p est le nombre d'orbites d'une permutation σ de S_n, alors :

$$\mathrm{sgn}(\sigma) = (-1)^{n-p}$$

Démonstration :

En effet, chaque permutation se décompose de façon unique en un produit de p cycles à supports disjoints :

$$\sigma = c_1 c_2 \ldots c_p$$

Donc : $$\mathrm{sgn}(\sigma) = \prod_{i=1}^{p} (-1)^{\mathrm{long}(c_i)-1} = (-1)^{\sum_{i=1}^{p}(\mathrm{long}(c_i)-1)} = (-1)^{\sum_{i=1}^{p}\mathrm{long}(c_i) - p} = (-1)^{n-p}$$

2.5. Définition

On appelle groupe alterné A_n le noyau du morphisme sgn :

$$A_n = \mathrm{Ker}(\mathrm{sgn}). \text{ (Ensemble des permutations paires)}$$

D'après les propriétés du noyau d'un morphisme de groupe, A_n est donc un sous-groupe distingué de S_n.

De plus, on a : $$\mathrm{Card}\left(S_n / A_n\right) = \mathrm{Card}(\{-1 ; 1\}) = 2$$

Donc : $$\mathrm{Card}(A_n) = \frac{n!}{2}$$

2.6. Théorème

Pour $n \geqslant 3$, le groupe alterné A_n est engendré par les 3-cycles

Démonstration :

Soit $\sigma \in A_n$.

Par définition de la signature, σ s'écrit donc comme un produit d'une nombre pair de transpositions.

Or, on remarque que tout produit de deux transpositions est un produit de 3-cycle :

$(a, b)(b, c) = (a, b, c)$

$(a, b)(a, c) = (a, c, b)$

$(a, b)(c, d) = (a, b)(b, c)(b, c)(c, d) = (a, b, c)(b, c, d)$

D'où le résultat.

2.7. Théorème

Pour $n \geqslant 5$, le groupe alterné A_n est simple

Démonstration :

Elle utilise les théorèmes de Sylow. Hors programme.

Ce résultat est fondamental, car il en résulte l'impossibilité de résoudre, par radicaux, des équations polynomiales de degré $n \geqslant 5$.

3. Applications

3.1. Théorème de Cayley

3.1.1. Théorème de Cayley

Tout groupe fini G d'ordre n est isomorphe à un sous-groupe de S_n.

Démonstration :

On fait opérer G sur lui même par translation à gauche :

$$\begin{aligned} \varphi : G \times G &\longrightarrow G \\ (g, x) &\longmapsto g \,.\, x = gx \end{aligned}$$

On sait que cette opération est simplement transitive. (Voir leçon sur les opérations de groupes)

Or, pour tout $g \in G$, l'application : $\theta(g) : \begin{array}{l} G \longrightarrow G \\ x \longmapsto g \,.\, x \end{array}$

est un endomorphisme de G. (Voir leçon sur les opérations de groupes)

Et l'application : $\theta : \begin{array}{l} G \longrightarrow \mathrm{Bij}(G) \\ g \longmapsto \theta(g) \end{array}$

est injective. (Car : $\theta(g_1) = \theta(g_2) \Rightarrow \forall x \in G, \theta(g_1)(x) = \theta(g_2)(x) \Rightarrow g_1x = g_2x \Rightarrow g_1 = g_2$)

En conséquence, G est isomorphe à $\mathrm{Im}(\theta)$, c'est-à-dire à un sous groupe de $\mathrm{Bij}(G) \cong S_n$.

3.2. Applications multilinéaires alternées

3.2.1 Définition

Soit E un $\mathbb{K}$-ev et $n \in \mathbb{N}^*$. ($\mathbb{K}$ étant un corps de caractéristique $\neq 2$)

Une application n-linéaire $\varphi : E^n \longrightarrow F$ est dite **alternée** si :

$$\forall (i, j) \in [\![1, n]\!]^2 \text{ tels que } i \neq j,\ \forall (x_1, \dots, x_n) \in E^n,\ (x_i = x_j \Rightarrow \varphi(x_1, \dots, x_n) = 0)$$

3.2.2. Proposition

Une application n-linéaire $\varphi : E^n \longrightarrow F$ est dite **alternée** si et seulement si :

$$\forall \sigma \in S_n,\ \forall (x_1, \dots, x_n) \in E^n,\ \varphi(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \mathrm{sgn}(\sigma)\varphi(x_1, \dots, x_n)$$

Démonstration :

Supposons φ alternée. Procédons en deux temps.

Cas où σ est une transposition τ :

Soient i et j dans $[\![1, n]\!]$ tels que $i < j$. Notons $\tau = (i, j)$.

D'après 3.2.1. :

$$\varphi(x_1, \dots, \underbrace{x_i + x_j}_{i^{\text{ème}} \text{ place}}, \dots, \underbrace{x_i + x_j}_{j^{\text{ème}} \text{ place}}, \dots, x_n) = 0$$

Par multilinéarité :

$$\varphi(x_1, \dots, x_i, \dots, x_i, \dots, x_n) + \varphi(x_1, \dots, x_i, \dots, x_j, \dots, x_n) + \varphi(x_1, \dots, x_j, \dots, x_i, \dots, x_n) + \varphi(x_1, \dots, x_j, \dots, x_j, \dots, x_n) = 0$$

$$\varphi(x_1, \dots, x_j, \dots, x_i, \dots, x_n) = -\varphi(x_1, \dots, x_i, \dots, x_j, \dots, x_n)$$

$$\varphi(x_{\tau(1)}, \dots, x_{\tau(n)}) = \mathrm{sgn}(\tau)\varphi(x_1, \dots, x_n)$$

Cas où σ est une permutation quelconque :

Dans ce cas, on a vu que σ se décompose en un produit de N transpositions :

$$\sigma = \tau_1 \dots \tau_N$$

Et on a de plus : $\mathrm{sgn}(\sigma) = (-1)^N$.

En appliquant N fois le cas précédent, on obtient :

$$\varphi(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \varphi(x_{\tau_1 \dots \tau_N(1)}, \dots, x_{\tau_1 \dots \tau_N(n)}) = -\varphi(x_{\tau_1 \dots \tau_{N-1}(1)}, \dots, x_{\tau_1 \dots \tau_{N-1}(n)}) = \dots = (-1)^N \varphi(x_1, \dots, x_n)$$

D'où : $\varphi(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \text{sgn}(\sigma)\varphi(x_1, \dots, x_n)$

Réciproquement, supposons :

$$\forall \sigma \in S_n, \forall (x_1, \dots, x_n) \in E^n, \varphi(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \text{sgn}(\sigma)\varphi(x_1, \dots, x_n)$$

Soient i et j dans $[\![1, n]\!]$ tels que $i < j$ et $(x_1, \dots, x_n) \in E^n$. Supposons $x_i = x_j$.

En notant $\tau = (i, j)$, on a :

$$\varphi(x_1, \dots, x_j, \dots, x_i, \dots, x_n) = -\varphi(x_1, \dots, x_i, \dots, x_j, \dots, x_n)$$

Et comme $x_i = x_j$, il vient : $2\varphi(x_1, \dots, x_n) = 0$

Et comme $2 \neq 0$: $\varphi(x_1, \dots, x_n) = 0$

3.3. Déterminant d'une famille de vecteurs

3.3.1 Définition

Soit E un $\mathbb{K}$-ev de dimension n. (Avec car($\mathbb{K}$) $\neq 2$)

Soit $B(e_1, \dots, e_n)$ une base de E.

On considère n vecteurs $v_1, \dots, v_n$ de E et on note, pour tout $i \in [\![1, n]\!]$: $v_i = \sum_{j=1}^{n} a_{ji} e_j$.

On appelle déterminant de $v_1, \dots, v_n$ dans la base B, le scalaire noté $\det_B(v_1, \dots, v_n)$ et défini par :

$$\det_B(v_1, \dots, v_n) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}$$

3.3.2. Propriété

On se place dans les hypothèses de la définition précédente.

L'application : $\det : E^n \longrightarrow \mathbb{K}$

est une forme n-linéaire alternée.

Démonstration :

La linéarité, par rapport à chaque place, est laissée à titre d'exercice.

Montrons que le déterminant est alterné :

On utilise 3.2.2. Soit $\pi \in S_n$.

$$\det_B(v_{\pi(1)}, \dots v_{\pi(n)}) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^{n} a_{\pi(i)\sigma(i)}$$

Pour chaque $\sigma \in S_n$, posons $\rho = \sigma\pi^{-1}$. Quand σ parcourt S_n, ρ aussi.

On a alors :

$$\det_B(v_{\pi(1)}, \dots v_{\pi(n)}) = \sum_{\rho \in S_n} \text{sgn}(\pi)\,\text{sgn}(\rho) \prod_{i=1}^{n} a_{\pi(i)\pi(\rho(i))} = \text{sgn}(\pi) \sum_{\rho \in S_n} \text{sgn}(\rho) \prod_{i=1}^{n} a_{i\rho(i)} = \text{sgn}(\pi) \det_B(v_1, \dots, v_n)$$