105 – Groupe des permutations d'un ensemble fini. Applications.

Soit E un ensemble fini de cardinal $n \in \mathbb{N}^*$.

1 Groupe des permutations d'un ensemble fini

1.1 Permutations, cycles et transpositions

Définition 1. On appelle permutation de E toute bijection de E dans lui-même. On note $\mathfrak{S}(E)$ l'ensemble des permutations de E. Si $E = [\![1, n]\!]$, on le note $\mathfrak{S}_n$. Si $a_1, \dots, a_n$ sont des entiers deux à deux distincts de $[\![1, n]\!]$, on note,

$$\begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} = \begin{cases} [\![1,n]\!] & \longrightarrow & [\![1,n]\!] \\ k & \longmapsto & a_k \end{cases}$$

Proposition 2. L'ensemble $\mathfrak{S}(E)$ muni de la composition est un groupe. On l'appelle groupe symétrique de E.

Remarque. Si $E = [\![1, n]\!]$, on l'appelle groupe symétrique d'ordre n.

Définition 3. Soit $r \in [\![2, n]\!]$. On appelle r-cycle de E toute permutation σ de E telle qu'il existe $x_1, \dots, x_r \in E$ deux à deux distincts vérifiant :

- pour tout $k \in [\![1, r-1]\!]$, $\sigma(x_k) = x_{k+1}$,
- $\sigma(x_r) = x_1$,
- pour tout $x \in E \setminus \{x_1, \dots, x_r\}$, $\sigma(x) = x$.

On note $(x_1, \dots, x_r)$ un tel cycle, et on dit que r est la longueur de ce cycle.

Exemple 4. Notons $\mathbb{U}_n$ le groupe des racines n-ièmes de l'unité. L'application $\mathbb{U}_n \to \mathbb{U}_n,\ z \mapsto e^{\frac{2i\pi}{n}} z$ est un n-cycle de $\mathbb{U}_n$: c'est le cycle $(1, e^{\frac{2i\pi}{n}}, \dots, e^{\frac{2i(n-1)\pi}{n}})$.

Proposition 5. Soit $r \in [\![2, n]\!]$. L'inverse d'un r-cycle $(x_1, \dots, x_r)$ dans $\mathfrak{S}(E)$ est un r-cycle de même support. Plus précisément,

$$(x_1, \dots, x_r)^{-1} = (x_r, x_{r-1}, \dots, x_1).$$

[JR] **Proposition 6.** Soit $r \in [\![2, n]\!]$. Un r-cycle est d'ordre r dans $\mathfrak{S}(E)$.

Définition 7. On appelle transposition de E un 2-cycle de E.

Exemple 8. L'application $\mathbb{U}_4 \to \mathbb{U}_4,\ z \mapsto \overline{z}$ est une transposition.

[JR] **Proposition 9.** Le groupe $\mathfrak{S}(E)$ est de cardinal $n!$.

[JR] **Proposition 10.** Le groupe $\mathfrak{S}(E)$ est isomorphe au groupe $\mathfrak{S}_n$.

Remarque. Dans la suite de cette leçon, on restreint notre étude au groupe $\mathfrak{S}_n$, sans pour autant perdre en généralité d'après ce qui précède.

1.2 Action naturelle du groupe symétrique

Proposition 11. Le groupe $\mathfrak{S}_n$ agit sur l'ensemble $[\![1, n]\!]$ par $(\sigma, x) \mapsto \sigma(x)$. En particulier, si $\sigma \in \mathfrak{S}_n$, le groupe cyclique $\langle\sigma\rangle$ agit sur l'ensemble $[\![1, n]\!]$ par restriction. Les orbites de l'action de $\langle\sigma\rangle$ sur $[\![1, n]\!]$ sont appelées les σ-orbites. La σ-orbite d'un élément x de E est :

$$\mathrm{Orb}_\sigma(x) = \{\sigma^k(x),\ k \in \mathbb{Z}\}.$$

Définition 12. Soit $\sigma \in \mathfrak{S}(E)$. On appelle support de σ, et on note $\mathrm{Supp}(\sigma)$, l'ensemble des éléments de E dont la σ-orbite possède au moins deux éléments, c'est-à-dire le complémentaire de l'ensemble des points fixes de σ.

Exemple 13. Le support d'un cycle $(x_1, \dots, x_r)$ est $\{x_1, \dots, x_r\}$.

Proposition 14. Soient $\sigma, \rho \in \mathfrak{S}_n$. Alors, [JR]

(i) $\sigma(\mathrm{Supp}(\sigma)) = \mathrm{Supp}(\sigma)$,

(ii) $\mathrm{Supp}(\sigma^{-1}) = \mathrm{Supp}(\sigma)$,

(iii) pour tout $r \in \mathbb{Z}$, $\mathrm{Supp}(\sigma^r) \subset \mathrm{Supp}(\sigma)$,

(iv) si $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\rho) = \varnothing$, $\sigma \circ \rho = \rho \circ \sigma$.

Proposition 15. Un élément σ de $\mathfrak{S}_n$ est un cycle si et seulement si une seule σ-orbite est non réduite à un point. [JR]

1.3 Générateurs

Théorème 16. Toute permutation σ différente de l'identité se décompose en un produit de cycles à supports deux à deux disjoints. Cette décomposition est unique à l'ordre près des facteurs. Si $\sigma = \gamma_1 \cdots \gamma_r$ est une telle décomposition, [JR]

$$\mathrm{Supp}(\sigma) = \bigcup_{k=1}^{p} \mathrm{Supp}(\gamma_k),\ \theta(\sigma) = \mathrm{ppcm}(\theta(\gamma_1), \dots, \theta(\gamma_p)),$$

où θ est l'application qui à un élément de $\mathfrak{S}_n$ associe son ordre dans ce groupe.

Remarque. En pratique, on applique l'algorithme de décomposition en annexe.

Exemple 17. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 2 & 5 \end{pmatrix} = (1, 3, 4)(2, 6, 5).$

[JR] **Lemme 18.** Pour tous $x_1, \dots, x_r \in [\![1, n]\!]$ deux à deux distincts,

$$(x_1, \dots, x_r) = (x_1, x_2)(x_2, x_3) \dots (x_{r-1}, x_r).$$

[JR] **Théorème 19.** Toute permutation se décompose en un produit de transpositions. En particulier, les transpositions engendrent $\mathfrak{S}_n$.

[JR] *Remarque.* Il existe d'autres parties génératrices de $\mathfrak{S}_n$, notamment :

$$\{(1,k),\ 2 \leq k \leq n\},\ \{(k,k+1),\ 1 \leq k \leq n-1\},\ \{(1,2),\ (1,2,\dots,n)\}.$$

1.4 Classes de conjugaison

[JR] **Proposition 20.** Le centre du groupe $\mathfrak{S}_n$, noté $Z(\mathfrak{S}_n)$, vérifie :

$$Z(\mathfrak{S}_n) = \begin{cases} \mathfrak{S}_n & \text{si } n \leq 2, \\ \{Id\} & \text{si } n \geq 3. \end{cases}$$

[JR] **Lemme 21.** Les conjugués d'un cycle sont les cycles de même longueur. Plus précisément, pour tout cycle $(x_1, \dots, x_r) \in \mathfrak{S}_n$, et pour tout $\sigma \in \mathfrak{S}_n$,

$$\sigma \circ (x_1, \dots, x_r) \circ \sigma^{-1} = (\sigma(x_1), \dots, \sigma(x_r)).$$

Définition 22. Soit $\sigma \in \mathfrak{S}_n$. On appelle type de σ la suite des cardinaux de ses σ-orbites rangés dans l'ordre croissant.

Remarque. Les σ-orbites formant une partition de l'ensemble $[\![1, n]\!]$, le type de σ forme donc une partition de l'entier n.

[FU] **Proposition 23.** Deux permutations de $\mathfrak{S}_n$ sont conjuguées si et seulement si elles ont même type.

Corollaire 24. Le nombre de classes de conjugaison de $\mathfrak{S}_n$ est le nombre de partitions de l'entier n.

2 Groupe alterné

2.1 Signature d'une permutation

Définition 25. Si $\sigma \in \mathfrak{S}_n$, on appelle signature de σ, et on note $\varepsilon(\sigma)$, le nombre réel (non nul) défini par,

$$\varepsilon(\sigma) = \prod_{\{i,j\} \subset [\![1,n]\!]} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Proposition 26. Pour tous $\sigma_1, \sigma_2 \in \mathfrak{S}_n$, $\varepsilon(\sigma_1 \circ \sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2)$.

Proposition 27. La signature d'une transposition est -1.

Corollaire 28. Soit $\sigma \in \mathfrak{S}_n$. Soient $\tau_1, \dots, \tau_d \in \mathfrak{S}_n$ des transpositions telles que $\sigma = \tau_1 \circ \dots \circ \tau_d$. Alors, $\varepsilon(\sigma) = (-1)^d$.

Théorème 29. L'application $\sigma \mapsto \varepsilon(\sigma)$ est un morphisme du groupe $(\mathfrak{S}_n, \circ)$ vers le groupe $(\{\pm 1\}, \times)$.

Remarque. Si $n \geq 2$, la signature est surjective.

Corollaire 30. Soit $r \in [\![2, n]\!]$. La signature d'un r-cycle est $(-1)^{r+1}$.

Exemple 31. $\varepsilon\left(\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 2 & 5 \end{pmatrix}\right) = 1.$

Corollaire 32. Soit $\sigma \in \mathfrak{S}_n$. Alors, $\varepsilon(\sigma) = (-1)^{n-\mu(\sigma)}$, où $\mu(\sigma)$ est le nombre de σ-orbites.

Remarque. La signature peut aussi être définie par l'expression ci-dessus.

2.2 Groupe alterné

Définition 33. On appelle groupe alterné d'ordre n, et on note $\mathfrak{A}_n$, le noyau du morphisme signature. Une permutation de $\mathfrak{S}_n$ est dite paire si elle est dans $\mathfrak{A}_n$, et impaire sinon.

Remarque. Il s'agit donc d'un sous-groupe distingué de $\mathfrak{S}_n$.

Proposition 34. Si $n \geq 2$, alors $\mathfrak{A}_n$ est de cardinal $\frac{n!}{2}$.

Proposition 35. Le centre du groupe $\mathfrak{A}_n$, noté $Z(\mathfrak{A}_n)$, vérifie : [JR]

$$Z(\mathfrak{A}_n) = \begin{cases} \mathfrak{A}_n & \text{si } n \leq 3, \\ \{Id\} & \text{si } n \geq 4. \end{cases}$$

Développement n°1

Théorème 36. Si $n \geq 3$, le groupe $\mathfrak{A}_n$ est engendré par les 3-cycles. [JR]

Lemme 37. Si $n \geq 5$, les 3-cycles sont conjugués dans $\mathfrak{A}_n$. [JR]

Théorème 38. Si $n = 3$ ou $n \geq 5$, le groupe $\mathfrak{A}_n$ est simple. [JR]

2.3 Conséquences de la simplicité du groupe alterné

Théorème 39. Si $n \geq 5$, les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{Id\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$. [JR]

Développement n°2

Lemme 40. Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$. Si l'image de toute transposition par φ est une transposition alors $\varphi \in \mathrm{Int}(\mathfrak{S}_n)$. [DP]

Théorème 41. Si $n \neq 6$, les automorphismes de $\mathfrak{S}_n$ sont tous intérieurs. [DP]

3 Applications

Soient $n \in \mathbb{N}^*$, $\mathbb{K}$ un corps commutatif, E un espace vectoriel de dimension n, et $\mathscr{B}$ une base de E.

3.1 Actions de groupes

[JR] **Théorème 42 (Théorème de Cayley).** Tout groupe G est isomorphe à un sous-groupe de $\mathfrak{S}(G)$. Plus précisément, l'application,

$$\begin{array}{rccc} \varphi & : & G & \longrightarrow & \mathfrak{S}(G) \\ & & g & \longmapsto & \left\{ \begin{array}{ccc} G & \to & G \\ h & \mapsto & gh \end{array} \right. \end{array}$$

est un morphisme de groupes injectif. Par le premier théorème d'isomorphisme, G est donc isomorphe à $\varphi(G)$, qui est bien un sous-groupe de $\mathfrak{S}(G)$.

[JR] **Proposition 43.** Reprenons les notations précédentes. Soit $g \in G$. Notons m l'ordre de g dans G et r l'indice de $\langle g \rangle$ dans G. Alors, $\varepsilon(\varphi(g)) = (-1)^{r(m-1)}$.

3.2 Déterminant

[JR] **Théorème 44.** L'espace vectoriel des formes n-linéaires alternées sur E est un espace vectoriel de dimension 1, engendré par l'élément,

$$\begin{array}{rccc} \det_{\mathscr{B}} & : & E^n & \longrightarrow & \mathbb{K} \\ & & (x_1, \dots, x_n) & \longmapsto & \displaystyle\sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) x_{1,\sigma(1)} \dots x_{n,\sigma(n)}. \end{array}$$

où l'on a noté, pour tout $i \in [\![1, n]\!]$, $x_{i,j}$ la j-ième coordonnée du vecteur x_i dans la base $\mathscr{B}$. L'application $\det_{\mathscr{B}}$ est appelée déterminant dans la base $\mathscr{B}$.

[JR] **Proposition 45.** Soient $x_1, \dots, x_n \in E$. Alors, la famille $(x_1, \dots, x_n)$ est libre si et seulement si $\det_{\mathscr{B}}(x_1, \dots, x_n) \neq 0$.

Définition 46. Soit $A \in M_n(\mathbb{K})$. On appelle déterminant de la matrice A le déterminant de ses colonnes dans la base canonique de $M_{n,1}(\mathbb{K})$.

[JR] **Proposition 47.** Soit $A \in M_n(\mathbb{K})$. Alors, A est inversible si et seulement si son déterminant est non nul.

Définition 48. Soit $A \in M_n(\mathbb{K})$. Soient $i, j \in [\![1, n]\!]$. On appelle mineur du couple (i, j), et on note $M_{i,j}$, le déterminant de la matrice obtenue en barrant la i-ième ligne et la j-ième colonne dans la matrice A. On appelle comatrice de A, et on note $\mathrm{Com}(A)$, la matrice de terme général $(-1)^{i+j} M_{i,j}$.

[JR] **Théorème 49.** Soit $A \in M_n(\mathbb{K})$. Alors, ${}^t\mathrm{Com}(A)A = A\,{}^t\mathrm{Com}(A) = I_n$. En particulier, si $\det(A) \neq 0$ alors $A^{-1} = \frac{1}{\det(A)}\,{}^t\mathrm{Com}(A)$.

3.3 Matrices de permutation

Pour tout $\sigma \in \mathfrak{S}_n$, on note P_σ la matrice de terme général $\delta_{i,\sigma(j)}$.

[JR] **Proposition 50.** L'application $\sigma \mapsto P_\sigma$ est un morphisme de groupes injectif de $\mathfrak{S}_n$ vers $GL_n(\mathbb{K})$. En particulier, l'ensemble des matrices de permutation est donc un sous-groupe de $GL_n(\mathbb{K})$ isomorphe à $\mathfrak{S}_n$.

Remarque. Tout groupe d'ordre $n \in \mathbb{N}^*$ est donc isomorphe à un sous-groupe de $GL_n(\mathbb{K})$.

[JR] **Proposition 51.** Pour tout $\sigma \in \mathfrak{S}_n$, $\det(P_\sigma) = \varepsilon(\sigma)$.

3.4 Polynômes symétriques

Définition 52. On dit qu'un polynôme $P \in \mathbb{K}[X_1, \dots, X_n]$ est symétrique si pour toute permutation $\sigma \in \mathfrak{S}_n$, $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$.

Exemple 53. Pour tout $k \in \{1, \dots, n\}$, on note Σ_k le polynôme,

$$\sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \dots X_{i_k} \in \mathbb{K}[X_1, \dots, X_n].$$

Les polynômes $\Sigma_1, \dots, \Sigma_n$ sont des polynômes symétriques, et on les appelle les polynômes symétriques élémentaires.

[JR] **Théorème 54.** Si $P \in \mathbb{K}[X_1, \dots, X_n]$ est symétrique, alors il existe un unique polynôme $Q \in \mathbb{K}[X_1, \dots, X_n]$ tel que $P(X_1, \dots, X_n) = Q(\Sigma_1, \dots, \Sigma_n)$.

[JR] **Théorème 55.** Soit $P \in \mathbb{K}[X]$ un polynôme de degré n scindé sur $\mathbb{K}$. On note $a_0, \dots, a_n$ ses coefficients et $\alpha_1, \dots, \alpha_n$ ses racines dans $\mathbb{K}$. Alors,

$$\forall k \in [\![0, n]\!], \ \frac{a_k}{a_n} = (-1)^k \Sigma_{n-k}(\alpha_1, \dots, \alpha_n).$$

3.5 Groupe des isométries affines

[JR] **Proposition 56.** Le groupe des isométries du plan qui conservent les sommets d'un triangle isocèle non équilatéral est isomorphe à $\mathfrak{S}_2$.

[JR] **Proposition 57.** Le groupe des isométries du plan qui conservent les sommets d'un triangle équilatéral (non plat) est isomorphe à $\mathfrak{S}_3$.

[JR] **Proposition 58.** Le groupe des isométries de l'espace conservant un tétraèdre régulier est isomorphe à $\mathfrak{S}_4$. Le groupe des isométries directes de l'espace qui conservent un tétraèdre régulier est isomorphe à $\mathfrak{A}_4$.

[JR] **Proposition 59.** Le groupe des isométries directes de l'espace conservant un cube est isomorphe à $\mathfrak{S}_4$. Celui des isométries de l'espace conservant un cube est isomorphe à $\mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

4 Annexe

4.1 Algorithme de décomposition en produit de cycles

Soit $\sigma \in \mathfrak{S}_n$. Le principe de l'algorithme de décomposition de σ est le suivant.

1. Si 1 n'est pas un point fixe de σ, on calcule les itérés $\sigma(1), \sigma^2(1), \ldots$, de 1 par σ jusqu'à obtenir $\sigma^{k_1} = 1$ pour $k_1 \in [\![1, n]\!]$, et on conserve les valeurs $\sigma(1), \ldots, \sigma^{k_1-1}(1)$ dans une liste.

2. On reproduit ensuite le même raisonnement pour l'entier naturel i_2 défini par $i_2 = \min [\![1, n]\!] \setminus \{1, \sigma(1), \ldots, \sigma^{k_1-1}(1)\}$, c'est-à-dire qu'on calcule ses itérés par σ jusqu'à obtenir i_2 à partir d'un rang $k_2 \in [\![1, n]\!]$, et on range les valeurs $\sigma(i_2), \ldots, \sigma^{k_2-1}(i_2)$ dans une liste.

3. En itérant le processus, on obtient $i_1, \ldots, i_r \in [\![1, n]\!]$ et $k_1, \ldots, k_r \in [\![1, n]\!]$, avec $i_1 = 1$, tels que l'ensemble,

$$\left\{ \left\{ i_l, \sigma(i_l), \ldots, \sigma^{k_l-1}(i_l) \right\},\ 1 \leq l \leq r \right\}.$$

   forme une partition du support de σ. Pour tout $l \in [\![1, n]\!]$, notons alors γ_l le cycle $(i_l, \sigma(i_l), \ldots, \sigma^{k_l-1}(i_l))$. Avec ces notations, $\sigma = \gamma_1 \circ \cdots \circ \gamma_r$ est la décomposition de σ en produit de cycles à supports deux à deux disjoints (voir la démonstration de [JR]), ce qui assure que l'algorithme fournit le résultat voulu.

```python
# sigma est la liste constitutée des valeurs de sigma
def decomposition(sigma):
    n = len(sigma)
    L = [k for k in range(1,n+1)]
    # Changement d'indice pour conserver les mêmes indices qu'en mathématiques
    sigma = [0]+[sigma[k] for k in range(n)]
    Cycles = []
    while L!=[]:
        x = L[0]
        L.remove(x)
        if sigma[x]!=x:
            Gamma = [x]
            y = sigma[x]
            while y!=x:
                L.remove(y)
                Gamma.append(y)
                y = sigma[y]
            Cycles.append(Gamma)
    return Cycles
```

5 Références

[JR] : Mathématiques pour l'agrégation, algèbre et géométrie de J. Rombaldi (De Boeck Supérieur).

[FU] : Théorie des groupes, cours et exercices de F. Ulmer (ellipses).

[DP] : Cours d'algèbre de D. Perrin (ellipses).

6 Références détaillées

[JR] : Chapitre 2, lemme 2.1.

[JR] : Chapitre 2, théorème 2.1.

[JR] : Chapitre 2, théorème 2.2.

[JR] : Chapitre 2, théorème 2.3.

[JR] : Chapitre 2, théorème 2.4.

[JR] : Chapitre 2, théorème 2.5.

[JR] : Chapitre 2, lemme 2.5.

[JR] : Chapitre 2, théorème 2.6.

[JR] : Chapitre 2, lemmes 2.6, 2.7 et 2.8.

[JR] : Chapitre 2, lemme 2.3.

[JR] : Chapitre 2, lemme 2.2.

[FU] : Chapitre 5, proposition 5.7.

[JR] : Chapitre 2, exercice 2.23.

[JR] : Chapitre 2, théorème 2.10.

[JR] : Chapitre 2, exercice 2.24.

[JR] : Chapitre 2, théorème 2.12.

[JR] : Chapitre 2, théorème 2.11.

[DP] : Chapitre I, proposition 8.8.

[DP] : Chapitre I, théorème 8.7.

[JR] : Chapitre 2, théorème 2.14.

[JR] : Chapitre 2, exercice 2.33.

[JR] : Chapitre 17, théorème 17.2.

[JR] : Chapitre 17, théorème 17.5.

[JR] : Chapitre 17, théorème 17.8.

[JR] : Chapitre 17, théorème 17.11.

[JR] : Chapitre 2, théorème 2.15.

[JR] : Chapitre 2, théorème 2.15.

[JR] : Chapitre 2, théorème 2.16.

[JR] : Chapitre 12, théorème 12.15.

[JR] : Chapitre 3, exercice 3.3.

[JR] : Chapitre 3, exercice 3.4.

[JR] : Chapitre 3, exercice 3.6.

[JR] : Chapitre 3, théorème 3.15.

7 Quelques preuves

7.1 Multiplicativité de la signature

Notons $\mathcal{P}$ l'ensemble des parties de $[\![1,n]\!]$. Alors,

$$\varepsilon(\sigma_1\circ\sigma_2)=\prod_{\{i,j\}\subset\mathcal{P}}\frac{\sigma_1(\sigma_2(i))-\sigma_1(\sigma_2(j))}{\sigma_2(i)-\sigma_2(j)}\prod_{\{i,j\}\subset\mathcal{P}}\frac{\sigma_2(i)-\sigma_2(j)}{i-j}.$$

Or, l'application $\{i,j\}\mapsto\{\sigma_2(i),\sigma_2(j)\}$ est une permutation de $\mathcal{P}$. Donc,

$$\prod_{\{i,j\}\subset\mathcal{P}}\frac{\sigma_1(\sigma_2(i))-\sigma_1(\sigma_2(j))}{\sigma_2(i)-\sigma_2(j)}=\prod_{\{k,l\}\subset\mathcal{P}}\frac{\sigma_1(k)-\sigma_1(l)}{k-l}.$$

Finalement,

$$\varepsilon(\sigma_1\circ\sigma_2)=\prod_{\{k,l\}\subset\mathcal{P}}\frac{\sigma_1(k)-\sigma_1(l)}{k-l}\prod_{\{i,j\}\subset\mathcal{P}}\frac{\sigma_2(i)-\sigma_2(j)}{i-j}=\varepsilon(\sigma_1)\varepsilon(\sigma_2).$$

7.2 Signature d'une transposition

Soit τ une signature. On note p et q les éléments de son support. Tout d'abord,

$$\prod_{\substack{\{i,j\}\subset\mathcal{P}\\ \{i,j\}\cap\{p,q\}=\varnothing}}\frac{\tau(i)-\tau(j)}{i-j}=\prod_{\substack{\{i,j\}\subset\mathcal{P}\\ \{i,j\}\cap\{p,q\}=\varnothing}}\frac{i-j}{i-j}=1.$$

D'autre part,

$$\prod_{\substack{\{i,j\}\subset\mathcal{P}\\ \{i,j\}\cap\{p,q\}\neq\varnothing}}\frac{\tau(i)-\tau(j)}{i-j}=\frac{\tau(p)-\tau(q)}{p-q}\prod_{\substack{i=1\\ i\neq p\\ i\neq q}}^{n}\frac{\tau(q)-\tau(i)}{q-i}\prod_{\substack{i=1\\ i\neq p\\ i\neq q}}^{n}\frac{\tau(p)-\tau(i)}{p-i}.$$

Et donc,

$$\prod_{\substack{\{i,j\}\subset\mathcal{P}\\ \{i,j\}\cap\{p,q\}\neq\varnothing}}\frac{\tau(i)-\tau(j)}{i-j}=\frac{q-p}{p-q}\prod_{\substack{i=1\\ i\neq p\\ i\neq q}}^{n}\frac{p-i}{q-i}\prod_{\substack{i=1\\ i\neq p\\ i\neq q}}^{n}\frac{q-i}{p-i}=-1.$$

Finalement,

$$\varepsilon(\tau)=\prod_{\substack{\{i,j\}\subset\mathcal{P}\\ \{i,j\}\cap\{p,q\}=\varnothing}}\frac{\tau(i)-\tau(j)}{i-j}\prod_{\substack{\{i,j\}\subset\mathcal{P}\\ \{i,j\}\cap\{p,q\}\neq\varnothing}}\frac{\tau(i)-\tau(j)}{i-j}=-1.$$

7.3 Autre expression de la signature

Soit $\sigma\in\mathfrak{S}_n$. Si $\sigma=Id$ alors $\mu(\sigma)=n$ et donc $(-1)^{n-\mu(\sigma)}=1=\varepsilon(\sigma)$. Sinon, σ possède au moins une σ-orbite non réduite à un point. Notons $O_1,\dots,O_r$ ses σ-orbites non réduites à un point. Puisque les σ-orbites forment une partition de l'ensemble $[\![1,n]\!]$, et que les σ-orbites restantes sont de cardinal 1 et sont au nombre de $\mu(\sigma)-r$, il vient,

$$\mu(\sigma)-r+\sum_{k=1}^{r}l_k=n$$

où l'on a noté, pour tout $k\in[\![1,r]\!]$, l_k le cardinal de O_k. Considérons ensuite, pour tout $k\in[\![1,r]\!]$, γ_k la permutation définie pour tout $x\in[\![1,n]\!]$ par,

$$\gamma_k(x)=\begin{cases}\sigma(x) & \text{si } x\in O_k,\\ x & \text{sinon.}\end{cases}$$

Avec ces notations, $\sigma=\gamma_1\circ\cdots\circ\gamma_r$ est donc la décomposition de σ en produit de cycles à supports deux à deux disjoints (voir la démonstration de [JR]). En particulier,

$$\varepsilon(\sigma)=\varepsilon(\gamma_1)\dots\varepsilon(\gamma_r)=(-1)^{l_1+\cdots+l_r-r}=(-1)^{n-\mu(\sigma)}.$$