10.10 Groupe symétrique et groupe alterné

10.10.1 Introduction

Comme exemple de groupes, nous avons donné dans 10.1.4 le groupe symétrique $\mathcal{S}_n$ l'ensemble des permutations de $\mathbb{N}_n$

Exemple pour $n = 5$

On considère les permutations σ et τ définies par :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$$

Alors, nous avons :

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix} \qquad \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}$$

— Nous avons, clairement $\sigma \circ \tau \neq \tau \circ \sigma$, ce qui montre que $\mathcal{S}_5$ n'est certainement pas un groupe commutatif.
— σ est une permutation circulaire ; il est évident que $\sigma^5 = \mathrm{Id}_5$; σ est donc d'ordre 5

Exercice 32 :

Quel est l'ordre de la permutation τ ?

10.10.2 Définition

Soit $\sigma \in \mathcal{S}_n$ une permutation de $\mathbb{N}_n$

1. Un élément $x \in \mathbb{N}_n$ est dit fixe ou invariant par σ si et seument si $\sigma(x) = x$
2. Le support de σ est l'ensemble des éléments $x \in \mathbb{N}_n$ tels que $\sigma(x) \neq x$ et on note

$$\mathrm{supp}(\sigma) = \{x \in \mathbb{N}_n \text{ tels que } \sigma(x) \neq x\}$$

Exemple 15 :

Ainsi, si

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix} \quad \text{et} \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}$$

Nous avons $\mathrm{supp}(\tau_1) = \{1, 3\}$ et $\mathrm{supp}(\tau_2) = \{2, 4, 5\}$

10.10.3 Notion de cycle

Soit $n \in \mathbb{N}$ avec $n \geqslant 2$, et on considère $\mathcal{S}_n$ l'ensemble des permutations de $\mathbb{N}_n$; soit $\sigma \in \mathcal{S}_n$

1. Soit $l \in \mathbb{N}^*$ ($l \geqslant 1$). Nous notons σ^l la permutation de $\mathcal{S}_n$ définie par : $\sigma^l = \underbrace{\sigma \circ \sigma \circ \cdots \sigma}_{l \text{ fois}}$
   On pose, en particulier $\sigma^0 = \mathrm{Id}_n$, l'identité de $\mathbb{N}_n$
2. Si $l \in \mathbb{Z}$ et $l < 0$, on note σ^l la permutation de $\mathcal{S}_n$ définie par : $\sigma^l = \left(\sigma^{-1}\right)^{-l} = \underbrace{\sigma^{-1} \circ \sigma^{-1} \circ \cdots \sigma^{-1}}_{-l \text{ fois}}$
3. Soit $k \in \mathbb{N}$ avec $k \geqslant 2$. Une permutation $\sigma \in \mathcal{S}_n$ est appelée cycle de longueur k, s'il existe k éléments deux à deux distincts $\{a_1, \ldots, a_k\}$ dans $\mathbb{N}_n$ tels que $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, $\cdots$, $\sigma(a_{k-1}) = a_k$, $\sigma(a_k) = a_1$ et si tout élément de $\mathbb{N}_n$ distinct de $a_1, \ldots, a_k$ est fixe par σ

Remarque 36 :

1. On dit qu'un cycle, ou permutation circulaire, de k lettres *(ou k chiffres)* est d'ordre k. Le nombre de lettres *(ou de chiffres)* du cycle est appelé longueur du cycle
2. Il est clair que si $\sigma \in \mathcal{S}_n$ est un cycle de longueur k, alors $\sigma^k = \mathrm{Id}_{\mathbb{N}_n}$, l'identité de $\mathbb{N}_n$
3. **Convention d'écriture**

   On note $\sigma = (a_1, a_2, \cdots, a_k)$ le k-cycle de la définition 10.10.3, les points fixes étant omis de l'écriture. Cette notation veut dire

   $$\sigma(a_1) = a_2 \quad \sigma(a_2) = a_3 \cdots \sigma(a_i) = a_{i+1} \cdots \sigma(a_k) = a_1$$

   Cette notation a le mérite d'être plus compacte que celle vue dans le tableau à deux lignes mais elle existe uniquement pour les cycles. Le support du k-cycle $(a_1, a_2, \cdots, a_k)$ est donc $\{a_1, a_2, \ldots, a_k\}$

   Ainsi, par exemple, dans $\mathcal{S}_5$ le cycle $c = (2, 4, 5)$ signifie :

   $$c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}$$

4. La notation $\sigma = (a_1, a_2, \cdots, a_k)$ n'est pas unique puisque nous pourrions aussi l'écrire $\sigma = (a_2, a_3, \cdots, a_k, a_1)$ ou $\sigma = (a_4, a_5, \cdots, a_k, a_1, a_2, a_3)$ etc ...

10.10.4 Définition de transposition

On appelle transposition de $\mathcal{S}_n$, toute permutation $\sigma \in \mathcal{S}_n$ telle que :

$$\sigma(i) = j \text{ et } \sigma(j) = i$$

et si, pour tout $k \in \mathbb{N}_n$, $k \neq i$ et $k \neq j$, $\sigma(k) = k$

Exemple 16 :

Exemple de transposition de $\mathcal{S}_5$:

$$T = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}$$

Nous avons $T(2) = 3$ et $T(3) = 2$, et si $i = 1$, $i = 4$ et $i = 5$, nous avons $T(i) = i$.
Une autre écriture de T est donc $T = (2, 3)$

Remarque 37 :

1. Une transposition est un cycle de longueur 2 qui peut être notée $\tau = (i, j)$
2. Une transposition est une permutation qui échange 2 nombres.

Exemple 17 :

1. Revenons dans $\mathcal{S}_5$. La permutation circulaire R ainsi définie :

   $$R = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix}$$

   R est une permutation ou cycle de longueur 3 qui peut aussi s'écrire $R = (3, 5, 4)$
2. Retour sur la permutation τ de $\mathcal{S}_5$ définie en 10.10.1
   — La permutation τ échange *(ou transpose)* les chiffres 1 et 3

— La permutation τ permute circulairement 2, 4 et 5.
On peut donc dire que τ est la composée de 2 autres permutations τ_1 et τ_2 définies par :

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix} = (1,3) \qquad \tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix} = (2,4,5)$$

τ_1 est donc un cycle de longueur 2, et τ_2 un cycle de longueur 3
Nous avons $\tau = \tau_1 \circ \tau_2 = \tau_2 \circ \tau_1$
Remarquons que τ_2 laisse invariant l'ensemble $\{1,3\}$, alors que τ_1 laisse invariant l'ensemble $\{2,4,5\}$.
On dit que τ_1 et τ_2 sont disjointes, c'est à dire $\text{supp}(\tau_1) \cap \text{supp}(\tau_2) = \emptyset$

10.10.5 Définition de permutations disjointes

Soient $\alpha \in \mathcal{S}_n$ et $\beta \in \mathcal{S}_n$ 2 permutations de $\mathbb{N}_n$.
α et β sont dites disjointes si et seulement si :

$$(\forall i \in \mathbb{N}_n)\,(\alpha(i) \neq i \Longrightarrow \beta(i) = i)$$

C'est à dire si $\text{supp}(\alpha) \cap \text{supp}(\beta) = \emptyset$

Exemple 18 :

τ_1 et τ_2 sont donc 2 permutations disjointes

10.10.6 Proposition

Deux permutations disjointes commutent, c'est à dire :
Soient $\alpha \in \mathcal{S}_n$ et $\beta \in \mathcal{S}_n$ 2 permutations de $\mathbb{N}_n$ disjointes, c'est à dire telles que $\text{supp}(\alpha) \cap \text{supp}(\beta) = \emptyset$.
Alors :

$$\alpha \circ \beta = \beta \circ \alpha$$

Démonstration

Soit $i \in \mathbb{N}_n$

1. Supposososns que i n'appartienne ni au support de α, ni à celui de β ; alors, $\alpha(i) = \beta(i) = i$, et nous avons bien $\alpha \circ \beta = \beta \circ \alpha$
2. Supposons que i appartienne au support de α ; il existe alors $j \in \mathbb{N}_n$, $j \neq i$, tel que $\alpha(i) = j$. Nous avons $j \in \text{supp}(\alpha)$ puisque si, au contraire, $\alpha(j) = j$, α n'est plus une permutation et il y a donc contradiction.
   Puisque les supports sont disjoints, nous avons $\beta(i) = i$. Alors :
   $$\beta(\alpha(i)) = \beta(j) = j$$
   $$\alpha(\beta(i)) = \alpha(i) = j$$
   Et nous avons donc $\alpha \circ \beta = \beta \circ \alpha$
3. La démonstration serait semblable si i appartenait au cycle de β.

Exercice 33 :

Nous nous plaçons dans $\mathcal{S}_9$. Nous considérons les permutations suivantes :

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 7 & 6 & 5 & 4 & 8 & 9 & 3 & 1 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 6 & 7 & 2 & 4 & 1 & 9 & 8 & 3 \end{pmatrix}$$

1. Calculer $\sigma_1 \circ \sigma_2$, $\sigma_2 \circ \sigma_1$, σ_1^{-1} et σ_2^{-1}
2. Décomposer σ_1 et σ_2 en produit de cycles à supports deux à deux disjoints
3. Donner une factorisation de σ_1 en produit de transpositions. Même question pour σ_2

Exercice 34 :

Nous nous plaçons, cette fois ci dans $\mathcal{S}_7$. Nous considérons les cycles suivants :

$$c_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 7 & 6 & 1 & 5 & 4 & 3 \end{pmatrix} \qquad c_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 6 & 3 & 4 & 2 & 1 & 7 \end{pmatrix}$$

1. Calculer $c_1 \circ c_2$ et $c_2 \circ c_1$.
2. Calculer le carré $c_1^2 = c_1 \circ c_1$ de c_1. Est-ce un cycle ?

Exercice 35 :

On appelle centre de $\mathcal{S}_n$ l'ensemble $Z(\mathcal{S}_n)$ des permutations qui commutent avec toutes les permutations de $\mathcal{S}_n$:

$$Z(\mathcal{S}_n) = \{\sigma \in \mathcal{S}_n \text{ tels que pour tout } s \in \mathcal{S}_n \text{ tel que } s \circ \sigma = \sigma \circ s\}$$

L'objet de cet exercice est de montrer que $Z(\mathcal{S}_n) = \{\mathrm{Id}_{\mathbb{N}_n}\}$ si $n \geqslant 3$.
Supposons donc $n \geqslant 3$ et soient $\sigma \in Z(\mathcal{S}_n)$, $i \in \mathbb{N}_n$, $j \in \mathbb{N}_n$ tels que $i \neq j$. On pose τ la transposition telle que $\tau(i) = j$

1. Montrer que $(\tau\sigma)(i) = \sigma(j)$
2. En déduire $\sigma(i) \in \{i, j\}$
3. Démontrer que $\sigma(i) = i$ *(Indication : on pourra faire intervenir un entier $k \notin \{i, j\}$ et la transposition $\tau_1(i) = k$)*. Conclure.
4. Que se passe-t-il si $n = 2$?

10.10.7 Proposition

Soit σ une permutation d'un ensemble fini X de cardinal n (X est en bijection avec $\mathbb{N}_n$ et peut donc être assimilé à $\mathbb{N}_n$)
Soit $\mathcal{R}$ la relation définie sur X par :

$$(\forall x \in X)(\forall y \in X)(x\mathcal{R}y \iff (\exists m \in \mathbb{Z})(y = \sigma^m(x)))$$

$\mathcal{R}$ est une relation d'équivalence sur X
On appelle orbite une classe d'équivalence pour cette relation $\mathcal{R}$

Démonstration

Nous allons démontrer que $\mathcal{R}$ vérifie les axiômes des relations d'équivalence

1. **Cette relation est réflexive**
   Soit $x \in X$; nous avons $x = \mathrm{Id}_X(x)$. Or, $\sigma^0 = \mathrm{Id}_X$, et donc $x = \sigma^0(x)$
   Ainsi, il existe $m \in \mathbb{Z}$, et $m = 0$ tel que $x = \sigma^m(x)$, et nous avons $x\mathcal{R}x$
   La relation $\mathcal{R}$ est donc réflexive.
2. **Cette relation est symétrique**
   Soient $x \in X$ et $y \in X$ tels que $x\mathcal{R}y$. Ceci veut donc dire qu'il existe $m \in \mathbb{Z}$ tel que $y = \sigma^m(x)$.
   σ étant une bijection, par les théorèmes de composition, il en va de même de σ^m ; il existe donc une bijection réciproque $(\sigma^m)^{-1} = \sigma^{-m}$, telle que que nous avons $x = \sigma^{-m}(y)$ et donc nous avons $y\mathcal{R}x$
   La relation $\mathcal{R}$ est donc symétrique

3. **Cette relation est transitive**
   Soient $x \in X$, $y \in X$ et $z \in X$ tels que $x\mathcal{R}y$ et $y\mathcal{R}z$.
   Ceci veut donc dire qu'il existe $m \in \mathbb{Z}$ et $p \in \mathbb{Z}$ tel que $y = \sigma^m(x)$ et $z = \sigma^p(y)$
   Donc, $z = \sigma^p(y) = \sigma^p(\sigma^m(x)) = \sigma^{m+p}(x)$. Il existe donc $k \in \mathbb{Z}$, et $k = m+p$ tels que $z = \sigma^k(x)$, et nous avons donc $x\mathcal{R}z$
   La relation $\mathcal{R}$ est donc transitive

La relation $\mathcal{R}$ est donc une relation d'équivalence.

Remarque 38 :

Soit $x \in X$; quelle est la classe d'équivalence de x pour la relation $\mathcal{R}$. L'orbite de x, notée $\mathcal{O}(x)$ est donnée par :

$$\mathcal{O}(x) = \left\{x, \sigma(x), \sigma^2(x), \ldots, \sigma^m(x), \ldots\right\}$$

Et si X est un ensemble fini, il existe sûrement $m \in \mathbb{Z}$ tel que $\sigma^m(x) = x$.
Cette remarque est utile dans le théorème qui suit

10.10.8 Théorème

Soit X un ensemble fini, et $\mathcal{S}_X$ son groupe de permutations.
Toute permutation $\sigma \in \mathcal{S}_X$ telle que $\sigma \neq \mathrm{Id}_X$ résulte de la décomposition $\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \gamma_k$ de cycles disjoints γ_i, chacune ayant un cycle de longueur 2 ou plus.

Démonstration

Soit $\sigma \in \mathcal{S}_X$ une permutation de X. On considère la relation d'équivalence $\mathcal{R}$ définie dans 10.10.7.
Soit $x \in X$

1. Alors, il existe une seule orbite C telle que $x \in C$, et nous pouvons écrire C par :

   $$C = \{y \in X \text{ tels que } y = \sigma^m(x) \text{ où } m \in \mathbb{Z}\} = \{x, \sigma(x), \ldots \sigma^m(x), \ldots\}$$

   X étant un ensemble fini, et comme $C \subset X$, C est forcément fini ; il existe donc $r \in \mathbb{Z}$ tel que $x = \sigma^r(x)$.
   Soit $m \in \mathbb{N}$ le plus petit entier positif tel que $x = \sigma^m(x)$. Alors, C contient exactement m éléments, c'est à dire :

   $$C = \left\{x, \sigma(x), \ldots \sigma^{m-1}(x)\right\}$$

2. Soit γ, la permutation circulaire suivante, de longueur m :

   $$\gamma = \begin{pmatrix} x & \sigma(x) & \sigma^2(x) & \cdots & \sigma^{m-1}(x) \\ \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\ \sigma(x) & \sigma^2(x) & \sigma^3(x) & \cdots & x \end{pmatrix}$$

   γ laisse inchangé les points n'appartenant pas à l'orbite C. nous avons donc, si $x \in C$, $\gamma(x) = \sigma(x)$, et si $y \notin C$, $\gamma(y) = y$

3. X étant un ensemble fini, les orbites étant des classes d'équivalence, donc disjointes, elles sont en nombre fini. Supposons donc qu'il y ait k orbites. Nous avons, bien entendu :

   $$X = \bigcup_{i=1}^{k} C_i \text{ et } \bigcap_{i=1}^{k} C_i = \emptyset$$

   On appelle γ_i la permutation circulaire définie comme ci-dessus et appliquée à l'orbite C_i, c'est à dire que γ_i est la permutation égale à σ sur C_i et à l'dentité en dehors de C_i
   Si $i \neq j$, γ_i laisse inchangé tout élément de C_j, et donc tout élément déplacé par γ_j. γ_i et γ_j sont donc disjointes, et d'après 10.10.6 commutent.

4. Montrons, maintenant, que $\sigma = \gamma_1 \circ \gamma_2 \circ \ldots \circ \gamma_k$
   Soit $y \in X$
   Alors, si $\sigma(y) = z$, y et z appartiennent à la même orbite. Il existe donc $1 \leqslant i \leqslant k$ tel que $y \in C_i$ et $z \in C_i$, et donc tel que $z = \gamma_i(y)$ et tel que, pour tout $j \neq i$, $\gamma_j(y) = y$ et $\gamma_j(z) = z$
   Par suite, nous avons bien $\gamma_1 \circ \gamma_2 \circ \ldots \circ \gamma_k \gamma_j(y) = z = \sigma(y)$, et ceci étant vrai pour tout $y \in X$, nous avons $\sigma = \gamma_1 \circ \gamma_2 \circ \ldots \circ \gamma_k$.

Ce que nous voulions

Exercice 36 :

Soit $\sigma \in \mathcal{S}_5$ défini par

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$$

1. Ecrire la décomposition de σ en produit de cycles de supports disjoints.
2. Donner la liste des éléments de $\Gamma(\sigma)$ le sous-groupe engendré par σ

10.10.9 Corollaire

Soit X un ensemble fini.
L'ordre d'une permutation $\sigma \in \mathcal{S}_X$ est égal au ppcm des longueurs de ses cycles disjoints

Démonstration

Soit X un ensemble fini et $\sigma \in \mathcal{S}_X$
On peut représenter σ comme la composée de k cycles disjoints $(\gamma_i)_{i=1,\cdots,k}$. Nous avons donc, pour tout i et j $\gamma_i \circ \gamma_j = \gamma_j \circ \gamma_i$ et $\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_k$
Pour tout entier $m \in \mathbb{N}$, nous avons $\sigma^m = \gamma_1^m \circ \gamma_2^m \circ \cdots \circ \gamma_k^m$, d'où, $\sigma^m = \mathrm{Id}_X$ si et seulement si, parce que les cycles sont disjoints, $\gamma_i^m = \mathrm{Id}_X$ pour tout $i = 1, \ldots, k$
m est donc un multiple commun des longueurs de tous les cycles.
L'ordre de σ est donc la plus petite valeur de ces multiples communs ; c'est donc le ppcm.

Exemple 19 :

On revient à la transformation τ

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$$

qui se décompose en deux cycles τ_1 et τ_2 $\tau = \tau_1 \circ \tau_2 = \tau_2 \circ \tau_1$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix} = (1,3) \qquad \tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix} = (2,4,5)$$

où τ_1 est un cycle de longueur 2, et τ_2 un cycle de longueur 3.
L'ordre de τ est donc 6 *(A vérifier en exercice)*

Exercice 37 :

Donner, si c'est possible, un exemple d'élément d'ordre 30 dans le groupe symétrique $\mathcal{S}_{10}$.

10.10.10 Proposition

Soit X un ensemble fini de cardinal n et $\mathcal{S}_n = \mathcal{S}_X$ son groupe de permutation.
On considère $\gamma \in \mathcal{S}_n$ un cycle de longueur m.
Alors, pour tout permutation $\sigma \in \mathcal{S}_n$, la permutation $\sigma \circ \gamma \circ \sigma^{-1}$ est aussi un cycle de longueur m

Démonstration

On note $X = \{x_1, \cdots, x_n\}$, et pour simplifier les choses, nous posons $\gamma = (x_1, \cdots, x_m)$, ce qui veut dire :
- Si $1 \leqslant i \leqslant m-1$, alors $\gamma(x_i) = x_{i+1}$ et $\gamma(x_m) = x_1$
- Si $m+1 \leqslant i \leqslant n$, alors $\gamma(x_i) = x_i$

Soit $y \in X$. σ étant une permutation, il existe un unique $x \in X$ tel que $y = \sigma(x) \Longleftrightarrow x = \sigma^{-1}(y)$

1. On suppose que x n'appartienne pas au cycle de γ
   Alors, $\gamma(x) = x$ et
   $$\sigma \circ \gamma \circ \sigma^{-1}(y) = \sigma \circ \gamma(x) = \sigma(x) = y$$
   y n'est donc pas dans le support de $\sigma \circ \gamma \circ \sigma^{-1}$, et dans la mesure où σ est une bijection, on peut dire qu'il y a $n-m$ éléments de X qui ne sont pas dans le support de $\sigma \circ \gamma \circ \sigma^{-1}$.
   On ne sait pas encore si $\sigma \circ \gamma \circ \sigma^{-1}$ est un cycle.
2. On suppose maintenant que x appartienne au cycle de γ
   Il existe donc i_0, avec $1 \leqslant i_0 \leqslant m$ tel que $x = x_{i_0}$
   ⋆ Si $1 \leqslant i_0 \leqslant m-1$, alors $\gamma(x) = \gamma(x_{i_0}) = x_{i_0+1}$ et
   $$\sigma \circ \gamma \circ \sigma^{-1}(y) = \sigma \circ \gamma(x_{i_0}) = \sigma(x_{i_0+1})$$
   ⋆ Et si $i_0 = m$, $\sigma \circ \gamma \circ \sigma^{-1}(y) = \sigma \circ \gamma(x_m) = \sigma(x_1)$
   Donc, $\sigma \circ \gamma \circ \sigma^{-1}(y) = \sigma \circ \gamma(x) = \sigma \circ \gamma(x_{i_0}) = \sigma(x_{i_0+1})$

Ce qui veut dire que $\sigma \circ \gamma \circ \sigma^{-1}$ est un cycle de longueur m.

Exemple 20 :

L'exemple ci après est toujours pris dans $\mathcal{S}_5$. On considère γ et σ deux permutations de $\mathcal{S}_5$

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

γ est donc un cycle de longueur 3
Considérons, maintenant, la permutation σ :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} \text{ et donc } \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$$

Et nous pouvons alors trouver $\sigma \circ \gamma \circ \sigma^{-1}$:

$$\sigma \circ \gamma \circ \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix} = (1,4,2)$$

$\sigma \circ \gamma \circ \sigma^{-1}$ est donc un cycle de longueur 3. Si $\mathcal{C}$ est le support de γ, nous avons $\mathcal{C} = \{2,4,5\}$, alors $\mathcal{C}'$, support de $\sigma \circ \gamma \circ \sigma^{-1}$ est donné par

$$\mathcal{C}' = \sigma(\mathcal{C}) = \{\sigma(2), \sigma(4), \sigma(5)\} = \{4,1,2\}$$

Exercice 38 :

Montrer que si c et c_1 sont deux cycles dans $\mathcal{S}_n$ de même longueur k, il existe $\sigma \in \mathcal{S}_n$ tel que $c_1 = \sigma \circ c \circ \sigma^{-1}$ *(on dit que c_1 et c sont conjugués dans $\mathcal{S}_n$).*

10.10.11 Théorème

Toute permutation $\sigma \in \mathcal{S}_n$ est un produit de transpositions
En particulier, un cycle γ de longueur m est un produit de $m-1$ transpositions

Démonstration

Soit $\sigma \in \mathcal{S}_n$
Alors, σ est le produit de k permutations circulaires disjointes γ_i, c'est à dire : $\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_k$
Si on réussit à montrer que toute permutation circulaire de $\mathcal{S}_n$ est le produit de transpositions, on pourra le généraliser à σ
Soit donc γ une permutation circulaire, et on montre que γ est le produit de transpositions
On appelle $\mathcal{C} = \{x_1, x_2, \ldots, x_m\}$ le cycle de la permutation γ, c'est à dire :

$$\gamma \begin{pmatrix} x_1 & x_2 & \cdots & x_m & x_{m+1} & \cdots & x_n \\ \downarrow & \downarrow & \cdots & \downarrow & \downarrow & \cdots & \downarrow \\ x_m & x_1 & \cdots & x_{m-1} & x_{m+1} & \cdots & x_n \end{pmatrix}$$

On considère les transpositions τ_i, $2 \leqslant i \leqslant m$ définies par : $\tau_i(x_1) = x_i$, $\tau_i(x_i) = x_1$ et $\tau_i(x_k) = x_k$ si $k \neq i$
Alors, nous avons $\gamma = \tau_2 \circ \tau_3 \circ \cdots \circ \tau_m$. En effet,
Si $k \geqslant m+1$, nous avons $\gamma(x_k) = x_k$, et, pour tout i, $\tau_i(x_k) = x_k$, donc, si $k \geqslant m+1$, nous avons $\gamma(x_k) = \tau_2 \circ \tau_3 \circ \cdots \circ \tau_m(x_k)$
Pour $2 \leqslant i \leqslant m$, $\gamma(x_i) = x_{i-1}$, et

$$\begin{aligned} \tau_2 \circ \tau_3 \circ \cdots \circ \tau_m(x_i) &= \tau_2 \circ \tau_3 \circ \cdots \circ \tau_i(x_i) \\ &= \tau_2 \circ \tau_3 \circ \cdots \circ \tau_{i-1}(x_1) \\ &= \tau_2 \circ \tau_3 \circ \cdots \circ \tau_{i-2}(x_{i-1}) \\ &= x_{i-1} \end{aligned}$$

Donc, si $2 \leqslant i \leqslant m$, nous avons $\gamma(x_i) = \tau_2 \circ \tau_3 \circ \cdots \circ \tau_m(x_i)$
D'autre part,$\gamma(x_1) = x_m$ et

$$\begin{aligned} \tau_2 \circ \tau_3 \circ \cdots \circ \tau_m(x_1) &= \tau_1 \circ \tau_2 \circ \cdots \circ \tau_{m-1}(x_m) \\ &= x_m \end{aligned}$$

Donc, pour tout $1 \leqslant i \leqslant n$, nous avons $\gamma(x_i) = \tau_2 \circ \tau_3 \circ \cdots \circ \tau_m(x_i)$ et nous avons montré qu'un cycle de longueur m est le produit de $m-1$ transpositions.

Exercice 39 :

Montrer que le produit de deux transpositions distinctes est un cycle de longueur 3 ou un produit de deux cycles de longueur 3.

10.10.12 Signature d'une permutation

Soit σ une permutation de $\mathcal{S}_n$

1. On dit qu'un couple (x_i, x_j) est une inversion pour σ, lorsque nous avons $i < j$ et $\sigma(x_i) > \sigma(x_j)$
2. Nous notons $I(\sigma)$ le nombre de d'inversions de σ
3. On appelle signature de la permutation σ que l'on note $sgn\ \sigma$ le nombre $\varepsilon(\sigma) = (-1)^{I(\sigma)}$

Remarque 39 :

On définit ainsi l'application « signature » : $\varepsilon : \mathcal{S}_n \longrightarrow \{-1; +1\}$. Elle dépend de n, mais on ne fait pas apparaître cette dépendance dans la notation ε

10.10.13 Définition de la parité d'une permutation

Soit σ une permutation de $\mathcal{S}_n$

1. On dit que la permutation σ est paire si $\varepsilon(\sigma) = 1$
2. On dit que la permutation σ est impaire si $\varepsilon(\sigma) = -1$

Remarque 40 :

Ceci veut simplement dire que si la permutation est paire, alors le nombre d'inversions de la permutation est un nombre pair, et donc que la permutation est impaire, si le nombre d'inversions de la permutation est un nombre impair

Exemple 21 :

Intéressons nous à $\mathbb{N}_5$ et à $\mathcal{S}_5$ son groupe de permutations. Soit $\sigma \in \mathcal{S}_5$ définie par

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix}$$

Regardons le nombre d'inversions
On peut, tout de suite dire que le couple $(1,2)$ est une inversion, car $\sigma(1) > \sigma(2)$. Plus généralement, comme $\sigma(1) = 5$, nous avons aussi comme inversion les couples $(1,3)$, $(1,4)$ et $(1,5)$
Le couple $(2,3)$ n'est pas une inversion, car $\sigma(2) < \sigma(3)$.
$(2,5)$, $(3,5)$, $(4,5)$ sont des inversions. Il y a donc en tout 7 inversions, et on en déduit que σ est une permutation impaire.

10.10.14 Proposition

Toute transposition est impaire

Démonstration

On considère l'ensemble fini $\mathbb{N}_n$ et σ une transposition de $\mathcal{S}_n$ telle que :

$$\begin{cases} \sigma(h) = k \text{ et } \sigma(k) = h \\ \text{Pour tout } i \in \mathbb{N}_n,\ i \neq h \text{ et } i \neq k\ \sigma(i) = i \end{cases}$$

On suppose $h < k$
Il est alors évident que si $h < i < k$, les couples (h,i) et (i,k) forment des inversions ; de même, le couple (h,k) forme une inversion, et ce sont les seuls qui forment des inversions.

- → Tous les couples (h,i) avec $h+1 \leqslant i \leqslant k$ sont donc des inversions, et il y en a $k-(h+1)+1 = k-h$ telles inversions
- → De même, tous les couples (i,k) avec $h+1 \leqslant i \leqslant k-1$ sont donc des inversions, et il y en a $k-1-(h+1)+1 = k-h-1$ telles inversions

Il y a donc, en tout $2(k-h)-1$ couples d'inversion, c'est à dire un nombre impair d'inversions et donc $\varepsilon(\sigma) = -1$

Remarque 41 :

Calculer la signature à partir du nombre d'inversions s'avère fastidieux dès que n est un tant soit peu grand. Nous allons voir ci-après, une méthode de calcul beaucoup plus aisée qui repose sur des propriétés fondamentales de la signature.

10.10.15 Proposition

Soit $n \in \mathbb{N}^*$. On considère $\mathcal{S}_n$ le groupe de permations de $\mathbb{N}_n$. Alors, pour tout $\sigma \in \mathcal{S}_n$, nous avons :

$$\varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Démonstration

1. σ est une permutation et donc une bijection. Comme $i<j$, c'est à dire $i\neq j$, nous avons $\sigma(i)\neq\sigma(j)$ et donc $\prod_{1\leqslant i<j\leqslant n}(\sigma(i)-\sigma(j))\neq 0$

   De la même manière, comme $i<j$, $i-j<0$ et $\prod_{1\leqslant i<j\leqslant n}(i-j)\neq 0$

2. Pour $1\leqslant i<j\leqslant n$, il existe h et k uniques, avec $1\leqslant h\leqslant n$, $1\leqslant k\leqslant n$ et $h\neq k$ tels que $\sigma(h)=i$ et $\sigma(k)=j$

   Et donc $\prod_{1\leqslant i<j\leqslant n}(i-j)=\prod_{1\leqslant i<j\leqslant n}(\sigma(i)-\sigma(j))$, c'est à dire que

   $$\left|\frac{\prod_{1\leqslant i<j\leqslant n}(\sigma(i)-\sigma(j))}{\prod_{1\leqslant i<j\leqslant n}(i-j)}\right|=1$$

3. D'autre part, nous avons

   $$\prod_{1\leqslant i<j\leqslant n}\frac{\sigma(i)-\sigma(j)}{i-j}=\prod_{\substack{1\leqslant i<j\leqslant n\\ \sigma(i)>\sigma(j)}}\frac{\sigma(i)-\sigma(j)}{i-j}\times\prod_{\substack{1\leqslant i<j\leqslant n\\ \sigma(i)<\sigma(j)}}\frac{\sigma(i)-\sigma(j)}{i-j}$$

   Lorsque $\sigma(i)>\sigma(j)$, le rapport $\frac{\sigma(i)-\sigma(j)}{i-j}<0$ et donc, le nombre de couples (i,j) avec $1\leqslant i<j\leqslant n$ tels que $\sigma(i)>\sigma(j)$ est $I(\sigma)$ le nombre de d'inversions de σ et le signe de $\left(\prod_{1\leqslant i<j\leqslant n}\frac{\sigma(i)-\sigma(j)}{i-j}\right)$ est celui de $(-1)^{I(\sigma)}$ et donc :

   $$\prod_{1\leqslant i<j\leqslant n}\frac{\sigma(i)-\sigma(j)}{i-j}=(-1)^{I(\sigma)}=\varepsilon(\sigma)$$

10.10.16 Proposition

Soit $n\in\mathbb{N}^*$. On considère $\mathcal{S}_n$ le groupe de permations de $\mathbb{N}_n$. Alors, pour tout $\sigma_1\in\mathcal{S}_n$ et tout $\sigma_2\in\mathcal{S}_n$, nous avons :

$$\varepsilon(\sigma_1\circ\sigma_2)=\varepsilon(\sigma_1)\times\varepsilon(\sigma_2)$$

Démonstration

En utilisant 10.10.15, nous avons :

$$\varepsilon(\sigma_1\circ\sigma_2)=\prod_{1\leqslant i<j\leqslant n}\frac{\sigma_1\circ\sigma_2(i)-\sigma_1\circ\sigma_2(j)}{i-j}$$

Nous allons modifier cette expression :

$$\varepsilon(\sigma_1\circ\sigma_2)=\prod_{1\leqslant i<j\leqslant n}\frac{\sigma_1\circ\sigma_2(i)-\sigma_1\circ\sigma_2(j)}{i-j}=\prod_{1\leqslant i<j\leqslant n}\frac{\sigma_1\circ\sigma_2(i)-\sigma_1\circ\sigma_2(j)}{\sigma_2(i)-\sigma_2(j)}\times\prod_{1\leqslant i<j\leqslant n}\frac{\sigma_2(i)-\sigma_2(j)}{i-j}$$

Nous reconnaissons déjà en $\prod_{1\leqslant i<j\leqslant n}\frac{\sigma_2(i)-\sigma_2(j)}{i-j}$, $\varepsilon(\sigma_2)$, la signature de σ_2

Il nous faut donc, maintenant, regarder de manière plus précise $\prod_{1\leqslant i<j\leqslant n}\frac{\sigma_1\circ\sigma_2(i)-\sigma_1\circ\sigma_2(j)}{\sigma_2(i)-\sigma_2(j)}$

σ_2 est une bijection de $\mathbb{N}_n$, et donc, pour chaque $x \in \mathbb{N}_n$ il existe un unique $i \in \mathbb{N}_n$ tel que $\sigma_2(i) = x$ et donc :

$$\prod_{1\leqslant i<j\leqslant n} \frac{\sigma_1\circ\sigma_2(i)-\sigma_1\circ\sigma_2(j)}{\sigma_2(i)-\sigma_2(j)} = \prod_{1\leqslant x<y\leqslant n} \frac{\sigma_1(x)-\sigma_2(y)}{x-y}$$

Où nous avons posé :

→ $\sigma_2(i) = x$ et $\sigma_2(j) = y$ lorsque $\sigma_2(i) < \sigma_2(j)$

→ $\sigma_2(i) = y$ et $\sigma_2(j) = x$ lorsque $\sigma_2(i) > \sigma_2(j)$

Et donc

$$\prod_{1\leqslant i<j\leqslant n} \frac{\sigma_1\circ\sigma_2(i)-\sigma_1\circ\sigma_2(j)}{\sigma_2(i)-\sigma_2(j)} = \prod_{1\leqslant x<y\leqslant n} \frac{\sigma_1(x)-\sigma_2(y)}{x-y} = \varepsilon(\sigma_1)$$

Ainsi $\varepsilon(\sigma_1\circ\sigma_2) = \varepsilon(\sigma_1)\times\varepsilon(\sigma_2)$, ce que nous voulions démontrer

Remarque 42 :

1. La proposition 10.10.16 signifie que la signature d'une permutation **est un morphisme de groupe**

   En effet, $(\{-1;+1\},\times)$ est un groupe multiplicatif de neutre $+1$ et la relation

   $$\varepsilon(\sigma_1\circ\sigma_2) = \varepsilon(\sigma_1)\times\varepsilon(\sigma_2)$$

   pour tout $\sigma_1 \in \mathcal{S}_n$ et tout $\sigma_2 \in \mathcal{S}_n$ définit bien un homomorphisme de groupe.
2. Il est très facile de montrer que, si σ est une permutation de $\mathcal{S}_n$, l'application Φ ainsi définie :

   $$\left\{\begin{array}{ccc} \Phi : \mathbb{N}_n\times\mathbb{N}_n & \longrightarrow & \mathbb{N}_n\times\mathbb{N}_n \\ (i,j) & \longmapsto & \Phi[(i,j)] = (\sigma(i),\sigma(j)) \end{array}\right.$$

   est une bijection
3. Rappelons que la signature d'une transposition est -1 *(Cf 10.10.14)*

10.10.17 Proposition

Soit $n \in \mathbb{N}^*$. On considère $\mathcal{S}_n$ le groupe de permations de $\mathbb{N}_n$.

1. La signature d'une permutation circulaire (ou cycle) de longueur k (ou d'ordre k est $(-1)^{k-1}$
2. Pour $\sigma \in \mathcal{S}_n$, si r est le nombre d'orbites dans la relation d'équivalence modulo σ (comme définie en 10.10.7), alors $\varepsilon(\sigma) = (-1)^{n-r}$

Démonstration

1. D'après le théorème 10.10.11 un cycle de longueur k est le produit de $k-1$ transpositions. Ainsi, si γ est un cycle de longueur k, nous avons :

   $$\gamma = \tau_1\circ\tau_2\circ\cdots\circ\tau_{k-1} \text{ et donc } \varepsilon(\gamma) = \prod_{j=1}^{k-1}\varepsilon(\tau_i) = (-1)^{k-1}$$

2. Soit $\sigma \in \mathcal{S}_n$. Nous considérons donc la relation d'équivalence définie en 10.10.7 à l'aide de σ
   (a) Notons $\mathcal{C}_1,\mathcal{C}_2,\cdots,\mathcal{C}_r$ les r classes d'équivalence *(ou orbites)* modulo cette relation d'équivalence.
   Alors $\bigcup_{k=1}^{r}\mathcal{C}_k = \mathbb{N}_n$ et si $i \neq j$, alors $\mathcal{C}_i\cap\mathcal{C}_j = \emptyset$
   (b) Dans ces orbites, il y a des singletons $\mathcal{C}_j = \{x\}$, c'est à dire des éléments qui sont en fait des points fixes par σ.
   Nous appelons donc $\mathcal{C}_1,\mathcal{C}_2,\cdots,\mathcal{C}_s$ les orbites qui ne sont pas des singletons et $\mathcal{C}_{s+1},\mathcal{C}_{s+2},\cdots,\mathcal{C}_r$ les orbites qui sont des singletons

(c) Pour $\mathcal{C}_j = \left\{x_1^j, x_2^j, \ldots, x_p^j\right\}$, nous notons c_j le cycle $c_j = \left(x_1^j, x_2^j, \ldots, x_p^j\right)$ et $l(c_j)$ la longueur de ce cycle. Notons que $l(c_j) = \text{Card}\,\mathcal{C}_j$.
Nous avons donc $n = l(c_1) + l(c_2) + \cdots + l(c_s) + (r-s)$
Les c_j ainsi construits sont des cycles disjoints tels que $\sigma = c_1 \circ c_2 \circ \cdots \circ c_s$

(d) En utilisant le résultat 10.10.16, nous avons :

$$\begin{aligned}\varepsilon(\sigma) &= \varepsilon(c_1) \times \varepsilon(c_2) \times \cdots \times \varepsilon(c_s)\\ &= (-1)^{l(c_1)-1} \times (-1)^{l(c_2)-1} \times \cdots \times (-1)^{l(c_s)-1}\\ &= (-1)^{l(c_1)+l(c_2)+\cdots+l(c_s)-s}\\ &= (-1)^{n-r} \text{ puisque } n = l(c_1) + l(c_2) + \cdots + l(c_s) + (r-s)\end{aligned}$$

10.10.18 Théorème

Soit $n \in \mathbb{N}$ tel que $n > 1$ et A_n est l'ensemble des permutations paires de $\mathbb{N}_n$

1. A_n est un sous groupe distingué de $\mathcal{S}_n$ contenant $\dfrac{n!}{2}$ éléments
2. A_n s'appelle sous-groupe alterné d'ordre n

Démonstration

1. A_n est un sous-groupe distingué de $\mathcal{S}_n$
Si nous considérons
$$\left\{\begin{array}{ccc}\varepsilon : \mathcal{S}_n & \longrightarrow & \{-1;+1\}\\ \sigma & \longmapsto & \varepsilon(\sigma)\end{array}\right.$$
ε est un homomorphisme de groupe de noyau $\ker\varepsilon = A_n$. Comme le noyau d'un homomorphisme est un sous-groupe distingué, A_n est un sous groupe distingué de $\mathcal{S}_n$

2. Card $A_n = \dfrac{n!}{2}$
Dans la relation d'équivalence modulo A_n, toutes les classes d'équivalence ont même nombre d'éléments ; et dans cette relation, les 2 classes sont définies par A_n et τA_n où τ est une transposition de $\mathcal{S}_n$.
Comme $A_n \cup \tau A_n = \mathcal{S}_n$ et que $A_n \cap \tau A_n = \emptyset$, 2Card $A_n = n!$, c'est à dire Card $A_n = \dfrac{n!}{2}$

Une autre démonstration, ou idée de démonstration qui rejoint ce qui a été écrit ci-dessus, est de considérer l'application Ψ de A_n dans $\mathcal{S}_n \setminus A_n$ définie par :
$$\left\{\begin{array}{ccc}\Psi : A_n & \longrightarrow & \mathcal{S}_n \setminus A_n\\ \sigma & \longmapsto & \Psi(\sigma) = \tau\sigma\end{array}\right.$$
Où τ est une transposition de $\mathcal{S}_n$. Il est facile de démontrer que Ψ est bijective (donc Card A_n = Card $(\mathcal{S}_n \setminus A_n)$) et que $\mathcal{S}_n = A_n \cup (\mathcal{S}_n \setminus A_n)$ et donc Card $A_n = \dfrac{n!}{2}$
(En fait, c'est une recopie de la démonstration du théorème de Lagrange et A_n est un sous-groupe distingué d'indice 2)