2

Permutations d'un ensemble fini, groupe symétrique. Applications

E est un ensemble ayant au moins deux éléments et Id_E est l'application identité sur E. On note $\text{card}(E)$ le cardinal de E.

2.1 Permutations, cycles et transpositions

On note $\mathcal{S}(E)$ (ou parfois $\mathfrak{S}(E)$) l'ensemble des bijections de E sur lui même.

Théorème 2.1 *$\mathcal{S}(E)$ est un groupe pour la composition des applications.*

Démonstration. C'est évident. ∎

Définition 2.1 *Le groupe $\mathcal{S}(E)$ est appelé groupe des permutations de E.*

Remarque 2.1 *Dans le cas où E est réduit à un élément, on peut quand même définir $\mathcal{S}(E)$ et il est réduit à $\{Id_E\}$.*

Pour $E = \{1, 2, \cdots, n\} \subset \mathbb{N}$, on note $\mathcal{S}_n$ le groupe $\mathcal{S}(E)$ et on l'appelle groupe symétrique à n éléments.

Le groupe symétrique joue un rôle important dans l'étude des polynômes symétriques, l'étude de la résolubilité des équations polynomiales et en algèbre multilinéaire.

Pour toute permutation $\sigma \in \mathcal{S}_n$, on note :

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

pour signifier que σ est la bijection $\sigma : k \in E \mapsto \sigma(k)$.

Avec cette notation, on calcule facilement la composée et l'inverse d'une permutation de $\mathcal{S}_n$. Par exemple, on a :

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

et :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$$

Pour toute permutation $\sigma \in \mathcal{S}(E)$ et tout entier relatif r, σ^r est la permutation de E définie par :

$$\sigma^r = \begin{cases} Id_E \text{ si } r = 0 \\ \sigma \circ \cdots \circ \sigma \ (r \text{ fois}) \text{si } r \geq 1 \\ (\sigma^{-r})^{-1} \text{ si } r \leq -1 \end{cases}$$

Définition 2.2 *Soit r un entier compris entre 2 et $\operatorname{card}(E)$. On appelle cycle d'ordre r (ou r-cycle), toute permutation $\sigma \in \mathcal{S}(E)$ qui permute circulairement r éléments de E et laisse fixe les autres, c'est-à-dire qu'il existe une partie $\{x_1, \cdots, x_r\}$ de E telle que :*

$$\begin{cases} \forall k \in \{1, \cdots, r-1\}, \ \sigma(x_k) = x_{k+1} \\ \sigma(x_r) = x_1 \\ \forall x \in E \setminus \{x_1, \cdots, x_r\}, \ \sigma(x) = x \end{cases}$$

On notera :

$$\sigma = (x_1, \cdots, x_r)$$

un tel cycle et on dit que $\{x_1, \cdots, x_r\}$ est le support de σ.

Remarque 2.2 *Les r permutations circulaires :*

$$(x_1, x_2, \cdots, x_r), \ (x_2, x_3, \cdots, x_r, x_1), \ , (x_r, x_1, \cdots, x_{r-1})$$

définissent le même r-cycle.

Exercice 2.1 *On suppose que $\operatorname{card}(E) = n \geq 2$. Montrer que, pour $2 \leq r \leq n$, dans $\mathcal{S}(E)$ il y a $C_n^r (r-1)!$ cycles d'ordre r distincts.*

Solution 2.1 *Pour définir un r-cycle, on choisit d'abord une liste $(x_1, \cdots, x_r)$ dans E, il y a $A_n^r = r! C_n^r = \dfrac{n!}{(n-r)!}$ possibilités. Pour un tel choix de la partie $\{x_1, \cdots, x_r\}$ de E, les r permutations circulaires :*

$$(x_1, \cdots, x_r), \ (x_2, x_3, \cdots, x_r, x_1), \ , (x_r, x_1, \cdots, x_{r-1})$$

donnent le même cycle, les autres permutations donnant des cycles différents, il y a donc $\dfrac{A_n^r}{r} = (r-1)! C_n^r$ possibilités.

Remarque 2.3 *L'inverse d'un r-cycle est un r-cycle de même support. Précisément, on a :*

$$(x_1, x_2, \cdots, x_r)^{-1} = (x_r, x_{r-1}, \cdots, x_1)$$

En effet, en notant $x_0 = x_r$, on a :

$$\begin{cases} \sigma(x_{k-1}) = x_k \ (1 \leq k \leq r) \\ \sigma(x) = x \ si \ x \in E \setminus \{x_1, \cdots, x_r\} \end{cases} \Leftrightarrow \begin{cases} \sigma^{-1}(x_k) = x_{k-1} \ (1 \leq k \leq r) \\ \sigma^{-1}(x) = x \ si \ x \in E \setminus \{x_1, \cdots, x_r\} \end{cases}$$

Nous verrons un peu plus loin que le produit de deux cycles n'est pas nécessairement un cycle.

Définition 2.3 *On appelle transposition, un cycle d'ordre 2.*

On peut remarquer qu'une transposition τ est d'ordre 2 dans le groupe $\mathcal{S}(E)$, c'est-à-dire que $\tau \neq Id_E$ et $\tau^2 = Id_E$. On a donc $\tau^{-1} = \tau$.

Plus généralement, on a le résultat suivant.

Lemme 2.1 *Un r-cycle est d'ordre r dans le groupe $(\mathcal{S}(E), \circ)$.*

Démonstration. Soit $\sigma = (x_1, \cdots, x_r)$ un r-cycle avec $r \geq 2$.

Pour tout entier k compris entre 1 et r, on a :

$$x_k = \sigma^{k-1}(x_1)$$

En effet, c'est vrai pour $k = 1$ et supposant le résultat acquis pour $1 \leq k-1 \leq r-1$, on a :

$$x_k = \sigma(x_{k-1}) = \sigma\left(\sigma^{k-2}(x_1)\right) = \sigma^{k-1}(x_1)$$

Il en résulte que $\sigma^r(x_k) = x_k$ pour tout k compris entre 1 et r. En effet, on a :

$$\begin{aligned}\sigma^r(x_k) &= \sigma^r\left(\sigma^{k-1}(x_1)\right) = \sigma^{k-1}(\sigma^r(x_1)) \\ &= \sigma^{k-1}\left(\sigma\left(\sigma^{r-1}(x_1)\right)\right) = \sigma^{k-1}(\sigma(x_r)) \\ &= \sigma^{k-1}(x_1) = x_k\end{aligned}$$

Comme $\sigma(x) = x$, pour $x \in E \setminus \{x_1, \cdots, x_r\}$, on en déduit que $\sigma^r = Id_E$.

Enfin avec $\sigma^{k-1}(x_1) = x_k \neq x_1$, pour $2 \leq k_r$, on déduit que $\sigma^{k-1} \neq Id_E$ et σ est d'ordre r. ■

On déduit du résultat précédent que l'inverse d'un r-cycle σ est le r-cycle σ^{r-1}.

Exercice 2.2 *Montrer que si l'ensemble E a au moins 3 éléments, alors le groupe $\mathcal{S}(E)$ n'est pas commutatif (voir aussi le lemme 2.3).*

Solution 2.2 *Soient x_1, x_2, x_3 distincts dans E et $\tau_1 = (x_1, x_2), \tau_2 = (x_2, x_3)$. On a $\tau_2 \circ \tau_1(x_1) = x_3$ et $\tau_1 \circ \tau_2(x_1) = x_2 \neq x_3$. Donc $\tau_2 \circ \tau_1 \neq \tau_1 \circ \tau_2$ et $\mathcal{S}(E)$ n'est pas commutatif.*

Lemme 2.2 *Soit r un entier compris entre 2 et* $\operatorname{card}(E)$.
Le conjugué dans $\mathcal{S}(E)$ d'un r-cycle est encore un r-cycle. Précisément, pour tout r-cycle $\sigma = (x_1, x_2, \cdots, x_r)$ et toute permutation τ, on a :

$$\tau \circ \sigma \circ \tau^{-1} = (\tau(x_1), \tau(x_2), \cdots, \tau(x_r))$$

Réciproquement, deux cycles de même longueur sont conjugués dans $\mathcal{S}(E)$, c'est-à-dire que si σ et σ' sont deux cycles de même longueur r-cycles, il existe alors une permutation τ telle que $\sigma' = \tau \circ \sigma \circ \tau^{-1}$.

Démonstration. En notant $\sigma'' = (\tau(x_1), \tau(x_2), \cdots, \tau(x_r))$, il s'agit de montrer que $\tau \circ \sigma = \sigma'' \circ \tau$.

Pour $x \in E \setminus \{x_1, \cdots, x_r\}$, on a $\sigma(x) = x$ et $\tau(x) \in E \setminus \{\tau(x_1), \cdots, \tau(x_r)\}$, ce qui donne :

$$\tau \circ \sigma(x) = \tau(x) = \sigma''(\tau(x)) = \sigma'' \circ \tau(x)$$

Si x est l'un des x_k, on a alors :

$$\tau \circ \sigma(x) = \tau(\sigma(x_k)) = \tau(x_{k+1})$$

en notant $x_{r+1} = x_1$ et :

$$\sigma'' \circ \tau(x) = \sigma''(\tau(x_k)) = \tau(x_{k+1})$$

On a donc bien $\tau \circ \sigma = \sigma'' \circ \tau$, soit $\tau \circ \sigma \circ \tau^{-1} = \sigma''$.

Soient $\sigma = (x_1, x_2, \cdots, x_r)$ et $\sigma' = (x'_1, x'_2, \cdots, x'_r)$ deux r-cycles. En se donnant une bijection φ de $E \setminus \{x_1, \cdots, x_r\}$ sur $E \setminus \{x'_1, \cdots, x'_r\}$, on définit une permutation τ de E en posant $\tau(x_k) = x'_k$ pour $k = 1, \cdots, r$ et $\tau(x) = \varphi(x)$ pour $x \in E \setminus \{x_1, \cdots, x_r\}$ et on a :

$$\tau \circ \sigma \circ \tau^{-1} = (\tau(x_1), \tau(x_2), \cdots, \tau(x_r)) = (x'_1, x'_2, \cdots, x'_r) = \sigma'$$

■

Le résultat précédent se traduit en disant que, pour tout entier r compris entre 2 et $\text{card}(E)$, le groupe $\mathcal{S}(E)$ agit par conjugaison de façon transitive sur l'ensemble des r-cycles.

En faisant agir $\mathcal{S}(E)$ par conjugaison sur l'ensemble des cycles, l'orbite d'un r-cycle pour cette action est l'ensemble de tous les r-cycles et son cardinal est $\dfrac{A_n^r}{r} = (r-1)!C_n^r$.

On désigne par $Z(\mathcal{S}(E))$ le centre du groupe de $\mathcal{S}(E)$, c'est-à-dire l'ensemble des éléments de $\mathcal{S}(E)$ qui commutent à tous les autres éléments de $\mathcal{S}(E)$.

Lemme 2.3 *On a :*

$$Z(\mathcal{S}(E)) = \begin{cases} \mathcal{S}(E) & \text{si } \text{card}(E) = 2 \\ \{Id_E\} & \text{si } \text{card}(E) \geq 3 \end{cases}$$

Démonstration. Si $\text{card}(E) = 2$, le groupe $\mathcal{S}(E)$ est commoutatif et $Z(\mathcal{S}(E)) = \mathcal{S}(E)$.

On suppose que $\text{card}(E) \geq 3$ et on se donne σ dans $Z(\mathcal{S}(E))$. Pour $x \neq y$ dans E, on a :

$$(\sigma(x), \sigma(y)) = \sigma(x, y)\sigma^{-1} = (x, y)\sigma\sigma^{-1} = (x, y)$$

et donc $\sigma\{x, y\} = \{x, y\}$. Pour $\text{card}(E) \geq 3$, on peut trouver, pour tout $x \in E$ deux éléments $y \neq z$ distincts de x et avec $\{x\} = \{x, y\} \cap \{x, z\}$, on déduit que :

$$\begin{aligned} \{\sigma(x)\} &= \sigma(\{x\}) = \sigma(\{x, y\} \cap \{x, z\}) \\ &= \sigma(\{x, y\}) \cap \sigma(\{x, z\}) = \{x, y\} \cap \{x, z\} = \{x\} \end{aligned}$$

ce qui donne $\sigma(x) = x$. On a donc $\sigma = Id_E$.

Le centre de $\mathcal{S}(E)$ est donc réduit à $\{Id\}$.

On retrouve ainsi le fait que $\mathcal{S}(E)$ n'est pas commutatif pour $n \geq 3$. ■

Exercice 2.3 *On suppose que* $\text{card}(E) \geq 3$. *Montrer que pour toute permutation* $\sigma \in \mathcal{S}(E) \setminus \{Id_E\}$, *il existe une transposition qui ne commute pas à* σ. *On a donc* $\sigma \notin Z(\mathcal{S}(E))$ *et on retrouve ainsi le fait que* $Z(\mathcal{S}(E)) = \{Id_E\}$.

Solution 2.3 *Si* $\sigma \in \mathcal{S}(E) \setminus \{Id\}$, *il existe* $x \in E$ *tel que* $y = \sigma(x) \neq x$. *On se donne* $z \in E \setminus \{x, y\}$ *(*E *a au moins* 3 *éléments) et* τ *est la transposition* $\tau = (y, z)$. *Avec :*

$$\sigma\tau(x) = \sigma(x) = y \text{ et } \tau\sigma(x) = \tau(y) = z \neq y$$

on déduit que $\sigma\tau \neq \tau\sigma$ *et* $\sigma \notin Z(\mathcal{S}(E))$.

2.2 Les groupes symétriques $\mathcal{S}_n$

Théorème 2.2 *Si* E, F *sont deux ensembles non vides et* φ *une bijection de* E *sur* F, *alors les groupes* $\mathcal{S}(E)$ *et* $\mathcal{S}(F)$ *sont isomorphes.*

Démonstration. L'application :

$$\begin{array}{rccc} \psi: & \mathcal{S}(E) & \to & \mathcal{S}(F) \\ & \sigma & \mapsto & \varphi\circ\sigma\circ\varphi^{-1} \end{array}$$

est un isomorphisme de groupes.

En effet, pour $\sigma\in\mathcal{S}(E)$, $\psi(\sigma)\in\mathcal{S}(F)$ comme composée de bijections et pour σ_1,σ_2 dans $\mathcal{S}(E)$, on a :

$$\begin{aligned}\psi(\sigma_1\circ\sigma_2) &= \varphi\circ\sigma_1\circ\sigma_2\circ\varphi^{-1} = \left(\varphi\circ\sigma_1\circ\varphi^{-1}\right)\circ\left(\varphi\circ\sigma_2\circ\varphi^{-1}\right)\\ &= \psi(\sigma_1)\circ\psi(\sigma_2)\end{aligned}$$

c'est-à-dire que ψ est un morphisme de groupes de $\mathcal{S}(E)$ dans $\mathcal{S}(F)$.

Si $\sigma\in\ker(\psi)$, on a alors $\varphi\circ\sigma\circ\varphi^{-1}=Id_F$ et $\sigma=\varphi^{-1}\circ Id_F\circ\varphi=Id_E$, donc ψ est injective.

Pour $\sigma'\in\mathcal{S}(F)$, l'application $\sigma=\varphi^{-1}\circ\sigma'\circ\varphi$ est dans $\mathcal{S}(E)$ et on a $\psi(\sigma)=\sigma'$, donc ψ est surjective. ■

Donc tout groupe de permutations d'un ensemble E à n éléments est isomorphe au groupe symétrique $\mathcal{S}_n$ des permutations de $\{1,2,\cdots,n\}$.

On rappelle que deux ensembles finis qui sont en bijection ont le même nombre d'éléments.

Théorème 2.3 *Pour tout entier $n\geq 1$ et tout ensemble E de cardinal n, on a* $\operatorname{card}(\mathcal{S}(E))=n!$

Démonstration. Une démonstration rapide peut se faire comme suit. Si $E=\{x_1,\cdots,x_n\}$ et $\sigma\in\mathcal{S}(E)$, il y a n possibilités pour $\sigma(x_1)$, puis, $\sigma(x_1)$ étant choisi, il reste $n-1$ possibilités pour $\sigma(x_2)$, $\cdots$, et enfin 1 possibilité pour $\sigma(x_n)$, ce qui donne $n!$ possibilités pour σ.

Une démonstration plus rigoureuse peut se faire par récurrence sur $n\geq 1$.

Pour $n=1$ c'est clair puisque $\mathcal{S}(E)=\{Id_E\}$.

Supposons le résultat acquis pour les ensembles à $n-1\geq 1$ éléments et soit $E=\{x_1,\cdots,x_n\}$ un ensemble à $n\geq 2$ éléments.

On désigne par H le sous-ensemble de $\mathcal{S}(E)$ formé des permutations de E qui laissent stable x_n. On vérifie facilement H est un sous-groupe de $\mathcal{S}(E)$.

En effet, on a $Id\in H$ et pour σ_1,σ_2 dans H, $\sigma_1\sigma_2^{-1}(x_n)=\sigma_1(x_n)=x_n$, donc $\sigma_1\sigma_2^{-1}\in H$ et H est un sous-groupe de $\mathcal{S}(E)$.

L'application qui associe à $\sigma\in H$ sa restriction à $F=\{x_1,\cdots,x_{n-1}\}$ réalise alors un isomorphisme de H sur $\mathcal{S}(F)$.

En désignant, pour tout entier k compris entre 1 et $n-1$, par τ_k la permutation $\tau_k=(x_k,x_n)$, on a $\mathcal{S}(E)/H=\{\tau_1H,\cdots,\tau_{n-1}H,H\}$.

En effet, pour tout $\sigma\in\mathcal{S}(E)$, il existe $k\in\{1,\cdots,n\}$ tel que $\sigma(x_n)=x_k$ et en notant $\tau_n=Id$, on a $\tau_k^{-1}\sigma(x_n)=\tau_k^{-1}(x_k)=x_n$, donc $\tau_k^{-1}\sigma\in H$ et $\sigma H=\tau_kH$. On a donc $\mathcal{S}(E)/H=\{\tau_1H,\cdots,\tau_nH\}$ avec $\tau_jH\neq\tau_kH$ pour $k\neq j$ (pour $1\leq k<j\leq n$, on a $\tau_k^{-1}\tau_j(x_n)=\tau_k(x_j)\neq x_n$, donc $\tau_k^{-1}\tau_j\notin H$).

En utilisant l'hypothèse de récurrence, on en déduit que :

$$\begin{aligned}\operatorname{card}(\mathcal{S}(E)) &= \operatorname{card}(\mathcal{S}(E)/H)\operatorname{card}(H) = \operatorname{card}(\mathcal{S}(E)/H)\operatorname{card}(\mathcal{S}(F))\\ &= n\cdot(n-1)! = n!\end{aligned}$$

■

On peut aussi montrer le théorème précédent en utilisant l'action naturelle de $\mathcal{S}(E)$ sur E (exercice 3.3).

Exemple 2.1 *Pour* $E = \{1, 2\}$, $\mathcal{S}_2$ *est formé des deux éléments :*

$$Id = \text{ et } \tau = (1, 2)$$

et c'est un groupe commutatif. Ce groupe est en fait cyclique engendré par τ *d'ordre* 2, *il est donc isomorphe à* $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$.

Exercice 2.4 *Montrer que le groupe des isométries du plan affine euclidien qui conservent les sommets d'un vrai triangle isocèle non équilatéral est isomorphe à* $\mathcal{S}_2$.

Solution 2.4 *On note* $\mathcal{P}$ *le plan affine euclidien et on se donne un vrai triangle isocèle non équilatéral* T *de sommets* A_1, A_2, A_3 *avec* $A_1A_2 = A_1A_3$ *(figure 2.1).On note* $Is(T)$ *le groupe*

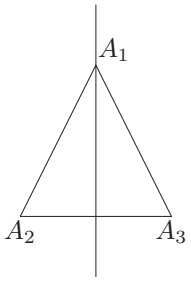

FIG. 2.1 –

des isométries de $\mathcal{P}$ *qui conservent* $E = \{A_1, A_2, A_3\}$.
Soit $\varphi \in Is(T)$. *Par conservation des barycentres, on a* $\varphi(O) = O$, *en désignant par* O *le centre de gravité du triangle (l'isobarycentre de* E*) et* $\varphi([A_2A_3])$ *est un coté du triangle de même longueur que* $[A_2A_3]$, *c'est donc* $[A_2A_3]$ *puisque le triangle est non équilatéral et isocèle en* A_1. *On a donc* $\varphi(\{A_2A_3\}) = \{A_2, A_3\}$ *et nécessairement* $\varphi(A_1) = A_1$. *Si* $\varphi(A_2) = A_2$, *alors* $\varphi = Id$ *puisque ces deux applications coïncident sur le repère affine* (O, A_1, A_2). *Si* $\varphi(A_2) = A_3$, *alors* φ *est la réflexion* σ *d'axe* (OA_1), *la médiatrice de* $[A_2A_3]$, *puisque ces deux applications coïncident sur le repère affine* (O, A_1, A_2). *On a donc* $Is(T) = \{Id, \sigma\} = \mathcal{S}(\{A_2, A_3\})$ *qui est isomorphe à* $\mathcal{S}_2$.

Exemple 2.2 $\mathcal{S}_3$ *est formé des six éléments :*

$$Id,\ \tau_1 = (1, 2),\ \tau_2 = (1, 3),\ \tau_3 = (2, 3)$$

$$\gamma_1 = (1, 2, 3) \text{ et } \gamma_2 = \gamma_1^2 = (1, 3, 2).$$

Ce groupe n'est pas commutatif puisque :

$$\tau_1\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \gamma_2 \text{ et } \tau_2\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \gamma_1 \neq \gamma_2$$

En remarquant que :

$$\gamma_2 = \gamma_1^2,\ \tau_2 = \tau_1\gamma_2 = \tau_1\gamma_1^2,\ \tau_3 = \tau_1\gamma_1$$

on déduit que :

$$\begin{aligned} \mathcal{S}_3 &= \left\{Id, \tau_1, \gamma_1, \gamma_1^2, \tau_1\gamma_1, \tau_1\gamma_1^2\right\} = \langle \tau_1, \gamma_1 \rangle \\ &= \left\{\tau_1^i\gamma_1^j \ ;\ i = 0, 1 \text{ et } j = 0, 1, 2\right\} \end{aligned}$$

Exercice 2.5 *Montrer que $\mathcal{S}_3$ est, à isomorphisme près, le seul groupe d'ordre 6 non commutatif.*

Solution 2.5 *Soit G un groupe non commutatif d'ordre 6.*
Le théorème de Cauchy nous dit qu'on peut trouver dans G, un élément g d'ordre 2 et un élément h d'ordre 3 (ce qui peut se montrer ici directement).
On vérifie alors que

$$G = \left\{g^i h^j \ ; \ i = 0,1 \text{ et } j = 0,1,2\right\}$$

Pour ce faire, il suffit de vérifier que les $g^i h^j$ sont deux à deux distincts.
Si $g^i h^j = g^{i'} h^{j'}$, on a alors $g^{i-i'} = h^{j'-j} \in \langle g\rangle \cap \langle h\rangle = \{1\}$ ($\langle g\rangle \cap \langle h\rangle$ étant contenu dans $\langle g\rangle$ d'ordre 2 et dans $\langle h\rangle$ d'ordre 3 a un ordre qui divise 2 et 3, cet ordre est donc 1). On a donc $g^{i-i'} = h^{j'-j} = 1$, donc 2 divise $i - i' \in \{-1, 0, 1\}$ et 3 divise $j - j' \in \{-2, -1, 0, 1, 2\}$, ce qui entraîne $i = i'$ et $j = j'$.
L'application φ de G dans $\mathcal{S}_3$ définie par :

$$\forall\, (i,j) \in \{0,1\} \times (0,1,2)\,,\ \varphi\left(g^i h^j\right) = \tau_1^i \gamma_1^j$$

réalise alors un isomorphisme de groupes de G sur $\mathcal{S}_3$.
En effet, cette application est bijective puisque les applications $(i,j) \mapsto g^i h^j$ et $(i,j) \mapsto \tau_1^i \gamma_1^j$ sont bijectives de $\{0,1\} \times (0,1,2)$ sur G et $\mathcal{S}_3$ respectivement.
Le fait que c'est un morphisme de groupes provient des égalités :

$$hg = gh^2 \text{ et } h^2 g = gh$$

dans G et $\mathcal{S}_3$ (avec $(g,h) = (\tau_1, \gamma_1)$ dans ce cas).
En effet, on a $hg \notin \{1_G, g, h, h^2, gh\}$ (comme g est d'ordre 2 et h d'ordre 3, $hg = 1_G$ donne $h = g$, $hg = g$ donne $h = 1_G$, $hg = h$ donne $g = 1_G$, $hg = h^2$ donne $g = 1_G$ et $hg = gh$ n'est pas possible car G est non commutatif), donc $hg = gh^2$ et $h^2 g = hgh^2 = gh^4 = gh$.
Tenant compte de $\varphi(g^i h^j) = \tau_1^i \gamma_1^j$ pour tout $(i,j) \in \mathbb{Z}^2$, il en résulte que pour $g^i h^j$, $g^{i'} h^{j'}$ dans G, on a :

$$g^i h^j \cdot g^{i'} h^{j'} = \begin{cases} g^i h^{j+j'} \text{ si } i' = 0 \\ g^{i+1} h^{j'} \text{ si } i' = 1 \text{ et } j = 0 \\ g^{i+1} h^{j'+2} \text{ si } i' = 1 \text{ et } j = 1 \\ g^{i+1} h^{j'+1} \text{ si } i' = 1 \text{ et } j = 2 \end{cases}$$

et :

$$\varphi\left(g^i h^j \cdot g^{i'} h^{j'}\right) = \begin{cases} \tau_1^i \gamma_1^{j+j'} = \tau_1^i \gamma_1^j \cdot \gamma_1^{j'} \text{ si } i' = 0 \\ \tau_1^{i+1} \gamma_1^{j'} = \tau_1^i \cdot \tau_1 \gamma_1^{j'} \text{ si } i' = 1 \text{ et } j = 0 \\ \tau_1^{i+1} \gamma_1^{j'+2} = \tau_1^i \tau_1 \gamma_1^2 \gamma_1^{j'} = \tau_1^i \gamma_1 \cdot \tau_1 \gamma_1^{j'} \text{ si } i' = 1 \text{ et } j = 1 \\ \tau_1^{i+1} \gamma_1^{j'+1} = \tau_1^i \tau_1 \gamma_1 \gamma_1^{j'} = \tau_1^i \gamma_1^2 \cdot \tau_1 \gamma_1^{j'} \text{ si } i' = 1 \text{ et } j = 2 \end{cases}$$

$$= \begin{cases} \varphi(g^i h^j)\, \varphi\left(h^{j'}\right) \text{ si } i' = 0 \\ \varphi(g^i)\, \varphi\left(gh^{j'}\right) \text{ si } i' = 1 \text{ et } j = 0 \\ \varphi(g^i h)\, \varphi\left(gh^{j'}\right) \text{ si } i' = 1 \text{ et } j = 1 \\ \varphi(g^i h^2)\, \varphi\left(gh^{j'}\right) \text{ si } i' = 1 \text{ et } j = 2 \end{cases} = \varphi\left(g^i h^j\right) \varphi\left(g^{i'} h^{j'}\right)$$

Remarque 2.4 *On peut se passer du théorème de Cauchy dans l'exercice précédent.*
Comme G est bon commutatif, il n'y a pas d'élément d'ordre 6 (sinon G est cyclique).
Si tous les éléments de $G \setminus \{1_G\}$ sont d'ordre 2, le groupe est alors commutatif. Il existe donc un élément d'ordre 3.

Si tous les éléments de $G \setminus \{1_G\}$ *sont d'ordre* 3, *on a alors* $g \neq g^{-1}$ *pour tout* $g \neq 1_G$ *et* $G \setminus \{1_G\} = \bigcup_{g \neq e} \{g, g^{-1}\}$ *serait de cardinal pair, ce qui est absurde. Il existe donc dans* $G \setminus \{1_G\}$ *au moins un élément d'ordre* 2.
En fait, de manière plus général, un groupe d'ordre $2n$ *avec* $n \geq 1$ *a au moins un élément d'ordre* 2. *En effet, pour* $n = 1$, *c'est clair et pour* $n \geq 2$, *s'il n'y a pas d'élément d'ordre* 2, *on a alors* $g \neq g^{-1}$ *pour tout* $g \neq 1_G$ *et* $G \setminus \{1_G\} = \bigcup_{g \neq e} \{g, g^{-1}\}$ *serait de cardinal pair, ce qui est en contradiction avec* $\text{card}(G \setminus \{1_G\}) = 2n - 1$.

Exercice 2.6 *Montrer que le groupe des isométries du plan affine euclidien qui conservent les sommets d'un vrai triangle équilatéral est isomorphe à* $\mathcal{S}_3$.

Solution 2.6 *On note* $\mathcal{P}$ *le plan affine euclidien, on se donne un vrai triangle équilatéral* T *de sommets* A_1, A_2, A_3, *et* $Is(T)$ *est le groupe des isométries de* $\mathcal{P}$ *qui conservent les sommets de ce triangle.*
En désignant par O *l'isobarycentre de* $E = \{A_1, A_2, A_3\}$, *on a* $A_k = \rho(A_{k-1})$ *pour* $k = 2, 3$ *où* ρ *est la rotation de centre* 0 *et de mesure d'angle égale à* $\frac{2\pi}{3}$. *Donc* $Is(T)$ *contient* $\langle \rho \rangle$ *qui est d'ordre* 3.
L'application Φ *qui associe à* $\varphi \in Is(T)$ *associe la permutation* $\sigma = \begin{pmatrix} A_1 & A_2 & A_3 \\ \varphi(A_1) & \varphi(A_2) & \varphi(A_3) \end{pmatrix}$ *réalise un morphisme de groupes de* $Is(T)$ *dans* $\mathcal{S}(E)$. *En effet, pour* φ, ψ *dans* $Is(T)$ *et* $k = 1, 2, 3$, *on a :*

$$\Phi(\varphi \circ \psi)(A_k) = (\varphi \circ \psi)(A_k) = \varphi(\psi(A_k)) = \Phi(\varphi) \circ \Phi(\psi)(A_k)$$

et comme (A_1, A_2, A_3) *est un repère affine de* E, *ce morphisme est injectif (deux applications affines qui coïncident sur un repère affine sont identiques). Il en résulte que* $Is(T)$ *est isomorphe à un sous-groupe de* $\mathcal{S}_3$ *et il est d'ordre* 3 *ou* 6.
La réflexion d'axe la médiatrice de l'un des cotés étant aussi dans $Is(T)$, *on a au moins* 4 *éléments dans* $Is(T)$ *et ce groupe est nécessairement d'ordre* 6. *Il est donc isomorphe à* $\mathcal{S}_3$.
On peut aussi dire que le groupe $Is(T)$ *contient les trois réflexions par rapport aux médiatrices et comme ces réflexions ont pour image par* Φ *les trois transpositions* (A_1, A_2), (A_1, A_3) *et* (A_2, A_3) *qui engendrent* $\mathcal{S}(E)$ *(voir plus loin), on en déduit que* $s(T)$ *est isomorphe à* $\mathcal{S}(E)$, *donc à* $\mathcal{S}_3$.

2.3 Support et orbites d'une permutation

Définition 2.4 *Le support d'une permutation* $\sigma \in \mathcal{S}(E)$ *est le complémentaire dans* E *de l'ensemble de ses points fixes, soit l'ensemble :*

$$\text{Supp}(\sigma) = \{x \in E \mid \sigma(x) \neq x\}$$

Remarque 2.5 Id_E *est l'unique permutation de support vide.*

Remarque 2.6 *Le support d'un cycle* $\sigma = (x_1, x_2, \cdots, x_r)$ *est* $\{x_1, x_2, \cdots, x_r\}$.

Théorème 2.4 *Soient* σ, σ' *dans* $\mathcal{S}(E)$.

1. $\sigma(\text{Supp}(\sigma)) = \text{Supp}(\sigma)$.

2. $\mathrm{Supp}(\sigma) = \mathrm{Supp}(\sigma^{-1})$.
3. *Pour tout* $r \in \mathbb{Z}$, *on a* $\mathrm{Supp}(\sigma^r) \subset \mathrm{Supp}(\sigma)$.
4. *Si* $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\sigma') = \emptyset$, *alors* $\sigma \circ \sigma' = \sigma' \circ \sigma$.

Démonstration.

1. Soit $x \in \mathrm{Supp}(\sigma)$. Comme σ est injective, de $\sigma(x) \neq x$ on déduit que $\sigma(\sigma(x)) \neq \sigma(x)$ et $\sigma(x) \in \mathrm{Supp}(\sigma)$. On a donc $\sigma(\mathrm{Supp}(\sigma)) \subset \mathrm{Supp}(\sigma)$ (dans le cas où E est fini, on a l'égalité puisque ces ensembles ont le même nombre d'éléments). Comme σ est surjective, tout $x \in \mathrm{Supp}(\sigma)$ s'écrit $x = \sigma(x')$ et $\sigma(x) = \sigma(\sigma(x')) \neq x = \sigma(x')$ impose $\sigma(x') \neq x'$, donc $x' \in \mathrm{Supp}(\sigma)$ et $x \in \sigma(\mathrm{Supp}(\sigma))$. On a donc $\mathrm{Supp}(\sigma) \subset \sigma(\mathrm{Supp}(\sigma))$ et $\sigma(\mathrm{Supp}(\sigma)) = \mathrm{Supp}(\sigma)$.
2. De $\sigma(x) = x$ équivalent à $x = \sigma^{-1}(x)$, on déduit que $x \in \mathrm{Supp}(\sigma)$ si, et seulement si, $x \in \mathrm{Supp}(\sigma^{-1})$ et donc $\mathrm{Supp}(\sigma) = \mathrm{Supp}(\sigma^{-1})$.
3. L'égalité $\sigma(x) = x$ entraîne $\sigma^r(x) = x$ pour tout $r \in \mathbb{Z}$, donc $\sigma^r(x) \neq x$ entraîne $\sigma(x) \neq x$ et $\mathrm{Supp}(\sigma^r) \subset \mathrm{Supp}(\sigma)$.
4. Soient σ, σ' telles que $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\sigma') = \emptyset$ et $x \in E$.
   Si $\sigma(x) = x = \sigma'(x)$, on a alors $\sigma' \circ \sigma(x) = \sigma'(x) = x = \sigma(x) = \sigma \circ \sigma'(x)$.
   Si $x \in \mathrm{Supp}(\sigma)$, alors $x \notin \mathrm{Supp}(\sigma')$ et $\sigma'(x) = x$, donc $\sigma \circ \sigma'(x) = \sigma(x)$. Mais on a aussi $\sigma(x) \in \mathrm{Supp}(\sigma)$, donc $\sigma(x) \notin \mathrm{Supp}(\sigma')$ et $\sigma' \circ \sigma(x) = \sigma(x) = \sigma \circ \sigma'(x)$.
   De manière analogue, on vérifie que $\sigma' \circ \sigma(x) = \sigma'(x) = \sigma \circ \sigma'(x)$ pour tout $x \in \mathrm{Supp}(\sigma')$ (on permute les rôles de σ et σ').
   On a donc $\sigma \circ \sigma' = \sigma' \circ \sigma$.

■

Remarque 2.7 *La réciproque du point* ***4.*** *du théorème précédent est fausse. Pour le voir, on prend* $\sigma \neq Id_E$ *et* $\sigma' = \sigma^{-1}$.

Pour la suite de ce paragraphe et les suivants, E est un ensemble fini de cardinal $n \geq 2$.
Soit $\sigma \in \mathcal{S}(E)$.
On a une action naturelle du groupe cyclique $H = \langle \sigma \rangle$ sur E définie par :

$$\left(\sigma^k, x\right) \mapsto \sigma^k \cdot x = \sigma^k(x)$$

Les orbites (ou σ-orbites) pour cette action, sont les parties de E :

$$H \cdot x = \{\gamma \cdot x \mid \gamma \in H\} = \left\{\sigma^k(x) \mid k \in \mathbb{Z}\right\}$$

où x décrit E.
On notera $Orb_\sigma(x)$ une telle orbite.
On rappelle que ces orbites sont aussi les classes d'équivalence pour la relation d'équivalence définie sur E par :

$$(x \mathcal{R}_\sigma y) \Leftrightarrow \left(\exists k \in \mathbb{Z} \mid y = \sigma^k(x)\right)$$

et les orbites deux à deux distinctes forment une partition de E.

Remarque 2.8 *Une* σ*-orbite* $Orb_\sigma(x)$ *est réduite à un point si, et seulement si,* $\sigma(x) = x$ *et la réunion des orbites non réduites à un point est égale au support de* σ.

Exemple 2.3 *Soit $\sigma = (x_1, \cdots, x_r)$ un r-cycle.*
Pour $x \in E \setminus \{x_1, \cdots, x_r\}$, on a $\sigma(x) = x$ et $Orb_\sigma(x) = \{x\}$.
Pour k compris entre 2 et r, on a $x_k = \sigma^{k-1}(x_1)$, donc $x_k \sim x_1$ modulo $\langle\sigma\rangle$ et comme $\sigma^r(x_1) = x_1$, on a :

$$\begin{aligned} Orb_\sigma(x_k) = Orb_\sigma(x_1) &= \left\{x_1, \sigma(x_1), \cdots, \sigma^{r-1}(x_1)\right\} \\ &= \{x_1, x_2, \cdots, x_r\} \end{aligned}$$

Il y a donc une seule orbite non réduite à un point.
Nous verrons un peu plus loin que cela caractérise les cycles.

Lemme 2.4 *Soient $\sigma \in \mathcal{S}(E) \setminus \{Id_E\}$ et O une σ-orbite de cardinal $r \geq 2$.*
Pour tout $x \in O$, r est le plus petit entier naturel non nul tel que $\sigma^r(x) = x$ et :

$$O = Orb_\sigma(x) = \left\{x, \sigma(x), \cdots, \sigma^{r-1}(x)\right\}$$

Démonstration. Comme $\sigma \neq Id_E$, il existe une orbite O non réduite à un point.
Il existe $y \in E$ tel que $O = Orb_\sigma(y) = \left\{\sigma^k(y) \mid k \in \mathbb{Z}\right\}$.
Si $x \in O$, il existe alors un entier k tel que $x = \sigma^k(y)$ et :

$$\begin{aligned} Orb_\sigma(x) &= \left\{\sigma^j(x) \mid j \in \mathbb{Z}\right\} = \left\{\sigma^{j+k}(y) \mid j \in \mathbb{Z}\right\} \\ &= \left\{\sigma^i(y) \mid i \in \mathbb{Z}\right\} = O \end{aligned}$$

Si $\sigma^k(x) \neq x$ pour tout $k \geq 1$, on a alors $\sigma^i(x) \neq \sigma^j(x)$ pour tous $i \neq j$ dans $\mathbb{Z}$ et O est infini, ce qui n'est pas. Il existe donc un plus petit entier naturel non nul s tel que $\sigma^s(x) = x$.

Comme $O = Orb_\sigma(x)$ est de cardinal $r \geq 2$, elle n'est pas réduite à un point et $\sigma(x) \neq x$. On a donc $s \geq 2$.

En utilisant le théorème de division euclidienne, tout entier $k \in \mathbb{Z}$ s'écrit $k = qs + j$ avec $q \in \mathbb{Z}$ et $0 \leq j \leq s-1$, ce qui donne :

$$\sigma^k(x) = \sigma^i(x)$$

et $O = \{x, \sigma(x), \cdots, \sigma^{s-1}(x)\}$.

Avec $\sigma^i(x) \neq \sigma^j(x)$ pour tous $i \neq j$ dans $\{0, 1, \cdots, s-1\}$ (caractère minimal de s), on déduit que $\text{card}(O) = s$ et $s = r$. ∎

Théorème 2.5 *Une permutation $\sigma \in \mathcal{S}(E)$ est un cycle d'ordre $r \geq 2$ si, et seulement si, il n'y a qu'une seule σ-orbite non réduite à un point.*

Démonstration. On a déjà vu qu'un r-cycle a une seule orbite non réduite à un point.
Réciproquement si σ a une seule orbite non réduite à un point :

$$O = \left\{x, \sigma(x), \cdots, \sigma^{r-1}(x)\right\} = \{x_1, x_2, \cdots, x_r\}$$

avec $r \geq 2$, on a alors :

$$\begin{cases} \sigma(x_k) = x_{k+1} \ (1 \leq k \leq r-1) \\ \sigma(x_r) = x_1 \\ \sigma(x) = x \text{ si } x \in E \setminus \{x_1, \cdots, x_r\} \end{cases}$$

et σ est le r-cycle $(x_1, x_2, \cdots, x_r)$. ∎

Remarque 2.9 *La composée de deux cycles n'est pas un cycle en général. Par exemple pour $\sigma = (1,2,3,4)$ dans $\mathcal{S}_4$, on a $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ avec $Orb_{\sigma^2}(1) = \{1,3\}$ et $Orb_{\sigma^2}(2) = \{2,4\}$, donc σ^2 n'est pas un cycle.*

Remarque 2.10 *Si σ est un r-cycle, le calcul de σ^m pour tout entier relatif m peut alors s'obtenir en effectuant la division euclidienne de m par r : on a $m = qr + i$ avec $0 \leq i \leq r-1$ et $\sigma^m = \sigma^i$.*

2.4 Décomposition d'un permutation en produit de cycles

Comme précisé au paragraphe précédent, E est un ensemble fini de cardinal $n \geq 2$.

En utilisant le fait que les σ-orbites forment une partition de E et que chaque σ-orbite non réduite à un point permet de définir un cycle, on obtient le résultat suivant qui nous donne un premier système de générateurs de $\mathcal{S}(E)$.

Théorème 2.6 *Toute permutation $\sigma \in \mathcal{S}(E) \setminus \{Id_E\}$ se décompose en produit de cycles de supports deux à deux disjoints (le groupe $\mathcal{S}(E)$ est engendré par les cycles). Cette décomposition est unique à l'ordre près.*
Si $\sigma = \sigma_1 \cdots \sigma_p$ est une telle décomposition, on a alors :

$$\mathrm{Supp}(\sigma) = \bigcup_{k=1}^{p} \mathrm{Supp}(\sigma_k)$$

Démonstration. Soient $\sigma \in \mathcal{S}(E) \setminus \{Id_E\}$ et $O_1, \cdots, O_p, \cdots, O_r$ les σ-orbites deux à deux distinctes avec $r_k = \mathrm{card}(O_k) \geq 2$ pour $k = 1, \cdots, p$ et $\mathrm{card}(O_k) = 1$ pour $k = p+1, \cdots, r$ (s'il en existe). On a alors la partition $E = \bigcup_{k=1}^{r} O_k$.

Pour tout entier k compris entre 1 et r, on désigne par γ_k la permutation de E définie par :

$$\forall x \in E,\ \gamma_k(x) = \begin{cases} \sigma(x) \text{ si } x \in O_k \\ x \text{ si } x \notin O_k \end{cases}$$

(γ_k est bien une permutation de E car la restriction de σ à une orbite O_k est une permutation de O_k). Si O_k est réduite à un point, alors $\gamma_k = Id_E$, sinon γ_k est un r_k-cycle : en effet, pour $x \notin O_k$, on a $\gamma_k(x) = x$ et $Orb_{\gamma_k}(x) = \{x\}$ et pour $x \in O_k$, on a :

$$\begin{aligned} Orb_{\gamma_k}(x) &= \left\{\gamma_k^j(x) \mid j \in \mathbb{Z}\right\} = \left\{\sigma^j(x) \mid j \in \mathbb{Z}\right\} \\ &= Orb_\sigma(x) = O_k \end{aligned}$$

donc γ_k a bien une seule orbite non réduite à un point.

On vérifie alors que $\sigma = \prod_{j=1}^{r} \gamma_j = \prod_{j=1}^{p} \gamma_j$. En effet, pour $x \in E$ il existe un unique indice k compris entre 1 et r tel que $x \in O_k$ et on a $\gamma_k(x) = \sigma(x)$, $\gamma_j(x) = x$ pour $j \neq k$ (puisque $x \notin O_j$) et tenant compte du fait que les γ_j commutent (leurs supports sont deux à deux disjoints), on en déduit que :

$$\left(\prod_{j=1}^{r} \gamma_j\right)(x) = \left(\gamma_k \prod_{\substack{j=1 \\ j \neq k}}^{r} \gamma_j\right)(x) = \gamma_k(x) = \sigma(x)$$

La réunion $\bigcup_{k=1}^{p} \mathrm{Supp}(\sigma_k)$ est la réunion des orbites O_k non réduites à un point, soit le support de σ.

Il reste à montrer l'unicité, à l'ordre près, d'une telle décomposition.

Si $\sigma = \prod_{k=1}^{p'} \sigma'_k$ est une autre décomposition en cycles de supports deux à deux disjoints. En notant $O'_1, \cdots, O'_{p'}$ ces supports, pour $k \in \{1, \cdots, p'\}$ et $x \in O'_k$, on a $\sigma(x) = \sigma'_k(x)$ ($x \notin O'_j$

pour $j \neq k$ et les cycles commutent), donc $O'_k = Orb_{\sigma'_k}(x) = Orb_\sigma(x)$. Les orbites O'_k sont donc les orbites non réduites à un point de σ et $p' = p$. On a donc $O'_k = O_j$ pour un unique j compris entre 1 et p. Pour $x \in O'_k$, on a $\sigma'_k(x) = \sigma(x) = \sigma_j(x)$ et pour $x \notin O'_k$, $\sigma'_k(x) = x = \sigma_j(x)$, ce qui donne $\sigma'_k = \sigma_j$ et l'unicité de la décomposition à l'ordre près. ■

Remarque 2.11 *On conviendra que l'identité est produit de* 0 *cycle :* $Id_E = \gamma^0$ *pour tout cycle* γ.

Pour $E = \{1, 2, \cdots, n\}$, une telle décomposition s'obtient en prenant, dans le cas où il n'est pas fixe, les images de 1 par $\sigma, \sigma^2, \cdots$, jusqu'au moment où on retombe sur 1 (l'orbite de 1), puis on recommence avec le plus petit entier dans $E \setminus Orb_\sigma(1)$ qui n'est pas fixe et ainsi de suite.

Par exemple, pour :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix}$$

on a $\sigma(1) = 2$, $\sigma^2(1) = 3$, $\sigma^3(1) = 4$, $\sigma^4(1) = 1$, $\sigma^5(1) = 1$, ce qui donne le premier cycle $(1, 2, 3, 4, 5)$, puis $\sigma(6) = 7$, $\sigma^2(6) = 6$ et $\sigma(8) = 8$, donc $\sigma = (1, 2, 3, 4, 5)(6, 7)$.

Exercice 2.7 *Soit* $\sigma \in \mathcal{S}_n$ *définie par :*

$$\forall k \in \{1, 2, \cdots, n\},\ \sigma(k) = n + 1 - k$$

(elle inverse l'ordre des entiers $1, 2, \cdots, n$*). Donner la décomposition de* σ *en produit de cycles de supports deux à deux disjoints.*

Solution 2.7 *On a :*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ n & n-1 & n-2 & \cdots & 2 & 1 \end{pmatrix}$$

Si n *est pair, soit* $n = 2p$ *avec* $p \geq 1$*, on a :*

$$\sigma(k) = 2p + 1 - k,\ \sigma^2(k) = \sigma(2p + 1 - k) = k$$

pour $k = 1, \cdots, p$ *(et* $2p + 1 - k = 2p, \cdots, p + 1$*), ce qui donne :*

$$\sigma = (1, 2p)(2, 2p - 1) \cdots (p, p + 1)$$

Si n *est impair, soit* $n = 2p + 1$ *avec* $p \geq 1$*, on a :*

$$\sigma(k) = 2p + 2 - k,\ \sigma^2(k) = \sigma(2p + 2 - k) = k$$

pour $k = 1, \cdots, p$ *(*$2p + 2 - k = 2p + 1, \cdots, p + 2$*) et* $\sigma(p + 1) = p + 1$ *ce qui donne :*

$$\sigma = (1, 2p + 1)(2, 2p) \cdots (p, p + 2)$$

Donc σ *est produit de transpositions de supports deux à deux disjoints et est d'ordre* 2 *(ce qui se voit directement sur sa définition).*

Exercice 2.8 *Soient* σ, γ *deux permutations dans* $\mathcal{S}(E) \setminus \{Id_E\}$*. Exprimer la décomposition en cycles de supports disjoints de* $\sigma\gamma\sigma^{-1}$ *en fonction de celle de* γ.

Solution 2.8 *Si* $\gamma = \prod_{j=1}^{p} \gamma_j$ *est la décomposition en cycles de supports disjoints de* γ*, alors* $\sigma\gamma\sigma^{-1} = \prod_{j=1}^{p} (\sigma\gamma_j\sigma^{-1})$ *est celle de* $\sigma\gamma\sigma^{-1}$ *puisque pour* $\gamma_j = (x_1, \cdots, x_r)$*, on a* $\sigma\gamma_j\sigma^{-1} = (\sigma(x_1), \cdots, \sigma(x_r))$ *et les supports de ces cycles sont* 2 *à* 2 *disjoints du fait que* σ *est bijective.*

Corollaire 2.1 *Si* $\sigma = \sigma_1 \cdots \sigma_p$ *est « la » décomposition de* $\sigma \in \mathcal{S}(E) \setminus \{Id_E\}$ *en produit de cycles de supports deux à deux disjoints, on a alors :*

$$\text{ordre}(\sigma) = \text{ppcm}(\text{ordre}(\sigma_1), \cdots, \text{ordre}(\sigma_p))$$

Démonstration. Notons $\mu = \text{ppcm}(\text{ordre}(\sigma_1), \cdots, \text{ordre}(\sigma_p))$.

Comme les cycles σ_k commutent, on a $\sigma^k = \sigma_1^k \cdots \sigma_p^k$ pour tout entier naturel k et $\sigma^k = Id_E$ si, et seulement si $\sigma_j^k = Id_E$ pour tout j compris entre 1 et p. En effet, il est clair que la condition est suffisante et si $\sigma^k = Id_E$, on a alors pour tout $x \in O_j$ ($O_1, \cdots, O_p$ sont toutes les σ-orbites) $\sigma_j^k(x) = \sigma^k(x) = x$ et aussi $\sigma_j^k(x) = x$ pour $x \notin O_j$, donc$\sigma_j^k = Id_E$. Donc l'ordre de σ est un multiple commun des ordres des σ_j et c'est un multiple de μ qui lui même est multiple de l'ordre de σ puisque $\sigma^\mu = Id_E$. ■

Remarque 2.12 *Comme l'ordre d'un cycle est égal à sa longueur, l'ordre de* σ *est aussi le* ppcm *des longueurs des cycles* σ_j*.*

Exercice 2.9 *Soit* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix}$*. Calculer* σ^{2009}*.*

Solution 2.9 *La permutation* $\sigma = (1,2,3,4,5)(6,7) = \gamma\tau$ *est d'ordre* $\text{ppcm}(5,2) = 10$*. En effectuant la division euclidienne, on a pour tout entier relatif* $m = 10q + r$ *où* $0 \leq r \leq 9$*,* $\sigma^m = \sigma^r$*. Ce qui donne*

$$\begin{aligned} \sigma^{2009} = \sigma^9 &= \gamma^9\tau^9 = \gamma^{-1}\tau \\ &= (5,4,3,2,1)(6,7) \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 2 & 3 & 4 & 7 & 6 & 8 \end{pmatrix} \end{aligned}$$

Exercice 2.10 *Quel est l'ordre maximal d'un élément de* $\mathcal{S}_5$*.*

Solution 2.10 *La décomposition en cycles disjoints d'un élément de* $\mathcal{S}_5 \setminus \{Id\}$ *(Id est d'ordre* 1*) est formée soit d'un* r*-cycle avec* $2 \leq r \leq 5$*, soit d'un* 2*-cycle et d'un cycle d'ordre* 2 *ou* 3 *et en utilisant le corollaire précédent, on voit que cet ordre est au maximum* 6*, qui est atteint pour* $(1,2)(3,4,5)$*.*

2.5 Divers systèmes de générateurs de $\mathcal{S}(E)$

On a déjà vu que $\mathcal{S}(E)$ est engendré par les cycles.

Lemme 2.5 *Pour* $2 \leq r \leq n$*, tout* r*-cycle dans* $\mathcal{S}(E)$ *s'écrit comme produit de* $r-1$ *transpositions.*

Démonstration. Résulte de :

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

■

Corollaire 2.2 *Toute permutation $\sigma \in \mathcal{S}(E)$ se décompose en produit de transpositions (le groupe $\mathcal{S}(E)$ est engendré par les transpositions).*

Démonstration. On a $Id_E = \tau^2$ pour toute transposition.
Toute permutation $\sigma \in \mathcal{S}(E) \setminus \{Id_E\}$ est produit de cycles et un cycle est produit de transpositions. ■

Exercice 2.11 *Montrer directement par récurrence sur $n \geq 2$, que $\mathcal{S}(E)$ est engendré par les transpositions.*

Solution 2.11 *Pour $E = \{x_1, x_2\}$, on a $\mathcal{S}(E) = \{Id_E, (x_1, x_2)\}$.*
Supposons le résultat acquis pour les ensembles de cardinal $n-1 \geq 2$ et soit E de cardinal n. Soient $\sigma \in \mathcal{S}(E)$. Si $\sigma = Id_E$, on a $\sigma = \tau^2$ pour toute transposition τ. Sinon il existe $x \in E$ tel que $y = \sigma(x) \neq x$. En désignant par τ la transposition $\tau = (x, y)$, on a $\tau\sigma(x) = x$ et la restriction de $\tau\sigma$ à $F = E \setminus \{x\}$ est une permutation de F, elle s'écrit donc comme produit de transpositions et $\tau\sigma = \tau_1 \cdots \tau_r$ où les τ_k sont des transpositions de E qui laissent fixe x. Il en résulte que $\sigma = \tau\tau_1 \cdots \tau_r$ est produit de transpositions.
Cette démonstration montre aussi que si $\{\tau_1, \cdots, \tau_r\}$ est une famille de transpositions qui engendre $\mathcal{S}(E)$, on a nécessairement $r \geq n-1$.

Exemple 2.4 *Pour* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix} = (1,2,3,4,5)(6,7)$, *on a :*

$$\sigma = (1,2)(2,3)(3,4)(4,5)(6,7)$$

Comme $\mathcal{S}(E)$ est isomorphe à $\mathcal{S}_n$, on se contente maintenant de décrire des générateurs de $\mathcal{S}_n$.

Lemme 2.6 *$\mathcal{S}_n$ est engendré par les $n-1$ transpositions $(1,k)$ où $2 \leq k \leq n$.*

Démonstration. Soit (i,j) une transposition avec $1 \leq i \neq j \leq n$. Si $i = 1$ ou $j = 1$, il n'y a rien à faire ($(i,j) = (j,i)$) et pour $i \neq 1$, $j \neq 1$, on remarque que :

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

Le résultat se déduit alors du fait que $\mathcal{S}_n$ est engendré par les transpositions. ■

Remarque 2.13 *Il n'est pas possible d'enlever une de ces transpositions car pour $2 \leq k \leq n$ et $2 \leq j \neq k \leq n$, toutes les transposition $(1,j)$ laissent fixe k.*

Exemple 2.5 *Pour* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix} = (1,2)(2,3)(3,4)(4,5)(6,7)$, *on a :*

$$\begin{aligned}\sigma &= (1,2)(1,2)(1,3)(1,2)(1,3)(1,4)(1,3)(1,4)(1,5)(1,4)(1,6)(1,7)(1,6) \\ &= (1,3)(1,2)(1,3)(1,4)(1,3)(1,4)(1,5)(1,4)(1,6)(1,7)(1,6)\end{aligned}$$

Lemme 2.7 *$\mathcal{S}_n$ est engendré par les $n-1$ transpositions $(k,k+1)$ où $1 \leq k \leq n-1$.*

Démonstration. Comme $\mathcal{S}_n$ est engendré par les transpositions $(1,k)$ où $2 \leq k \leq n$, il suffit d'écrire chaque transposition $(1,k)$ comme produit de transpositions du type $(i,i+1)$.

Pour $3 \leq k \leq n$, on a :

$$(1,k) = (k-1,k)(1,k-1)(k-1,k)$$

(lemme 2.2). Pour $k=3$, on a $(1,k-1) = (1,2)$ et c'est terminé, sinon on écrit $(1,k-1) = (k-2,k-1)(1,k-2)(k-2,k-1)$ et on continue ainsi de suite si nécessaire.Pour $k=2$, la transposition $(1,k) = (1,2)$ est de la forme souhaitée. ∎

Remarque 2.14 *Il n'est pas possible d'enlever une de ces transpositions car pour $1 \leq k \leq n-1$ et $1 \leq j \neq k \leq n-1$, toutes les transposition $(j,j+1)$ laissent globalement invariant la partie $\{1,\cdots,k\}$.*

Lemme 2.8 *$\mathcal{S}_n$ est engendré par $(1,2)$ et $(1,2,\cdots,n)$ ($\mathcal{S}_n$ est dicyclique).*

Démonstration. Comme $\mathcal{S}_n$ est engendré par les transpositions $(k,k+1)$ où $1 \leq k \leq n-1$, il suffit de montrer que chaque transposition $(k,k+1)$ est dans le sous-groupe G de $\mathcal{S}_n$ engendré par $\tau = (1,2)$ et $\gamma = (1,2,\cdots,n)$.

On a déjà $(1,2) \in G$ et, pour $n \geq 3$:

$$\begin{cases} \gamma(1,2)\gamma^{-1} = (\gamma(1),\gamma(2)) = (2,3) \\ \gamma(2,3)\gamma^{-1} = (\gamma(2),\gamma(3)) = (3,4) \\ \vdots \\ \gamma(n-2,n-1)\gamma^{-1} = (\gamma(n-2),\gamma(n-1)) = (n-1,n) \end{cases}$$

soit $(k,k+1) = \gamma^{k-1}(1,2)\left(\gamma^{k-1}\right)^{-1}$ pour $1 \leq k \leq n-1$. ∎

Exercice 2.12 *Montrer que, pour $n \geq 3$, $\mathcal{S}_n$ est engendré par $(1,2)$ et $(2,3,\cdots,n)$.*

Solution 2.12 *Comme $\mathcal{S}_n$ est engendré par les transpositions $(1,k)$ où $2 \leq k \leq n$, il suffit de montrer que chaque transposition $(1,k)$ est dans le sous-groupe G de $\mathcal{S}_n$ engendré par $(1,2)$ et $(2,3,\cdots,n)$.*
On a déjà $(1,2) \in G$.
En notant $\sigma_k = (2,3,\cdots,n)^{k-2}$ pour $3 \leq k \leq n$, on a $\sigma_k(1) = 1$, $\sigma_k(2) = k$, et :

$$(1,k) = \sigma_k(1,2)\sigma_k^{-1} \in H$$

2.6 Signature d'une permutation

Pour toute permutation $\sigma \in \mathcal{S}(E)$, on note $\mu(\sigma)$ le nombre de σ-orbites distinctes.

Si $\sigma = \prod_{k=1}^{p} \sigma_k$ est la décomposition de σ en produit de cycles de supports deux à deux disjoints, on a vu que p est le nombre de σ-orbites non réduites à un point et $\mu(\sigma) = p + \varphi(\sigma)$ où $\varphi(\sigma)$ est le nombre de points fixes de σ.

Définition 2.5 *La signature d'une permutation $\sigma \in \mathcal{S}(E)$ est l'élément $\varepsilon(\sigma)$ de $\{-1,1\}$ défini par :*

$$\varepsilon(\sigma) = (-1)^{n-\mu(\sigma)}$$

Exemple 2.6 *L'identité a n orbites réduites à un point et* $\varepsilon(Id_E) = 1$.

Exemple 2.7 *Si* σ *est un* r*-cycle, il a une orbite non réduite à un point et* $n-r$ *orbites réduites à un point, donc* $\mu(\sigma) = n - r + 1$ *et* $\varepsilon(\sigma) = (-1)^{r-1}$.

Exemple 2.8 *Si* τ *est une transposition, on a* $\varepsilon(\sigma) = -1$.

Lemme 2.9 *Pour toute permutation* $\sigma \in \mathcal{S}(E)$ *et toute transposition* $\tau \in \mathcal{S}(E)$, *on a :*

$$\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$$

Démonstration. Soit $\tau = (x, y)$ une transposition dans $\mathcal{S}(E)$ avec $x \neq y$.

Si $\sigma = Id_E$, on a alors $\tau\sigma = \tau$ et $\varepsilon(\tau\sigma) = -1$.

Pour $\sigma \neq Id_E$, on a la décomposition en produit de cycles de supports deux à deux disjoints, $\sigma = \sigma_1 \cdots \sigma_p$, où les $O_k = \text{Supp}(\sigma_k)$, pour k compris entre 1 et p, sont toutes les orbites non réduites à un point.

Si $\{x, y\} \cap \bigcup_{k=1}^{p} O_k = \emptyset$, le nombre de points fixes de $\sigma' = \tau\sigma$ est alors $\varphi(\sigma') = \varphi(\sigma) - 2$ et le nombre de σ'-orbites est :

$$\mu(\sigma') = p + 1 + \varphi(\sigma) - 2 = \mu(\sigma) - 1$$

ce qui donne $\varepsilon(\sigma') = -\varepsilon(\sigma)$.

Si $\{x, y\}$ est contenu dans l'une des σ-orbites O_k, comme les cycles σ_j commutent, on a :

$$\sigma' = \tau\sigma_k \prod_{\substack{j=1 \\ j\neq k}}^{p} \sigma_j$$

avec :

$$y \in O_k = Orb_\sigma(x) = \left\{x, \sigma(x), \cdots, \sigma^{r_k-1}(x)\right\} = \{x_1, \cdots, x_{r_k}\}$$

Il existe donc $j \in \{2, \cdots, r_k\}$ tel que $y = x_j$ et :

$$\begin{aligned} \tau\sigma_k &= (x_1, x_j)(x_1, \cdots, x_j, \cdots, x_{r_k}) \\ &= (x_1, \cdots, x_{j-1})(x_j, \cdots, x_{r_k}) = \sigma'_k\sigma''_k \end{aligned}$$

(pour $j = 1$ on a $\sigma'_k = Id_E$ et pour $j = r_k$, $\sigma''_k = Id_E$), ce qui donne la décomposition en produit de cycles de supports deux à deux disjoints :

$$\sigma' = \sigma'_k\sigma''_k \prod_{\substack{j=1 \\ j\neq k}}^{p} \sigma_j$$

On a donc, $\mu(\sigma') = \mu(\sigma) + 1$ et $\varepsilon(\sigma') = -\varepsilon(\sigma)$.

Enfin, la dernière possibilité est que x et y soient dans deux σ-orbites distinctes, soit $\{x, y\} \cap O_k = \{x\}$ et $\{x, y\} \cap O_j = \{y\}$ avec $j \neq k$. On a alors :

$$O_k = Orb_\sigma(x) = \left\{x, \sigma(x), \cdots, \sigma^{r_k-1}(x)\right\} = \{x_1, \cdots, x_{r_k}\}$$

et :

$$O_j = Orb_\sigma(y) = \left\{y, \sigma(y), \cdots, \sigma^{r_j-1}(y)\right\} = \left\{y_1, \cdots, y_{r_j}\right\}$$

donc :

$$\begin{aligned}\tau\sigma_k\sigma_j &= (x_1, y_1)(x_1, \cdots, x_{r_k})\left(y_1, \cdots, y_{r_j}\right)\\ &= \left(x_1, \cdots, x_{r_k}, y_1, \cdots, y_{r_j}\right) = \sigma'_k\end{aligned}$$

et la décomposition en produit de cycles de supports deux à deux disjoints :

$$\sigma' = \tau\sigma_k\sigma_j \prod_{\substack{i=1\\ i\notin\{j,k\}}}^{p} \sigma_i = \sigma'_k \prod_{\substack{i=1\\ i\notin\{j,k\}}}^{p} \sigma_i$$

On a donc, $\mu(\sigma') = \mu(\sigma) - 1$ et $\varepsilon(\sigma') = -\varepsilon(\sigma)$. ■

On en déduit le théorème qui suit qui nous donne une définition équivalente de la signature d'une permutation.

Théorème 2.7 *Si $\sigma \in \mathcal{S}(E)$ est produit de p transpositions, on a alors $\varepsilon(\sigma) = (-1)^p$ (la parité de p est donc uniquement déterminée par σ).*

Démonstration. C'est une conséquence immédiate du lemme précédent et du fait que $\varepsilon(\tau) = -1$ pour toute transposition τ. ■

Théorème 2.8 *Les seuls morphismes de groupes de $(\mathcal{S}(E), \circ)$ dans $(\mathbb{R}^*, \cdot)$ sont l'application constante égale à 1 et la signature ε. La signature étant surjective de $\mathcal{S}(E)$ sur $\{-1, 1\}$.*

Démonstration. Montrons tout d'abord que ε est un morphisme de groupes surjectif de $(\mathcal{S}(E), \circ)$ sur $\{-1, 1\}$.

On a vu que ε est à valeurs dans $\{-1, 1\}$ et avec $\varepsilon(Id_E) = 1$, $\varepsilon(\tau) = -1$ pour toute transposition τ (E a au moins deux éléments), on déduit que σ est surjectif.

Si σ, σ' sont deux permutations elles s'écrivent respectivement comme produit de p et q transpositions, ce qui permet d'écrire $\sigma\sigma'$ comme produit de $p+q$ transpositions et on a $\varepsilon(\sigma\sigma') = (-1)^{p+q} = \varepsilon(\sigma)\varepsilon(\sigma')$. Donc ε est un morphisme de groupes.

Soit φ un morphisme de groupe de $\mathcal{S}(E)$ dans $\mathbb{R}^*$.

Si τ_1 et τ_2 sont deux transpositions, il existe une permutation σ telle que $\tau_2 = \sigma\tau_1\sigma^{-1}$ (lemme 2.2) et comme le groupe multiplicatif $\mathbb{R}^*$ est commutatif, on a :

$$\varphi(\tau_2) = \varphi(\sigma)\varphi(\tau_1)\varphi(\sigma)^{-1} = \varphi(\sigma)\varphi(\sigma)^{-1}\varphi(\tau_1) = \varphi(\tau_1)$$

c'est-à-dire que φ est constant sur les transpositions. Avec :

$$\varphi(Id_E) = \varphi\left(\tau^2\right) = (\varphi(\tau))^2$$

pour toute transposition τ, on déduit que $\varphi(\tau) = 1$ pour toute transposition τ ou $\varphi(\tau) = -1$ pour toute transposition τ. Dans le premier cas, on a $\varphi(\sigma) = 1$ pour toute permutation σ puisque les transpositions engendrent $\mathcal{S}(E)$ et dans le second cas, comme toute permutation $\sigma \in \mathcal{S}(E)$ s'écrit $\sigma = \prod_{k=1}^{p} \tau_k$ où les τ_k sont des transpositions, on a $\varphi(\sigma) = \prod_{k=1}^{p} \varphi(\tau_k) = (-1)^p = \varepsilon(\sigma)$. ■

Exercice 2.13 *Déterminer la signature de :*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 5 & 1 & 2 & 3 & 4 & 7 & 6 & 8 \end{pmatrix}$$

Solution 2.13 *On a :*

$$\sigma = (1,5,4,3,2)(6,7)$$

et $\varepsilon(\sigma) = (-1)^{5-1}(-1) = -1$.
On peut aussi écrire σ *comme produit de transpositions :*

$$\sigma = (1,5)(5,4)(4,3)(3,2)(6,7)$$

et $\varepsilon(\sigma) = (-1)^5 = -1$.

Le résultat qui suit nous donne une autre définition de la signature d'une permutation $\sigma \in \mathcal{S}_n$ (on peut toujours se ramener à ce cas).

Théorème 2.9 *Pour toute permutation* $\sigma \in \mathcal{S}_n$, *on a :*

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

Démonstration. Soit φ l'application définie sur $\mathcal{S}_n$ par $\varphi(\sigma) = \prod_{1\leq i<j\leq n} \frac{\sigma(j)-\sigma(i)}{j-i}$. Pour montrer que $\varphi = \varepsilon$, il suffit de montrer que φ est un morphisme de groupes non constant de $\mathcal{S}_n$ dans $\mathbb{R}^*$.

Comme σ est bijective, on a $\varphi(\sigma) \in \mathbb{R}^*$ pour tout $\sigma \in \mathcal{S}_n$.

Pour σ_1, σ_2 dans $\mathcal{S}_n$, on a :

$$\begin{aligned}
\varphi(\sigma_1\sigma_2) &= \prod_{1\leq i<j\leq n} \frac{\sigma_1(\sigma_2(j))-\sigma_1(\sigma_2(i))}{\sigma_2(j)-\sigma_2(i)} \frac{\sigma_2(j)-\sigma_2(i)}{j-i} \\
&= \prod_{1\leq i<j\leq n} \frac{\sigma_1(\sigma_2(j))-\sigma_1(\sigma_2(i))}{\sigma_2(j)-\sigma_2(i)} \prod_{1\leq i<j\leq n} \frac{\sigma_2(j)-\sigma_2(i)}{j-i} \\
&= \prod_{1\leq i'<j'\leq n} \frac{\sigma_1(j')-\sigma_1(i')}{j'-i'} \prod_{1\leq i<j\leq n} \frac{\sigma_2(j)-\sigma_2(i)}{j-i}
\end{aligned}$$

puisque σ_2 est bijective de $\{1,\cdots,n\}$ sur $\{1,\cdots,n\}$ et $\frac{\sigma_1(j')-\sigma_1(i')}{j'-i'} = \frac{\sigma_1(i')-\sigma_1(j')}{i'-j'}$, ce qui donne $\varphi(\sigma_1\sigma_2) = \varphi(\sigma_1)\varphi(\sigma_2)$.

On a $\varphi(Id_E)$ et pour $\tau = (1,2)$:

$$\begin{aligned}
\varphi(\tau) &= \prod_{i=1}^{n-1}\prod_{j=i+1}^{n} \frac{\tau(j)-\tau(i)}{j-i} \\
&= \prod_{j=2}^{n} \frac{\tau(j)-2}{j-1} \prod_{j=3}^{n} \frac{j-1}{j-2} = -\prod_{j=3}^{n} \frac{j-2}{j-1}\frac{j-1}{j-2} = -1
\end{aligned}$$

donc φ est non constant et c'est la signature. ∎

Du théorème précédent, on déduit que $\varepsilon(\sigma) = (-1)^{\nu(\sigma)}$, où :

$$\nu(\sigma) = \operatorname{card}\left\{(i,j) \in \mathbb{N}^2 \mid 1 \leq i < j \leq n \text{ et } \sigma(j) < \sigma(i)\right\}$$

est le nombre d'inversions de σ. Ce qui nous donne une définition supplémentaire de la signature.

Exemple 2.9 *Pour :*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 2 & 3 & 4 & 7 & 6 & 8 \end{pmatrix}$$

on a 5 *inversions, donc* $\varepsilon(\sigma) = (-1)^5 = -1$.

2.7 Le groupe alterné

Définition 2.6 *On dit qu'une permutation $\sigma \in \mathcal{S}(E)$ est paire [resp. impaire] si $\varepsilon(\sigma) = 1$ [resp. $\varepsilon(\sigma) = -1$].*

Exemple 2.10 *Les cycles de longueur paire [resp. impaire] sont impaires [resp. paires].*

Définition 2.7 *Le groupe alterné est le sous-ensemble de $\mathcal{S}(E)$ formé des permutations paires. On le note $\mathcal{A}(E)$.*

Pour $E = \{1, 2, \cdots, n\}$, on note $\mathcal{A}_n$ le groupe alterné.

Remarque 2.15 *$\mathcal{A}(E)$ est un sous-groupe distingué de $\mathcal{S}(E)$ puisque c'est le noyau du morphisme ε.*
$\mathcal{A}(E)$ est d'indice 2 ($\operatorname{card}\left(\dfrac{\mathcal{S}(E)}{\mathcal{A}(E)}\right) = \operatorname{card}\{-1, 1\} = 2$*) et* $\operatorname{card}(\mathcal{A}(E)) = \dfrac{n!}{2}$.

Pour $n = 2$, on a $\mathcal{A}(E) = \{Id_E\}$.
Dans ce qui suit, on suppose que $n \geq 3$.

Remarque 2.16 *$\mathcal{A}_3$ est cyclique engendré par $(1, 2, 3)$. En effet* $\operatorname{card}(\mathcal{A}_3) = \dfrac{3!}{2} = 3$ *et le cycle $(1, 2, 3)$ est d'ordre 3.*

Exercice 2.14

1. *Soient G un groupe d'ordre $2n$ et H un sous-groupe de G d'ordre n.*
   (a) *Montrer que, pour tout $g \in G \setminus H$, on a la partition $G = H \cup gH$.*
   (b) *En déduire que $g^2 \in H$ pour tout $g \in G$.*
2. *Montrer que tout 3-cycle $\sigma \in \mathcal{A}_n$ est le carré d'un élément de $\mathcal{A}_n$.*
3. *Donner la liste de tous les éléments de $\mathcal{A}_4$ en précisant leur ordre.*
4. *Montrer que $\mathcal{A}_4$ (qui est d'ordre 12) n'a pas de sous-groupe d'ordre 6.*

Solution 2.14

1. (a) *Si $H \cap gH \neq \emptyset$, il existe alors un élément h de H tel que $k = gh$ soit dans H. Mais alors, $g = kh^{-1} \in H$, ce qui n'est pas. On a donc $H \cap gH = \emptyset$ et* $\operatorname{card}(H \cup gH) = 2\operatorname{card}(H) = \operatorname{card}(G)$ *(l'application $h \mapsto gh$ réalise une bijection de H sur gH, donc ces ensembles ont le même nombre d'éléments), ce qui entraîne $G = H \cup gH$.*
   (b) *Soit $g \in G$. Si $g \in H$, on a alors $g^2 \in H$ puisque H est un groupe. Si $g \notin H$, il ne peut pas exister d'élément $h \in H$ tel que $g^2 = gh$ (sinon $g = h \in H$), donc $g^2 \notin gH$ et $g^2 \in H$ puisque l'on a la partition $G = H \cup gH$.*
2. *Un 3-cycle $\sigma \in \mathcal{A}_n$ étant d'ordre 3, on a $\sigma^4 = \sigma$, soit $\sigma = \gamma^2$ avec $\gamma = \sigma^2 \in \mathcal{A}_n$.*
3. *On note τ_{ij} la transposition (i, j) dans $\mathcal{S}_4$ pour $1 \leq i \neq j \leq 4$.*
   On a dans le groupe $\mathcal{A}_4$ les 12 éléments distincts suivants :
   – *l'identité ;*
   – *les 3 éléments d'ordre 2 : $\tau_{12} \circ \tau_{34}, \tau_{13} \circ \tau_{24}, \tau_{23} \circ \tau_{14}$ (le produit de deux transpositions de supports disjoints est d'ordre 2 puisque ces transpositions commutent) ;*

– *les* 8 *éléments d'ordre* 3 *:* $(2,3,4)$, $(2,4,3)$, $(1,3,4)$, $(1,4,3)$, $(1,2,4)$, $(1,4,2)$, $(1,2,3)$ $(1,3,2)$ *(un* 3*-cycle fixe un élément de* $\{1,2,3,4\}$ *et il y en a deux qui fixent* k*, pour* $k=1,2,3,4$*)*

et on a ainsi tous les éléments puisque $\mathcal{A}_4$ *est de cardinal* $\dfrac{4!}{2}=12$.

4. *Si* H *est un sous-groupe de* $\mathcal{A}_4$ *d'ordre* 6*, on a alors* $\sigma^2\in H$ *pour tout* $\sigma\in\mathcal{A}_4$ *et en particulier* H *va contenir tous les* 3*-cycles, soit* 8 *éléments, ce qui n'est pas possible.*

Lemme 2.10 *Un produit de deux transpositions est un produit de* 3*-cycles. Précisément, pour* x,y,z,t *deux à distincts dans* E*, on a :*

$$(x,y)(x,z)=(x,z,y)\ \text{ et }\ (x,y)(z,t)=(y,z,x)(z,t,y).$$

Démonstration. Soient τ_1 et τ_2 deux transpositions. Si $\tau_1=\tau_2$, on a alors $\tau_1\tau_2=\tau_1^2=Id_E=\gamma^3$ pour n'importe quel 3-cycle.

Si $\tau_1\neq\tau_2$, on a alors deux possibilités. Soit $\mathrm{Supp}(\tau_1)\cap\mathrm{Supp}(\tau_2)=\{x\}$, donc $\tau_1=(x,y)$, $\tau_2=(x,z)$ avec x,y,z distincts et :

$$\tau_1\tau_2=(x,z,y)$$

soit $\mathrm{Supp}(\tau_1)\cap\mathrm{Supp}(\tau_2)=\emptyset$, donc $\tau_1=(x,y)$, $\tau_2=(z,t)$ avec x,y,z,t distincts et :

$$\begin{aligned}\tau_1\tau_2&=(x,y)(z,t)=(x,y)(y,z)(y,z)(z,t)\\&=(y,x)(y,z)(z,y)(z,t)=(y,z,x)(z,t,y)\end{aligned}$$

■

Exercice 2.15 *Montrer que, pour* $n\geq 5$*, les produits de deux transpositions de supports disjoints sont conjugués dans* $\mathcal{A}(E)$.

Solution 2.15 *Soient* $\sigma=(x_1,x_2)(x_3,x_4)$ *et* $\sigma'=(x_1',x_2')(x_3',x_4')$ *deux produits de deux transpositions de supports disjoints. On se donne* $x_5\in E\setminus\{x_1,x_2,x_3,x_4\}$ *et* $x_5'\in E\setminus\{x_1',x_2',x_3',x_4'\}$*. En désignant par* τ *une permutation dans* $\mathcal{S}(E)$ *telle que* $\tau(x_k)=x_k'$ *pour* $1\leq k\leq 5$*, on a :*

$$\begin{aligned}\tau\sigma\tau^{-1}&=\tau(x_1,x_2)\tau^{-1}\tau(x_3,x_4)\tau^{-1}=(\tau(x_1),\tau(x_2))(\tau(x_3),\tau(x_4))\\&=(x_1',x_2')(x_3',x_4')=\sigma'\end{aligned}$$

Si $\tau\in\mathcal{A}(E)$ *c'est terminé, sinon* $\gamma=(x_3',x_4')\tau$ *est dans* $\mathcal{A}(E)$ *et :*

$$\begin{aligned}\gamma\sigma\gamma^{-1}&=(\gamma(x_1),\gamma(x_2))(\gamma(x_3),\gamma(x_4))\\&=(x_1',x_2')(x_4',x_3')=\sigma'\end{aligned}$$

Théorème 2.10 *Pour* $n\geq 3$*,* $\mathcal{A}(E)$ *est engendré par les* 3*-cycles.*

Démonstration. Comme $\mathcal{S}(E)$ est engendré par les transpositions, on déduit du théorème 2.7 qu'une permutation paire est le produit d'un nombre pair de transpositions et le lemme qui précède nous dit que ce produit s'écrit comme produit de 3-cycles. ■

Théorème 2.11 *Pour* $n\geq 5$*, les sous-groupes distingués de* $\mathcal{S}(E)$ *sont* $\{Id\}$, $\mathcal{A}(E)$ *et* $\mathcal{S}(E)$.

Démonstration. Soit H un sous-groupe distingué non trivial de $\mathcal{S}(E)$ (i. e. distinct de $\{Id\}$ et de $\mathcal{S}(E)$). Pour montrer que $H = \mathcal{A}(E)$, il suffit de montrer que H contient un 3-cycle (il les contient alors tous puisqu'ils sont conjugués dans $\mathcal{S}(E)$, donc $\mathcal{A}(E) \subset H$ et $H = \mathcal{A}(E)$ puisque les 3-cycles engendrent $\mathcal{A}(E)$ et $H \neq \mathcal{S}(E)$: en effet, on a $\mathcal{A}(E) \subset H \subset \mathcal{S}(E)$, donc $\operatorname{card}(H) = p\dfrac{n!}{2} = p\dfrac{q\operatorname{card}(H)}{2}$ et $pq = 2$, soit $p = 1$ et $H = \mathcal{A}(E)$ ou $p = 2$ et $H = \mathcal{S}(E)$).

On se donne $\sigma \in H \setminus \{Id\}$ et $\tau = (x, y)$ une transposition qui ne commute pas à σ (voir l'exercice 2.3). Comme H est distingué dans $\mathcal{S}(E)$, on a :

$$\sigma' = \tau\sigma\tau\sigma^{-1} = \left(\tau\sigma\tau^{-1}\right)\sigma^{-1} \in H$$

et en écrivant que :

$$\sigma' = (x, y)\left(\sigma(x, y)\,\sigma^{-1}\right) = (x, y)(\sigma(x), \sigma(y))$$

on voit que σ' est produit de deux transpositions.

L'égalité $\sigma' = Id$ est réalisée si, et seulement si, $\tau\sigma\tau\sigma^{-1} = Id$, soit $\tau\sigma = \sigma\tau^{-1} = \sigma\tau$, ce qui n'est pas.

Si $\{x, y\} \cap \{\sigma(x), \sigma(y)\}$ est réduit à un point, alors σ' est un 3-cycle et dans ce cas $H = \mathcal{A}(E)$, sinon cette intersection est vide et en prenant z dans $E \setminus \{x, y, \sigma(x), \sigma(y)\}$ (on a $n \geq 5$), le groupe H contient $(x, y)(\sigma(x), z)$ puisque le produit de deux transpositions de supports disjoints sont conjugués dans $\mathcal{S}(E)$ et H est distingué. Il en résulte que H contient :

$$(x, y)(\sigma(x), \sigma(y))(x, y)(\sigma(x), z) = (\sigma(x), \sigma(y))(\sigma(x), z)$$

qui est un 3-cycle. ■

Exercice 2.16 *Montrer que $\mathcal{A}(E)$ est stable par tout automorphisme de $\mathcal{S}(E)$.*

Solution 2.16 *Si φ est un automorphisme de $\mathcal{S}(E)$, alors pour tout 3-cycle $\sigma \in \mathcal{A}(E)$, $\varphi(\sigma)$ est d'ordre 3 dans $\mathcal{S}(E)$. Comme $\varphi(\sigma)$ est produit de cycles et l'ordre de $\varphi(\sigma)$ est le* ppcm *des longueurs de ces cycles, ils sont nécessairement tous d'ordre 3 et $\varphi(\sigma) \in \mathcal{A}(E)$.*

Exercice 2.17 *Décomposer en produit de 3-cycles dans $\mathcal{A}_7$ la permutation :*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \end{pmatrix}$$

Solution 2.17 *On a la décomposition en produit de transpositions :*

$$\sigma = (1, 2)(2, 3)(3, 4)(4, 5)(5, 6)(6, 7)$$

donc $\varepsilon(\sigma) = 1$ et $\sigma \in \mathcal{A}_7$. Puis :

$$\sigma = (2, 3, 1)(4, 5, 3)(6, 7, 5) = (1, 2, 3)(3, 4, 5)(5, 6, 7)$$

Exercice 2.18 *Montrer que, pour $n \geq 3$, $\mathcal{A}_n$ est engendré par les 3-cycles $\gamma_k = (1, 2, k)$ où $3 \leq k \leq n$ (en particulier $\mathcal{A}_4$ est dicyclique engendré par $(1, 2, 3)$ et $(1, 2, 4)$).*

Solution 2.18 *Il suffit de montrer que tout 3-cycle peut s'écrire comme produit de cycles du type $(1, 2, k)$. Pour i, j, k distincts de $1, 2$, on a :*

$$(i, j, k) = (1, 2, i)(2, j, k)(1, 2, i)^{-1}$$

et :

$$(2,j,k)=(1,2,j)(1,2,k)(1,2,j)^{-1}$$

(exercice 2.2).
On peut aussi procéder par récurrence. Pour $n=3$, c'est vrai ($\mathcal{A}_3=\langle(1,2,3)\rangle$). Supposons le résultat acquis pour $n\geq 3$ et soit $\sigma\in\mathcal{A}_{n+1}$. Si $\sigma(n+1)=n+1$, alors la restriction de σ à $\{1,\cdots,n\}$ est dans $\mathcal{A}_n$, donc elle s'écrit comme produit de γ_k avec $3\leq k\leq n$ et il en est de même de σ. Sinon, $\sigma(n+1)=j\leq n$ et avec :

$$\left(\gamma_{n+1}^{-1}\circ\gamma_j\circ\sigma\right)(n+1)=\left(\gamma_{n+1}^{-1}\circ\gamma_j\right)(j)=\left(\gamma_{n+1}^{-1}\right)(1)=n+1$$

on déduit $\sigma'=\gamma_{n+1}^{-1}\circ\gamma_j\circ\sigma\in\mathcal{A}_{n+1}$ est produit de γ_k avec $3\leq k\leq n$ et $\sigma=\gamma_j^{-1}\circ\gamma_{n+1}\circ\sigma=\gamma_j^2\circ\gamma_{n+1}\circ\sigma$ est produit de γ_k avec $3\leq k\leq n+1$.

Exercice 2.19 *Montrer que, pour $n\geq 3$, $\mathcal{A}_n$ est engendré par les 3-cycles $(k,k+1,k+2)$ où $1\leq k\leq n-2$.*

Solution 2.19 *Comme $\mathcal{A}_n$ est engendré par les 3-cycles $\gamma_k=(1,2,k)$ où $3\leq k\leq n$, il suffit d'écrire chaque γ_k comme produit 3-cycles du type $(j,j+1,j+2)$ et $(i,i+1,i+2)^{-1}=(i+2,i+1,i)$ où $1\leq i,j\leq n-2$.*
Pour $4\leq k\leq n$, on a :

$$(1,2,k)=(k-1,k,k+1)(1,2,k-1)(k-1,k,k+1)^{-1}$$

Pour $k=4$, on a $(1,2,k-1)=(1,2,3)$ et c'est terminé, sinon on écrit $(1,2,k-1)=(k-2,k-1,k)(1,2,k-2)(k-2,k-1,k)^{-1}$ et on continue ainsi de suite si nécessaire.
Pour $k=3$, le cycle $(1,2,3)$ est de la forme souhaitée.

Exercice 2.20 *Déterminer, pour $n\geq 4$, le centre de $\mathcal{A}(E)$ (c'est-à-dire l'ensemble des éléments de $\mathcal{A}(E)$ qui commutent à tous les autres éléments de $\mathcal{A}(E)$).*

Solution 2.20 *Si $\sigma\in\mathcal{A}(E)\setminus\{Id\}$, il existe $x\in E$ tel que $y=\sigma(x)\neq x$. On se donne $z\in E\setminus\{x,y,\sigma(y)\}$ (E a au moins 4 éléments) et γ est le 3-cycle $\gamma=(x,y,z)\in\mathcal{A}(E)$. On a alors :*

$$\sigma\gamma(x)=\sigma(y)\ \text{ et }\gamma\sigma(x)=\gamma(y)=z\neq\sigma(y)$$

donc $\sigma\gamma\neq\gamma\sigma$ et $\sigma\notin Z(\mathcal{A}(E))$. Le centre de $\mathcal{A}(E)$ est donc réduit à $\{Id\}$.
Pour $n=3$, $\mathcal{A}(E)$ est cyclique, donc commutatif et $Z(\mathcal{A}(E))=\mathcal{A}(E)$.

Exercice 2.21 *Le groupe $\mathcal{S}(E)$ est-il isomorphe au produit direct $\mathcal{A}(E)\times\{-1,1\}$?*

Solution 2.21 *Pour $n=2$, on a $\mathcal{S}(E)\underset{\rightarrow}{\backsim}\{-1,1\}$ et $\mathcal{A}(E)=\{Id_E\}$, donc $\mathcal{S}(E)$ est isomorphe au produit direct $\mathcal{A}(E)\times\{-1,1\}$.*
Pour $n=3$, $\mathcal{A}(E)$ est d'ordre 3, donc cyclique et $\mathcal{A}(E)\times\{-1,1\}$ qui est commutatif ne peut être isomorphe à $\mathcal{S}(E)$.
Pour $n\geq 4$, $\gamma=(Id,-1)$ est dans le centre de $\mathcal{A}(E)\times\{-1,1\}$, il est d'ordre 2, donc si φ est un isomorphisme de $\mathcal{A}(E)\times\{-1,1\}$ sur $\mathcal{S}(E)$, l'élément $\varphi(\gamma)$ serait d'ordre 2 dans le centre de $\mathcal{S}(E)$, ce qui contredit le fait que $Z(\mathcal{S}(E))=\{Id\}$. Donc $\mathcal{S}(E)$ n'est pas isomorphe au produit direct $\mathcal{A}(E)\times\{-1,1\}$.

Exercice 2.22

1. *Montrer que, pour $n\geq 5$, deux 3-cycles sont conjugués dans $\mathcal{A}(E)$.*

2. *En déduire que le groupe dérivé* $D(\mathcal{A}(E))$ *de* $\mathcal{A}(E)$ *(i. e. le groupe engendré par les commutateurs* $[\sigma,\tau]=\sigma\tau\sigma^{-1}\tau^{-1}$ *où* σ *et* τ *sont dans* $\mathcal{A}(E)$*) est* $\mathcal{A}(E)$.

Solution 2.22

1. *On sait déjà que deux 3-cycles sont conjugués dans* $\mathcal{S}(E)$ *(exercice 2.2).*
   Soient $\gamma=(x_1,x_2,x_3)$ *et* $\gamma'=(x'_1,x'_2,x'_3)$ *deux 3-cycles. On se donne une permutation* $\sigma\in\mathcal{S}(E)$ *telle que* $\sigma(x_k)=x'_k$ *pour* $k=1,2,3$ *et on a alors* $\sigma^{-1}\gamma'\sigma=\gamma$. *En effet, on a* $\gamma(x_k)=x_{k+1}$ *pour* $k=1,2$ *[resp.* $\gamma(x_3)=x_1$*] et* $\sigma^{-1}\gamma'\sigma(x_k)=\sigma^{-1}\gamma'(x'_k)=\sigma^{-1}\left(x'_{k+1}\right)=x_{k+1}$ *pour* $k=1,2$ *[resp.* $\sigma^{-1}\gamma'\sigma(x_3)=\sigma^{-1}\gamma(x'_3)=\sigma^{-1}(x'_1)=x_1$*] et pour* $x\notin\{x_1,x_2,x_3\}$, *on a* $\gamma(x)=x$ *et* $\sigma^{-1}\gamma'\sigma(x)=\sigma^{-1}(\sigma(x))=x$ *puisque* $\sigma(x)\notin\{x'_1,x'_2,x'_3\}$.
   Si $\sigma\in\mathcal{A}(E)$, *c'est terminé, sinon en prenant* x_4,x_5 *dans* $E\setminus\{x_1,x_2,x_3\}$ *(*E *a au moins* 5 *éléments), la permutation* $\sigma'=(x_4,x_5)\sigma$ *est dans* $\mathcal{A}(E)$ *avec* $\sigma'(x_k)=x'_k$ *pour* $k=1,2,3$ *et on est ramené au cas précédent.*
2. *Comme* $\mathcal{A}(E)$ *est engendré par les 3-cycles, il suffit de montrer que tout 3-cycle est dans* $D(\mathcal{A}(E))$. *Si* γ *est un 3-cycle, il en est de même de* $\gamma^{-1}=\gamma^2$, *donc* γ^2 *est conjugué à* γ *dans* $\mathcal{A}(E)$, *c'est-à-dire qu'il existe* $\sigma\in\mathcal{A}(E)$ *tel que* $\gamma^2=\sigma^{-1}\gamma\sigma$ *et* $\gamma=\gamma^{-1}\sigma^{-1}\gamma\sigma\in D(\mathcal{A}(E))$.

Exercice 2.23 *On se propose de montrer que, pour* $n=5$, $\mathcal{A}(E)$ *est simple (i. e. n'a pas de sous-groupes distingués autres que lui même et* $\{Id\}$*). Ici* E *est un ensemble à* 5 *éléments.*

1. *Donner une description de* $\mathcal{A}(E)$ *en classant ses élément en fonction de leur ordre.*
2. *Montrer que* $\mathcal{A}(E)$ *est simple.*

Solution 2.23

1. *Pour* $n=5$, *notons* $E=\{x_1,x_2,x_3,x_4,x_5\}$ *et pour* $1\leq i\neq j\leq 5,\tau_{ij}$ *la transposition* (x_i,x_j) *dans* $\mathcal{S}(E)$. *On décrit d'abord le groupe* $\mathcal{A}(E)$.
   Dans ce groupe, on a les 60 *éléments distincts suivants :*
   - *l'identité ;*
   - $\dfrac{C_5^2C_3^2}{2}=15$ *éléments d'ordre* 2 *donnés par le produit de deux transpositions de supports disjoints :* $\tau_{12}\circ\tau_{34}$, $\tau_{12}\circ\tau_{35}$, $\tau_{12}\circ\tau_{45}$, $\cdots$ *(deux transpositions de supports disjoints commutent et leur produit est d'ordre* 2*) ;*
   - $2C_5^3=20$ *cycles d'ordre* 3 *distincts (un même support à* 3 *éléments donne* 2 *cycles) ;*
   - $4!=24$ *cycles d'ordre* 5 *:* (x_1,x_2,x_3,x_4,x_5), (x_1,x_3,x_4,x_5,x_2), $\cdots$ *(si* $\gamma^5=1$, *alors* $\gamma^{-1}=\gamma^4\in\mathcal{A}(E)$ *et* $\gamma\in\mathcal{A}(E)$*)*

   et on a ainsi tous les éléments puisque $\mathcal{A}(E)$ *est de cardinal* $\dfrac{5!}{2}=60$.
2. *Soit* H *un sous-groupe distingué de* $\mathcal{A}(E)$ *non réduit à* $\{Id\}$.
   Si H *contient un 3-cycle, il les contient alors tous puisqu'ils sont conjugués et* $H=\mathcal{A}(E)$ *puisque les 3-cycles engendrent* $\mathcal{A}(E)$.
   Si H *contient un produit* $\sigma=(x,y)(z,t)$ *de deux transpositions de supports disjoints, il contient alors, pour* $u\in E\setminus\{x,y,z,t\}$, *le commutateur :*

$$\begin{aligned}\sigma(x,y,u)\,\sigma^{-1}(x,y,u)^{-1}&=(\sigma(x),\sigma(y),\sigma(u))(u,y,x)\\&=(y,x,u)(u,y,x)=(x,y,u)\end{aligned}$$

($\sigma \in H$, donc $\sigma^{-1} \in H$ puisque H est un groupe et $(x,y,u)\,\sigma^{-1}\,(x,y,u)^{-1} \in H$ puisque H est distingué) qui est un 3-cycle, donc $H = \mathcal{A}(E)$.

Si H contient un 5-cycle $\sigma = (x,y,z,t,u)$, il contient alors le commutateur :

$$\begin{aligned}(x,y,z)\,\sigma\,(x,y,z)^{-1}\,\sigma^{-1} &= (x,y,z)\,\sigma\,(z,y,x)\,\sigma^{-1} = (x,y,z)\,(\sigma(z),\sigma(y),\sigma(x)) \\ &= (x,y,z)\,(t,z,y) = (y,t,x)\end{aligned}$$

qui est un 3-cycle, donc $H = \mathcal{A}(E)$.

En utilisant les groupes de Sylow, on peut montrer qu'un groupe simple d'ordre 60 est isomorphe à $\mathcal{A}_5$ (cf Pellerin).

Plus généralement, on a le résultat suivant.

Théorème 2.12 *Pour $n = 3$ ou $n \geq 5$ le groupe $\mathcal{A}(E)$ est simple (i. e. n'a pas de sous-groupes distingués autres que lui même et $\{Id\}$).*

Démonstration. Pour $n = 3$, $\mathcal{A}(E)$ est cyclique d'ordre 3 et n'a pas de sous-groupe trivial.

On suppose $n \geq 5$ et on se donne un sous-groupe distingué H de $\mathcal{A}(E)$ distinct de $\{Id\}$. Pour montrer que $H = \mathcal{A}(E)$, il suffit de montrer que H contient un 3-cycle puisqu'ils sont tous conjugués dans $\mathcal{A}(E)$ et l'engendrent.

On se donne $\sigma \in H \setminus \{Id\}$ et $\gamma = (x,z,y) \in \mathcal{A}(E)$ un 3-cycle avec $y = \sigma(x)$ qui ne commute pas à σ (voir l'exercice 2.20). Comme H est distingué dans $\mathcal{A}(E)$, on a :

$$\sigma' = \sigma\gamma\sigma^{-1}\gamma^{-1} = \sigma\left(\gamma\sigma^{-1}\gamma^{-1}\right) \in H$$

et en écrivant que :

$$\begin{aligned}\sigma' &= \left(\sigma(x,z,y)\,\sigma^{-1}\right)(y,z,x) = (\sigma(x),\sigma(z),\sigma(y))\,(y,z,x) \\ &= (y,\sigma(z),\sigma(y))\,(y,z,x)\end{aligned}$$

on voit que σ' est produit de deux 3-cycles qui agissent sur l'ensemble $F = \{x,y,z,\sigma(y),\sigma(z)\}$ formé d'au plus 5 éléments (tous les points de $E \setminus F$ sont fixes).

L'égalité $\sigma' = Id$ est réalisée si, et seulement si, $\sigma\gamma\sigma^{-1}\gamma^{-1} = Id$, soit $\tau\sigma = \gamma\sigma$, ce qui n'est pas, donc $\sigma' \neq Id$.

Dans $\mathcal{S}(F)$ la permutation σ' s'écrit comme produit de cycles de supports disjoints, cette décomposition étant celle de $\mathcal{S}(E)$ et comme $\sigma' \in \mathcal{A}(E)$, il n'y a que trois possibilités : σ' est soit un 3-cycle, soit un produit de deux transpositions de supports disjoints, soit un 5-cycle.

Dans le premier cas c'est terminé.

Dans le deuxième cas, on a $\sigma' = (x_1,x_2)\,(x_3,x_4)$ et choisissant $x_5 \in E \setminus \{x_1,x_2,x_3,x_4\}$, on a :

$$\sigma'' = (x_1,x_5)\,\sigma'\,(x_1,x_5)\,(\sigma')^{-1} = \left((x_1,x_5)\,\sigma'\,(x_1,x_5)^{-1}\right)(\sigma')^{-1} \in H$$

avec :

$$\sigma'' = (x_1,x_5)\,(\sigma'(x_1),\sigma'(x_5)) = (x_1,x_5)\,(x_2,x_5) = (x_1,x_5,x_2)$$

et c'est terminé.

Dans le troisième cas, on a $\sigma' = (x_1,x_2,x_3,x_4,x_5)$ et :

$$\sigma'' = (x_1,x_2)\,\sigma'\,(x_1,x_2)\,(\sigma')^{-1} = \left((x_1,x_2)\,\sigma'\,(x_1,x_2)^{-1}\right)(\sigma')^{-1} \in H$$

avec :

$$\sigma'' = (x_1,x_2)\,(\sigma'(x_1),\sigma'(x_2)) = (x_1,x_2)\,(x_2,x_3) = (x_1,x_3,x_2)$$

et c'est terminé. ∎

Exercice 2.24 *On se propose de montrer ici que pour $n \geq 2$, il n'existe pas de morphisme de groupes injectif de $\mathcal{S}_n$ dans $\mathcal{A}_{n+1}$.*

1. *Montrer le résultat pour $n = 2$ et $n = 3$.*
2. *Montrer le résultat pour n pair.*
3. *On suppose que $n = 2p+1$ est impair avec $p \geq 2$ et qu'il existe un morphisme de groupes injectif φ de $\mathcal{S}_{2p+1}$ dans $\mathcal{A}_{2p+2}$. On note $H = \varphi(\mathcal{S}_{2p+1})$ et $E = \mathcal{A}_{2p+2}/H$ est l'ensemble quotient des classes à gauche modulo H.*

   (a) *Montrer que l'application :*

$$\begin{array}{rccc} \psi: & \mathcal{A}_{2p+2} & \to & \mathcal{S}(E) \\ & \sigma & \mapsto & (\gamma H \mapsto \sigma\gamma H) \end{array}$$

   est un morphisme de groupes (action par translation à gauche de $\mathcal{A}_{2p+2}$ sur E).

   (b) *Conclure en utilisant le fait que $\mathcal{A}_{2p+2}$ est simple.*

Solution 2.24

1. *Pour $n = 2$, on a $\mathcal{S}_2 = \{Id, (1,2)\}$ qui est d'ordre 2 et $\mathcal{A}_3$ qui est d'ordre 3, il ne peut donc exister de morphisme de groupes injectif de $\mathcal{S}_2$ dans $\mathcal{A}_3$.*
   Pour $n = 3$, $\mathcal{S}_3$ est d'ordre 6 et $\mathcal{A}_4$ n'a pas de sous-groupe d'ordre 6 (exercice 2.14), il ne peut donc exister de morphisme de groupes injectif de $\mathcal{S}_3$ dans $\mathcal{A}_4$.
2. *On suppose que $n \geq 4$. Comme $\mathcal{S}_n$ est d'ordre $n!$ et $\mathcal{A}_{n+1}$ d'ordre $\dfrac{(n+1)!}{2}$, une condition nécessaire est que $n!$ divise $\dfrac{(n+1)!}{2}$, ce qui revient à dire que $n+1$ est pair, ou encore que $n = 2p+1$ est impair avec $p \geq 2$.*
3. *$H = \varphi(\mathcal{S}_{2p+1})$ est un sous-groupe d'ordre $(2p+1)!$ de $\mathcal{A}_{2p+2}$ et l'ensemble quotient $E = \mathcal{A}_{2p+2}/H$ des classes à gauche modulo H est de cardinal $\dfrac{(2p+2)!}{2(2p+1)!} = p+1$.*

   (a) *Pour σ et γ dans $\mathcal{A}_{2p+2}$, $\sigma\gamma H$ est dans E ; $\sigma\gamma H = \sigma\gamma' H$ entraîne $\gamma H = \gamma' H$, donc $\psi(\sigma)$ est injective et $\gamma' H = \sigma\sigma^{-1}\gamma' H$ avec $\sigma^{-1}\gamma' \in \mathcal{A}_{2p+2}$ et $\sigma^{-1}\gamma' H \in E$, donc $\psi(\sigma)$ est surjective et c'est bien un élément de $\mathcal{S}(E)$; pour σ, σ', γ dans $\mathcal{A}_{2p+2}$, on a :*

$$\psi(\sigma\sigma')(\gamma H) = \sigma\sigma'\gamma H = \psi(\sigma) \circ \psi(\sigma')(\gamma H)$$

   et $\psi(\sigma\sigma') = \psi(\sigma) \circ \psi(\sigma')$, donc ψ est bien un morphisme de groupes.

   (b) *Comme $\mathcal{A}_{2p+2}$ est simple pour $p \geq 2$, $\ker(\psi)$ qui est distingué dans $\mathcal{A}_{2p+2}$ est $\{Id\}$ ou $\mathcal{A}_{2p+2}$. Avec $\operatorname{card}(\mathcal{S}(E)) = (p+1)!$ et :*

$$\operatorname{card}(\mathcal{A}_{2p+2}) = \frac{(2p+2)!}{2} = (p+1)(2p+1)! > (p+1)!$$

   on déduit que ψ ne peut être injectif et $\ker(\psi) = \mathcal{A}_{2p+2}$, ce qui entraîne que pour tout $\sigma \in \mathcal{A}_{2p+2}$, on a $\psi(\sigma)(H) = H$, soit $\sigma H = H$, donc $\sigma \in H$ et $\mathcal{A}_{2p+2} \subset H \subset \mathcal{A}_{2p+2}$, soit $H = \mathcal{A}_{2p+2}$ avec $\operatorname{card}(H) = (2p+1)!$ et $\operatorname{card}(\mathcal{A}_{2p+2}) = (p+1)(2p+1)!$, ce qui est impossible.

Exercice 2.25 *Soit p un nombre premier avec $p \geq 5$ et H un sous-groupe strict de $\mathcal{S}_p$ d'indice $r \leq p-1$.*

1. *Montrer que H contient tous les cycles d'ordre p.*
2. *Montrer que H contient tous les cycles d'ordre 3, puis que $H = \mathcal{A}_p$.*
3. *En déduire qu'il n'existe pas dans $\mathcal{S}_5$ de groupe d'ordre 30 ou 40.*

Solution 2.25

1. *Soit σ un p-cycle et $\overline{\sigma} = \sigma H$ sa classe à gauche modulo H. Comme $r = \operatorname{card}(\mathcal{S}_p/H) \leq p-1$, il existe deux entiers $j < j$ compris entre 0 et $p-1$ tels que $\overline{\sigma}^k = \overline{\sigma}^j$, ce qui revient à dire que $\overline{\sigma}^{k-j} = \overline{\sigma^{k-j}} = \overline{1}$ ou encore que $\sigma^s \in H$ avec $1 \leq s = k-j \leq p-1$. Comme p est premier, il est premier avec s et il existe u, v dans $\mathbb{Z}$ tels que $us + vp = 1$, ce qui donne, compte tenu du fait que σ est d'ordre p dans $\mathcal{S}_p$, $\sigma = \sigma^{us+vp} = (\sigma^s)^u \in H$.*
2. *Soit $\gamma = (x_1, x_2, x_3)$ un 3-cycle. En désignant par $x_4, \cdots, x_p$ les autres éléments de $E = \{1, \cdots, p\}$ (on a $p \geq 5$), on a :*

$$(x_2, x_3, x_1, x_4, \cdots, x_p)^{-1} (x_2, x_1, x_3, x_4, \cdots, x_p) = (x_p, x_{p-1}, \cdots, x_1, x_3, x_2) (x_2, x_1, x_3, x_4, \cdots, x_p) = \gamma$$

et $\gamma \in H$. Comme $\mathcal{A}_p$ est engendré par les 3-cycles, on en déduit que $\mathcal{A}_p \subset H$ et $\operatorname{card}(\mathcal{A}_p) = \dfrac{p!}{2} \leq \operatorname{card}(H) = \dfrac{p!}{r}$, donc $r = 1$ ou $r = 2$. Mais $r = 1$ signifie que $H = \mathcal{S}_p$, ce qui n'est pas. On a donc $r = 2$ et $\mathcal{A}_p = H$.
3. *On a $\operatorname{card}(\mathcal{S}_5) = 120$ et $\operatorname{card}(\mathcal{A}_5) = 60$. Si H est un sous-groupe de $\mathcal{S}_5$ d'ordre 30 ou 40, son indice est 4 ou 3 et H devrait être égal à $\mathcal{A}_5$, ce qui n'est pas possible vu les cardinaux.*

Exercice 2.26 *On se propose de montrer que, pour $n \geq 5$, les sous-groupes d'indice n de $\mathcal{S}_n$ sont isomorphes à $\mathcal{S}_{n-1}$.*
Soit H un sous-groupe d'indice n de $\mathcal{S}_n$. On note $E = \mathcal{S}_n/H$ l'ensemble quotient des classes à gauche modulo H.

1. *Montrer que l'application :*

$$\begin{array}{rccc} \psi : & \mathcal{S}_n & \to & \mathcal{S}(E) \\ & \sigma & \mapsto & (\gamma H \mapsto \sigma\gamma H) \end{array}$$

est un morphisme de groupes injectif (action par translation à gauche de $\mathcal{A}_{2p+2}$ sur E).
2. *Conclure.*

Solution 2.26

1. *Pour σ et γ dans $\mathcal{S}_n$, $\sigma\gamma H$ est dans E ; $\sigma\gamma H = \sigma\gamma' H$ entraîne $\gamma H = \gamma' H$, donc $\psi(\sigma)$ est injective et $\gamma' H = \sigma\sigma^{-1}\gamma' H$ avec $\sigma^{-1}\gamma' \in \mathcal{S}_n$ et $\sigma^{-1}\gamma' H \in E$, donc $\psi(\sigma)$ est surjective et c'est bien un élément de $\mathcal{S}(E)$; pour σ, σ', γ dans $\mathcal{S}_n$, on a :*

$$\psi(\sigma\sigma')(\gamma H) = \sigma\sigma'\gamma H = \psi(\sigma) \circ \psi(\sigma')(\gamma H)$$

et $\psi(\sigma\sigma') = \psi(\sigma) \circ \psi(\sigma')$, donc ψ est bien un morphisme de groupes.
Le noyau de ψ est un sous-groupe distingué de $\mathcal{S}_n$, c'est donc $\{Id\}$, $\mathcal{A}_n$ ou $\mathcal{S}_n$ (on a $n \geq 5$). Si $\sigma \in \ker(\psi)$, on a alors $\sigma\gamma H = \gamma H$ pour tout $\gamma \in \mathcal{S}_n$, donc $\sigma H = H$ et $\sigma \in H$. On a donc $\ker(\psi) \subset H$ avec $\operatorname{card}(H) = \dfrac{\operatorname{card}(\mathcal{S}_n)}{n} = (n-1)!$ (H est d'indice n dans $\mathcal{S}_n$), donc $\ker(\psi) = \{Id\}$ (ce ne peut être $\mathcal{S}_n$ puisque $\operatorname{card}(\ker(\psi)) \leq (n-1)!$ et ce ne peut être $\mathcal{A}_n$ puisque $\dfrac{n!}{2}$ ne divise pas $(n-1)!$ pour $n \geq 3$) et ψ est injectif.

2. *$\psi(H)$ est un sous-groupe de $\mathcal{S}(E)$ isomorphe à H de cardinal $(n-1)!$ avec E de cardinal n. Mais les éléments de $\psi(H) \subset \mathcal{S}(E)$ laissent fixe $H = \overline{Id}$ (pour $\sigma \in H$, $\psi(\sigma)(H) = \sigma H = H$), donc $\psi(H) \subset \mathcal{S}(E \setminus \{H\})$ et ces ensembles sont égaux puisque de même cardinal $(n-1)!$ En définitive H est isomorphe à $\psi(H) = \mathcal{S}(E \setminus \{H\})$, donc à $\mathcal{S}_{n-1}$.*
   Pour $n = 4$, le résultat est encore valable (voir Ortiz, p. 28).
   Pour $n = 3$, un sous-groupe d'indice 3 de $\mathcal{S}_3$ est d'ordre 2, donc commutatif et isomorphe à $\mathcal{S}_2$.

Exercice 2.27 *Montrer que si H est un sous-groupe d'indice r compris entre 2 et $n-1$ de $\mathcal{S}_n$, avec $n \geq 5$, alors $r = 2$ et $H = \mathcal{A}_n$.*

Solution 2.27 *L'ensemble quotient $E = \mathcal{S}_n/H$ des classes à gauche modulo H est de cardinal r et le morphisme de groupes :*

$$\begin{array}{rccc} \psi: & \mathcal{S}_n & \to & \mathcal{S}(E) \\ & \sigma & \mapsto & (\gamma H \mapsto \sigma\gamma H) \end{array}$$

ne peut être injectif puisque $\mathrm{card}(\mathcal{S}_n) = n! > \mathrm{card}(\mathcal{S}(E)) = r!$ *Son noyau est donc $\mathcal{A}_n$ (ce ne peut être $\mathcal{S}_n$ puisque $H \neq \mathcal{S}_n$). On a donc $\mathcal{A}_n = \ker(\psi) \subset H$ (si $\sigma \in \ker(\psi)$, on a alors $\sigma\gamma H = \gamma H$ pour tout $\gamma \in \mathcal{S}_n$ et $\sigma \in H$) et* $\mathrm{card}(\mathcal{A}_n) = \dfrac{n!}{2}$ *divise* $\mathrm{card}(H) = \dfrac{n!}{r}$, *ce qui impose $r = 2$ et $H = \mathcal{A}_n$.*

2.8 Utilisations du groupe symétrique

2.8.1 Dérangements d'un ensemble fini

Exercice 2.28 *On appelle dérangement de l'ensemble $I_n = \{1, 2, \cdots, n\}$ toute permutation σ de cet ensemble n'ayant aucun point fixe (i. e. telle que $\sigma(i) \neq i$ pour tout $i \in I_n$). Pour tout entier naturel non nul p, on note δ_p le nombre de dérangements de I_p. On a $\delta_1 = 0$ et, par convention, on pose $\delta_0 = 1$.*

1. *Soient $(f_n)_{n\in\mathbb{N}}$ et $(g_n)_{n\in\mathbb{N}}$ deux suites de réels telles que :*

$$\forall n \in \mathbb{N},\ f_n = \sum_{k=0}^{n} C_n^k g_k.$$

   Montrer que :

$$\forall n \in \mathbb{N},\ g_n = \sum_{k=0}^{n} (-1)^{n-k} C_n^k f_k.$$

   (Formule d'inversion de Pascal).

2. *Montrer que :*

$$\forall n \in \mathbb{N},\ n! = \sum_{k=0}^{n} C_n^k \delta_k. \tag{2.1}$$

3. *En déduire, en utilisant la formule d'inversion de Pascal, que :*

$$\forall n \in \mathbb{N},\ \delta_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

4. *Montrer ce résultat directement, sans utiliser la formule d'inversion de Pascal.*
5. *On se propose de montrer le résultat précédent en utilisant la série entière* $\sum \frac{\delta_n}{n!} z^n$.
   (a) *Montrer que la série entière* $\sum \frac{\delta_n}{n!} z^n$ *est convergente pour* $|z| < 1$. *On note* $f(z)$ *sa somme.*
   (b) *En utilisant* (2.1), *montrer que, pour* $|z| < 1$, *on a :*
   $$f(z) = \frac{e^{-z}}{1-z}$$
   (c) *En déduire que* $\delta_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$.
   (d) *Montrer que* $\delta_n = E\left(\frac{n!}{e} + \frac{1}{2}\right)$ *pour tout* $n \geq 1$, *où* E *est la fonction partie entière.*
6. *On considère* n *couples qui se présentent à un concours de danse, chaque danseur choisissant une partenaire au hasard.*
   (a) *Quelle est la probabilité* p_n *pour que personne ne danse avec son conjoint ?*
   (b) *Calculer la limite de* p_n *quand* n *tend vers l'infini.*

Solution 2.28

1. *Pour* $n = 0$, *c'est clair. En supposant* $n \geq 1$, *on note* F *et* G *les vecteurs de* $\mathbb{R}^{n+1}$ *définis par* $F = (f_k)_{0 \leq k \leq n}$, $G = (g_k)_{0 \leq k \leq n}$ *et on a* $F = PG$, *où* P *est la matrice carrée d'ordre* $n+1$ *:*
$$P = \begin{pmatrix} C_0^0 & 0 & \cdots & \cdots & 0 \\ C_1^0 & C_1^1 & 0 & \cdots & 0 \\ C_2^0 & C_2^1 & C_2^2 & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & 0 \\ C_n^0 & C_n^1 & \cdots & C_n^{n-1} & C_n^n \end{pmatrix}$$
et il s'agit alors de montrer que P *est inversible, puis de calculer son inverse.*
En écrivant, pour k *compris entre* 0 *et* n, *l'égalité dans* $\mathbb{R}_n[X]$ *:*
$$(1+X)^k = \sum_{j=0}^{k} C_k^j X^j$$
on remarque que $P = {}^tQ$, *où :*
$$Q = \begin{pmatrix} C_0^0 & C_1^0 & C_2^0 & \cdots & C_n^0 \\ 0 & C_1^1 & C_2^1 & \cdots & C_n^1 \\ 0 & 0 & C_2^2 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & C_n^{n-1} \\ 0 & 0 & \cdots & 0 & C_n^n \end{pmatrix}$$
est la matrice de passage de la base canonique $\left(X^k\right)_{0 \leq k \leq n}$ *de* $\mathbb{R}_n[X]$ *à la base* $\left((1+X)^k\right)_{0 \leq k \leq n}$.
La matrice Q *est inversible et son inverse est la matrice de passage de* $\left((1+X)^k\right)_{0 \leq k \leq n}$

à $\left(X^k\right)_{0\leq k\leq n}$, *qui s'obtient avec :*

$$X^k = (1+X-1)^k = \sum_{j=0}^{k} C_k^j \,(1+X)^j \,(-1)^{k-j}$$

On a donc :

$$Q^{-1} = \begin{pmatrix} C_0^0 & -C_1^0 & C_2^0 & \cdots & (-1)^n C_n^0 \\ 0 & C_1^1 & -C_2^1 & \cdots & (-1)^{n-1} C_n^1 \\ 0 & 0 & C_2^2 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & (-1)\, C_n^{n-1} \\ 0 & 0 & \cdots & 0 & C_n^n \end{pmatrix}$$

et :

$$P^{-1} = {}^tQ^{-1} = \begin{pmatrix} C_0^0 & 0 & \cdots & \cdots & 0 \\ -C_1^0 & C_1^1 & 0 & \cdots & 0 \\ C_2^0 & -C_2^1 & C_2^2 & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & 0 \\ (-1)^n C_n^0 & (-1)^{n-1} C_n^1 & \cdots & (-1)\, C_n^{n-1} & C_n^n \end{pmatrix}$$

L'égalité $G = P^{-1}F$ *nous donne alors :*

$$g_n = \sum_{k=0}^{n} (-1)^{n-k} \, C_n^k f_k$$

On peut aussi procéder par récurrence sur $n \geq 0$.
Pour $n = 0$, *c'est clair et supposant le résultat acquis jusqu'au rang* $n \geq 0$, *on a :*

$$\begin{aligned} g_{n+1} &= f_{n+1} - \sum_{k=0}^{n} C_{n+1}^k g_k = f_{n+1} - \sum_{k=0}^{n} C_{n+1}^k \sum_{j=0}^{k} (-1)^{k-j} \, C_k^j f_j \\ &= f_{n+1} + \sum_{j=0}^{n} \left(\sum_{k=j}^{n} C_{n+1}^k \,(-1)^{k-j+1} \, C_k^j \right) f_j \end{aligned}$$

avec :

$$\begin{aligned} \sum_{k=j}^{n} C_{n+1}^k \,(-1)^{k-j+1} \, C_k^j &= \sum_{k=j}^{n} \frac{(n+1)!}{k!\,(n+1-k)!} \frac{k!}{j!\,(k-j)!} \,(-1)^{k-j+1} \\ &= \frac{(n+1)!}{j!\,(n+1-j)!} \,(-1)^{n+1-j} \sum_{k=j}^{n} \frac{(n+1-j)!}{(n+1-k)!\,(k-j)!} \,(-1)^{k-n} \\ &= C_{n+1}^j \,(-1)^{n+1-j} \sum_{k=j}^{n} C_{n+1-j}^{k-j} \,(-1)^{n-k} \\ &= -C_{n+1}^j \sum_{i=0}^{n-j} C_{n-j+1}^i \,(-1)^i \end{aligned}$$

et :

$$\begin{aligned} \sum_{i=0}^{n-j} C_{n-j+1}^i \,(-1)^i &= \sum_{i=1}^{n-j+1} C_{n-j+1}^i \,(-1)^i - (-1)^{n-j+1} \\ &= (1-1)^{n-j+1} + (-1)^{n-j} = (-1)^{n-j} \end{aligned}$$

ce qui donne :

$$\sum_{k=j}^{n} C_{n+1}^{k} (-1)^{k-j+1} C_k^j = C_{n+1}^{j} (-1)^{n+1-j}$$

et :

$$g_{n+1} = f_{n+1} + \sum_{j=0}^{n} C_{n+1}^{j} (-1)^{n+1-j} f_j = \sum_{j=0}^{n+1} C_{n+1}^{j} (-1)^{n+1-j} f_j$$

2. *Pour $n = 0$ c'est clair vu les conventions $0! = \delta_0 = 1$.*
   Pour $n \geq 1$, $n!$ qui est le nombre de permutations de I_n peut s'écrire $n! = \sum_{k=0}^{n} \pi_{n,k}$, où $\pi_{n,k}$ est le nombre de permutations de I_n ayant exactement k points fixes. En choisissant un ensemble de k points fixes dans I_n, il y a δ_{n-k} dérangements possibles pour les $n-k$ points restants et comme il y a C_n^k façons de choisir ces k points fixes, on déduit que $\pi_{n,k} = C_n^k \delta_{n-k}$ et :

$$n! = \sum_{k=0}^{n} C_n^k \delta_{n-k} = \sum_{k=0}^{n} C_n^{n-k} \delta_k = \sum_{k=0}^{n} C_n^k \delta_k.$$

3. *Avec la formule d'inversion de Pascal, on en déduit que :*

$$\delta_n = \sum_{k=0}^{n} (-1)^{n-k} C_n^k k! = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

4. *On peut aussi écrire que :*

$$\begin{aligned} n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} &= \sum_{k=0}^{n} (-1)^k \frac{n!}{k!\,(n-k)!} (n-k)! \\ &= \sum_{k=0}^{n} (-1)^k C_n^k \sum_{j=0}^{n-k} C_{n-k}^{j} \delta_j \\ &= \sum_{j=0}^{n} \left(\sum_{k=0}^{n-j} (-1)^k C_n^k C_{n-k}^{j} \right) \delta_j \end{aligned}$$

($0 \leq j \leq n-k \Leftrightarrow 0 \leq k \leq n-j$) et remarquer que, pour $0 \leq j \leq n$, on a :

$$\begin{aligned} \sum_{k=0}^{n-j} (-1)^k C_n^k C_{n-k}^{j} &= \sum_{k=0}^{n-j} (-1)^k \frac{n!}{k!\,(n-k)!} \frac{(n-k)!}{j!\,(n-k-j)!} \\ &= \frac{n!}{j!} \sum_{k=0}^{n-j} (-1)^k \frac{1}{k!\,(n-k-j)!} \\ &= \frac{n!}{j!\,(n-j)!} \sum_{k=0}^{n-j} (-1)^k \frac{(n-j)!}{k!\,(n-k-j)!} \\ &= C_n^j \sum_{k=0}^{n-j} (-1)^k C_{n-j}^{k} = C_n^j (1-1)^{n-j} = \begin{cases} 0 \ si\ 0 \leq j \leq n-1 \\ 1 \ si\ j = n \end{cases} \end{aligned}$$

ce qui nous donne $n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} = \delta_n$.

5.

(a) Comme $0 \leq \dfrac{\delta_n}{n!} \leq 1$ *pour tout* $n \geq 0$, *la série entière* $\sum \dfrac{\delta_n}{n!} z^n$ *est convergente pour* $|z| < 1$.

(b) Pour $|z| < 1$, *on a le produit de Cauchy des séries entières :*

$$\begin{aligned} f(z)\, e^z &= \left(\sum_{n=0}^{+\infty} \frac{\delta_n}{n!} z^n\right)\left(\sum_{n=0}^{+\infty} \frac{1}{n!} z^n\right) \\ &= \sum_{n=0}^{+\infty} \left(\sum_{k=0}^{n} \frac{\delta_k}{k!} \frac{1}{(n-k)!}\right) z^n \\ &= \sum_{n=0}^{+\infty} \frac{1}{n!} \left(\sum_{k=0}^{n} C_n^k \delta_k\right) z^n = \sum_{n=0}^{+\infty} z^n = \frac{1}{1-z} \end{aligned}$$

et donc :

$$f(z) = \frac{e^{-z}}{1-z}$$

(c) Utilisant à nouveau le produit de Cauchy des séries entières, on en déduit que :

$$f(z) = \sum_{n=0}^{+\infty} \frac{\delta_n}{n!} z^n = \left(\sum_{n=0}^{+\infty} \frac{(-1)^n}{n!} z^n\right)\left(\sum_{n=0}^{+\infty} z^n\right) = \sum_{n=0}^{+\infty} \left(\sum_{k=0}^{n} \frac{(-1)^k}{k!}\right) z^n$$

et on retrouve $\delta_n = n! \sum_{k=0}^{n} \dfrac{(-1)^k}{k!}$.

(d) On a, pour tout $n \geq 0$ *:*

$$e^{-1} = \sum_{n=0}^{+\infty} \frac{(-1)^n}{n!} = \frac{\delta_n}{n!} + R_n$$

où :

$$|R_n| = \left|\sum_{k=n+1}^{+\infty} \frac{(-1)^k}{k!}\right| \leq \frac{1}{(n+1)!}$$

(majoration du reste d'une série alternée). Il en résulte que, pour $n \geq 2$, *on a :*

$$\left|\frac{n!}{e} - \delta_n\right| = n!\,|R_n| \leq \frac{1}{n+1} < \frac{1}{2}$$

donc :

$$-\frac{1}{2} < \frac{n!}{e} - \delta_n < \frac{1}{2}$$

et :

$$\delta_n < \frac{n!}{e} + \frac{1}{2} < \delta_n + 1$$

ce qui entraîne que $\delta_n = E\left(\dfrac{n!}{e} + \dfrac{1}{2}\right)$.

Pour $n = 1$, *on a* $\delta_1 = 0 = E\left(\dfrac{1}{e} + \dfrac{1}{2}\right)$.

6.

(a) En supposant qu'on est dans le cadre de l'équiprobabilité, on a :

$$p_n = \frac{\delta_n}{n!} = \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

(b) $\lim_{n\to+\infty} p_n = \frac{1}{e}$.

2.8.2 Le théorème de Cayley

Théorème 2.13 (Cayley) *Tout groupe G est isomorphe à un sous-groupe de $\mathcal{S}(G)$.*

Démonstration. Soit G un groupe. Pour tout $g \in G$, l'application :

$$\varphi(g) : h \mapsto g \cdot h$$

est dans $\mathcal{S}(G)$. En effet, pour tout $k \in G$, l'équation $g \cdot h = k$ a une unique solution donnée par $h = g^{-1}k$, ce qui signifie que $\varphi(g)$ est une bijection de G sur lui même.

Avec :

$$\varphi(gg')(h) = gg'h = \varphi(g)(\varphi(g')(h)) = \varphi(g) \circ \varphi(g')(h)$$

pour tous g, g', h dans G, on déduit que $\varphi(gg') = \varphi(g) \circ \varphi(g')$ pour tous g, g' dans G, ce qui signifie que φ est un morphisme de groupes.

Enfin, si $g \in \ker(\varphi)$, on a $g \cdot h = h$ pour tout $h \in G$ et $g = 1$, donc φ est injectif et réalise un isomorphisme de G sur $\mathrm{Im}(\varphi)$ qui est un sous-groupe de $\mathcal{S}(G)$. ∎

Exercice 2.29 *Soient G un groupe d'ordre $n \geq 2$ et $\varphi : g \mapsto (\varphi(g) : h \mapsto g \cdot h)$ l'injection de G dans $\mathcal{S}(G)$.*

1. *Montrer que, pour tout $g \in G \setminus \{1\}$, la permutation $\varphi(g)$ se décompose en produit de cycles tous de longueur égale à l'ordre $\theta(g)$ de g dans G.*
2. *En déduire la signature de $\varphi(g)$ pour tout $g \in G$.*
3. *En déduire que, si G est un groupe d'ordre impair, il est alors isomorphe à un sous-groupe du groupe alterné $\mathcal{A}(G)$.*

Solution 2.29 *Notons $G = \{1, g_1, \cdots, g_{n-1}\}$.*

1. *Pour $g = 1$, on a $\varphi(1) = Id$.*
   Pour g d'ordre $m \geq 2$, en notant $r = [G, \langle g\rangle]$ l'indice de $H = \langle g\rangle$ dans G, on a $H\backslash G = \{H, Hg_1, \cdots, Hg_{r-1}\}$ (classes à droite modulo H) et la partition $G = H \cup Hg_1 \cup \cdots \cup Hg_{r-1}$, donc $\varphi(g)$ est la permutation :

$$\sigma = \begin{pmatrix} 1 & g & \cdots & g^{m-1} & g_1 & gg_1 & \cdots & g^{m-1}g_1 & \cdots & g_{r-1} & \cdots & g^{m-1}g_{r-1} \\ g & g^2 & \cdots & 1 & gg_1 & g^2g_1 & \cdots & g_1 & \cdots & gg_{r-1} & \cdots & g_{r-1} \end{pmatrix}$$
$$= \left(1, g, \cdots, g^{m-1}\right)\left(g_1, gg_1, \cdots, g^{m-1}g_1\right)\cdots\left(g_{r-1}, gg_{r-1}, \cdots, g^{m-1}g_{r-1}\right)$$

   produit de r cycles de longueur m.
2. *Il en résulte que pour $g \in G \setminus \{1\}$ d'ordre $m \geq 2$, la signature de $\varphi(g)$ est :*

$$\varepsilon(\varphi(g)) = (-1)^{r(m-1)} = (-1)^{[G,\langle g\rangle](\theta(g)-1)}$$

   ce résultat étant encore valable pour $g = 1$.
   Si $n = \mathrm{card}(G)$ est impair, alors $\theta(g)$ est impair pour tout $g \in G$ (puisqu'il divise n) et $\varepsilon(\varphi(g)) = 1$. Donc $\varphi(G)$ est un sous-groupe du groupe alterné $\mathcal{A}(G)$.

2.8.3 Matrices de permutations

On désigne par $\mathbb{K}$ un corps commutatif.

À toute permutation $\sigma \in \mathcal{S}_n$, on associe la matrice de passage P_σ de la base canonique $\mathcal{B} = (e_j)_{1\leq j\leq n}$ de $\mathbb{K}^n$ à la base $\mathcal{B}_\sigma = \left(e_{\sigma(j)}\right)_{1\leq j\leq n}$. On dit que P_σ est la matrice de permutation associée à σ.

On peut remarquer que $P_\sigma e_j = e_{\sigma(j)}$ pour tout j compris entre 1 et n et en conséquence, pour tout vecteur $x = (x_i)_{1\leq i\leq n}$, on a :

$$P_\sigma x = \left(x_{\sigma^{-1}(i)}\right)_{1\leq i\leq n}$$

En effet, en écrivant que $x = \sum_{j=1}^{n} x_j e_j$, on a :

$$P_\sigma x = \sum_{j=1}^{n} x_j P_\sigma e_j = \sum_{j=1}^{n} x_j e_{\sigma(j)}$$

et le changement d'indice $k = \sigma(j)$ (σ est bijective), donne :

$$P_\sigma x = \sum_{k=1}^{n} x_{\sigma^{-1}(k)} e_k$$

Théorème 2.14 *L'application $P : \sigma \mapsto P_\sigma$ est un morphisme de groupes injectif de $\mathcal{S}_n$ dans $GL_n(\mathbb{K})$ et pour toute permutation $\sigma \in \mathcal{S}_n$, on a :*

$$\det(P_\sigma) = \varepsilon(\sigma)$$

Démonstration. On a bien $P_\sigma \in GL_n(\mathbb{K})$ pour toute permutation $\sigma \in \mathcal{S}_n$.

Pour σ, σ' dans $GL_n(\mathbb{K})$ et j compris entre 1 et n, on a :

$$P_\sigma(P_{\sigma'} e_j) = P_\sigma e_{\sigma'(j)} = e_{\sigma(\sigma'(j))} = e_{\sigma\sigma'(j)} = P_{\sigma\sigma'} e_j$$

donc $P_\sigma P_{\sigma'} = P_{\sigma\sigma'}$ et P est un morphisme de groupes.

Si $\sigma \in \ker(P)$, on a $P_\sigma = I_n$ et $e_j = e_{\sigma(j)}$ pour tout j, ce qui revient à dire que $j = \sigma(j)$ pour tout j et donc que $\sigma = Id$. Le morphisme P est donc injectif.

Si τ est une transposition, la matrice P_τ est déduite de I_n en permutant deux colonnes et utilisant les propriétés du déterminant (qui peut se définir avec les opérations élémentaires et sans référence au groupe symétrique), on en déduit que $\det(P_\tau) = -\det(I_n) = -1$ (sous-entendu $-1_\mathbb{K}$). En écrivant $\sigma \in \mathcal{S}_n$ comme produit de p transpositions et en utilisant le fait que P est un morphisme de groupes, on en déduit que $\det(P_\sigma) = (-1)^p = \varepsilon(\sigma)$ (sous-entendu $\varepsilon(\sigma)\, 1_\mathbb{K}$). ■

Remarque 2.17 *Prenant $\mathbb{K} = \mathbb{R}$, le résultat précédent nous donne une définition équivalent de la signature, dans la mesure où on a défini le déterminant d'une matrice carrée sans référence au groupe symétrique.*

Corollaire 2.3 *Tout groupe fini d'ordre $n \geq 1$ est isomorphe à un sous-groupe de $GL_n(\mathbb{Z}_p)$ où $\mathbb{Z}_p = \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ et $p \geq 2$ est un nombre premier.*

Démonstration. Le théorème de Cayley nous dit que G est isomorphe à un sous-groupe de $\mathcal{S}_n$ (qui est isomorphe à $\mathcal{S}(G)$ pour G d'ordre n) et le théorème précédent que $\mathcal{S}_n$ est isomorphe à un sous-groupe de $GL_n(\mathbb{Z}_p)$. Il en résulte que G est isomorphe à un sous-groupe de $GL_n(\mathbb{Z}_p)$.
■

2.8.4 Isométries laissant une partie invariante

On désigne par E un espace affine euclidien de dimension $n \geq 2$.

Pour A, B dans E, on note $d(A,B) = \left\|\overrightarrow{AB}\right\|$ la distance de A à B.

On rappelle qu'une isométrie affine est une application affine $\varphi : E \to E$ telle que $d(\varphi(A), \varphi(B)) = d(A,B)$ pour tout couple (A,B) de points de E.

Une application affine $\varphi : E \to E$ est une isométrie affine si, et seulement si, son application linéaire associée $\overrightarrow{\varphi} : \overrightarrow{AB} \mapsto \overrightarrow{\varphi(A)\varphi(B)}$ est une isométrie vectorielle.

On note $Is(E)$ le groupe des isométries de E, $Is^+(E)$ le sous-groupe des déplacements de E (i. e. des isométries telles que $\det(\overrightarrow{\varphi}) = 1$) et $Is^-(E)$ l'ensemble des antidéplacements de E (i. e. des isométries telles que $\det(\overrightarrow{\varphi}) = -1$).

Pour toute partie non vide $\mathcal{P}$ de E, on note $Is(\mathcal{P})$ [resp. $Is^+(\mathcal{P})$, $Is^-(\mathcal{P})$] l'ensemble des isométries [resp. des déplacements, antidéplacements] φ de E qui conservent $\mathcal{P}$, c'est-à-dire telles [resp. tels] que $\varphi(\mathcal{P}) = \mathcal{P}$.

Si $\varphi \in Is(\mathcal{P})$, alors sa restriction à $\mathcal{P}$ est une permutation de $\mathcal{P}$.

Théorème 2.15 *Si $\mathcal{P}$ est une partie non vide de E, alors :*

1. *$Is(\mathcal{P})$ est un sous-groupe de $Is(E)$ et $Is^+(\mathcal{P})$ est un sous-groupe distingué de $Is(\mathcal{P})$;*
2. *l'application qui associe à $\varphi \in Is(\mathcal{P})$ sa restriction à $\mathcal{P}$ est un morphisme de groupes de $Is(\mathcal{P})$ dans $\mathcal{S}(\mathcal{P})$; dans le cas où $\mathcal{P}$ est un repère affine de E, cette application est injective et $Is(\mathcal{P})$ est isomorphe à un sous-groupe de $\mathcal{S}_{n+1}$;*
3. *si $Is^-(\mathcal{P}) \neq \emptyset$, alors pour toute isométrie $\sigma \in Is^-(\mathcal{P})$, l'application $\rho \mapsto \sigma \circ \rho$ réalise une bijection de $Is^+(\mathcal{P})$ sur $Is^-(\mathcal{P})$; dans le cas où $\mathcal{P}$ est fini, on a $\operatorname{card}(Is(\mathcal{P})) = 2\operatorname{card}(Is^+(\mathcal{P}))$;*
4. *si $\mathcal{P}$ est fini, alors toute isométrie $\varphi \in Is(\mathcal{P})$ laisse fixe l'isobarycentre de $\mathcal{P}$.*

Démonstration.

1. On a $Id \in Is(\mathcal{P})$ et pour φ, ψ dans $Is(\mathcal{P})$, la composée $\varphi \circ \psi^{-1}$ est aussi dans $Is(\mathcal{P})$, donc $Is(\mathcal{P})$ est un sous-groupe de $Is(E)$ et $Is^+(\mathcal{P}) = Is(\mathcal{P}) \cap Is^+(E)$ un sous-groupe de $Is^+(E)$. Le groupe $Is^+(\mathcal{P})$ est distingué dans $Is(\mathcal{P})$ comme noyau du morphisme de groupes $\det : \varphi \in Is(\mathcal{P}) \to \det(\overrightarrow{\varphi}) \in \{-1, 1\}$ (on peut aussi dire que pour $\rho \in Is^+(\mathcal{P})$ et $\varphi \in Is(\mathcal{P})$, $\varphi^{-1} \circ \rho \circ \varphi \in Is^+(\mathcal{P})$).

■

Exercice 2.30 *On se fixe un entier $n \geq 2$.*
On dit qu'un groupe G est diédral de type $\mathcal{D}_{2n}$, s'il est dicyclique engendré par un élément ρ d'ordre n et un élément $\sigma \neq \rho$ d'ordre 2 tels que $\rho\sigma\rho\sigma = 1$.

1. *On se place dans le plan complexe muni de sa structure euclidienne canonique et on définit les applications ρ et σ par :*

$$\forall z \in \mathbb{C},\ \rho(z) = e^{\frac{2i\pi}{n}} z,\ \sigma(z) = \overline{z}$$

(ρ est la rotation d'angle $\dfrac{2\pi}{n}$ et σ est la réflexion d'axe O_x).

   (a) *Montrer que le sous-groupe $G = \langle \rho, \sigma \rangle$ de $\mathcal{S}(\mathbb{C})$ est diédral de type $\mathcal{D}_{2n}$.*

   (b) *On vérifiera que G est le groupe des isométries du plan complexe qui conservent l'ensemble $\Gamma_n = \left\{ e^{\frac{2ik\pi}{n}} \mid 0 \leq k \leq n-1 \right\}$ des sommets d'un polygone régulier à n cotés.*

2. *Soit $G = \langle \rho, \sigma \rangle$ un groupe diédral de type $\mathcal{D}_{2n}$.*
   (a) *Montrer que :*
   $$G = \left\{ Id, \rho, \cdots, \rho^{n-1} \right\} \cup \left\{ \sigma, \sigma\rho, \cdots, \sigma\rho^{n-1} \right\}$$
   et que G est d'ordre $2n$.
   (b) *Montrer que deux groupes diédraux de type $\mathcal{D}_{2n}$ sont isomorphe.*
3. *Montrer que $\mathcal{S}_3$ est diédral de type $\mathcal{D}_6$ (le groupe du triangle équilatéral).*

Solution 2.30 *On rappelle que le groupe $G = \langle \rho, \sigma \rangle$ engendré par deux éléments ρ et σ est :*
$$\Gamma = \left\{ g_1 \cdots g_p \mid g_i \in \left\{ \rho, \rho^{-1}, \sigma, \sigma^{-1} \right\} \right\}$$

1. *On remarque que, pour tout entier relatif m, on a $\rho^m(z) = e^{\frac{2im\pi}{n}} z$ pour tout $z \in \mathbb{C}$.*
   (a) *On a $\sigma \neq Id$, $\sigma^2 = Id$, donc σ est d'ordre 2 et $\rho^m = Id$ si, et seulement si, $e^{\frac{2im\pi}{n}} = 1$, ce qui équivaut à $m \equiv 0 \bmod (n)$, donc ρ est d'ordre n.*
   Pour tout $z \in \mathbb{C}$, on a :
   $$\rho\sigma\rho\sigma(z) = e^{\frac{2i\pi}{n}} \overline{e^{\frac{2i\pi}{n}} \overline{z}} = z$$
   donc $\rho\sigma\rho\sigma = Id$ ($\rho\sigma$ est la réflexion d'axe $\mathbb{R}e^{\frac{i\pi}{n}}$)
   Le groupe $G = \langle \rho, \sigma \rangle$ est donc bien diédral de type $\mathcal{D}_{2n}$.
   On peut aussi considérer le sous-groupe de $GL_2(\mathbb{R})$ engendré par :
   $$R = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix} \text{ et } S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
   (c'est le même).
   (b) *Soit $Is(\Gamma_n)$ le groupe des isométries qui conservent Γ_n.*
   Pour tout entier k compris entre 0 et $n-1$, on a :
   $$\sigma\left(e^{\frac{2ik\pi}{n}}\right) = e^{-\frac{2ik\pi}{n}} = e^{\frac{2i(n-k)\pi}{n}} \in \Gamma_n$$
   et :
   $$\rho\left(e^{\frac{2ik\pi}{n}}\right) = e^{\frac{2i(k+1)\pi}{n}} \in \Gamma_n$$
   donc ρ et σ sont dans $Is(\Gamma_n)$ et $G = \langle \rho, \sigma \rangle \subset Is(\Gamma_n)$.
   Réciproquement si $\varphi \in Is(\Gamma_n)$, c'est soit une rotation, soit une réflexion. Si $\varphi : z \mapsto e^{i\alpha} z$ est une rotation avec $0 \leq \alpha < 2\pi$, comme $\varphi(1) \in \Gamma_n$, il existe un entier k compris entre 0 et $n-1$ tel que $\varphi(1) = e^{i\alpha} = e^{\frac{2ik\pi}{n}}$ et $\alpha = \dfrac{2k\pi}{n}$, donc $\varphi = \rho^k \in G$.
   Si c'est une réflexion, alors $\sigma \circ \varphi$ est une rotation dans $Is(\Gamma_n)$, donc $\sigma \circ \varphi \in G$ et $\varphi = \sigma \circ (\sigma \circ \varphi) \in G$.
   On a donc $Is(\Gamma_n) \subset G$ et $G = Is(\Gamma_n)$.

2.
   (a) *Comme ρ est d'ordre n et σ d'ordre 2, on a $\rho^{-1} = \rho^{n-1}$ (puisque $\rho^n = Id$) et $\sigma^{-1} = \sigma$, donc :*
   $$\begin{aligned} G = \langle \rho, \sigma \rangle &= \left\{ g_1 \cdots g_p \mid g_i \in \left\{ \rho, \rho^{-1}, \sigma, \sigma^{-1} \right\} \right\} \\ &= \left\{ g_1 \cdots g_p \mid g_i \in \left\{ \rho, \rho^{n-1}, \sigma \right\} \right\} \\ &= \left\{ \sigma^{k_1} \rho^{j_1} \cdots \sigma^{k_p} \rho^{j_p} \mid p \geq 1,\ k_i \geq 0,\ j_i \geq 0 \right\} \\ &= \left\{ \sigma^{k_1} \rho^{j_1} \cdots \sigma^{k_p} \rho^{j_p} \mid p \geq 1,\ 0 \leq k_i \leq 1,\ 0 \leq j_i \leq n-1 \right\} \end{aligned}$$

Notons $G' = \{Id, \rho, \cdots, \rho^{n-1}\} \cup \{\sigma, \sigma\rho, \cdots, \sigma\rho^{n-1}\}$.
Il est clair que $\sigma^k\rho^j \in G'$ *pour tout* $k \in \{0,1\}$ *et* $j \in \{0, \cdots, n-1\}$ *(pour* $k = 0$, *on a* ρ^j *et pour* $k = 1$, *on a* $\sigma\rho^j$*).*
Montrons que le produit de deux tels éléments est encore dans G'.
Soient donc $g = \sigma^k\rho^j$ *et* $g' = \sigma^{k'}\rho^{j'}$ *dans* G.
Si $(k,k') = (0,0)$ *ou* $(k,k') = (1,0)$, *on a alors* $gg' = \rho^{j+j'} = \rho^r$ *ou* $gg' = \sigma\rho^{j+j'} = \sigma\rho^r$ *avec* $0 \leq r \leq n-1$ *(*r *est le reste dans la division euclidienne de* $j + j'$ *par* n*).*
Si $(k,k') = (0,1)$, *on a alors* $gg' = \rho^j\sigma\rho^{j'}$. *Pour* $j = 0$, *c'est terminé. Pour* $j \geq 1$, *on utilise l'égalité* $\rho\sigma\rho\sigma = 1$ *qui se traduit par* $\rho\sigma = (\rho\sigma)^{-1} = \sigma^{-1}\rho^{-1} = \sigma\rho^{-1}$, *pour écrire que :*

$$gg' = \rho^{j-1}\rho\sigma\rho^{j'} = \rho^{j-1}\sigma\rho^{j'-1}$$

et au bout d'un nombre fini d'étapes, on arrive à $gg' = \sigma\rho^{j'-p} = \sigma\rho^r$ *avec* $0 \leq r \leq n-1$ *(*r *est le reste dans la division euclidienne de* $j' - p$ *par* n*).*
Si $(k,k') = (1,1)$, *on a alors* $gg' = \sigma\rho^j\sigma\rho^{j'}$. *Pour* $j = 0$, *on a* $gg' = \sigma^2\rho^{j'} = \rho^{j'}$ *et c'est terminé. Pour* $j \geq 1$, *on a :*

$$gg' = \sigma\rho^{j-1}\rho\sigma\rho^{j'} = \sigma\rho^{j-1}\sigma\rho^{j'-1}$$

et au bout d'un nombre fini d'étapes, on arrive à $gg' = \rho^{j'-p} = \rho^r$ *avec* $0 \leq r \leq n-1$.
On en déduit alors par récurrence sur $p \geq 1$ *que tout élément de la forme* $\sigma^{k_1}\rho^{j_1}\cdots\sigma^{k_p}\rho^{j_p}$ *avec* $0 \leq k_i \leq 1$, $0 \leq j_i \leq n-1$ *est dans* G'. *Pour* $p = 1$, *c'est clair et supposant le résultat acquis pour* $p \geq 1$, *on a :*

$$\sigma^{k_1}\rho^{j_1}\cdots\sigma^{k_{p+1}}\rho^{j_{p+1}} = \sigma^k\rho^j\sigma^{k_{p+1}}\rho^{j_{p+1}} = \sigma^{k'}\rho^{j'} \in G'.$$

On a donc $G \subset G'$ *et* $G = G'$. *Il en résulte que* G *est d'ordre* $2n$.

(b) *Soient* $G = \langle\rho,\sigma\rangle$ *et* $G' = \langle\rho',\sigma'\rangle$ *deux groupes diédraux d'ordre* $2n$. *L'application* $\varphi : G \to G'$ *définie par* $\varphi(\rho^j) = (\rho')^j$ *et* $\varphi(\sigma\rho^j) = \sigma(\rho')^j$ *pour* $0 \leq j \leq n-1$ *réalise un isomorphisme de* G *sur* G'.

3. *On vu que* $\mathcal{S}_3$ *est isomorphe au groupe du triangle équilatéral (exercice 2.6), donc à* $\mathcal{D}_6$. *On peut aussi utiliser le fait que* $\mathcal{S}_3$ *est dicyclique engendré par* $\sigma = (1,2)$ *d'ordre* 2 *et* $\rho = (1,2,3)$ *d'ordre* 3 *avec* $\rho\sigma = (1,3)$ *d'ordre* 2 *(exercice 2.8).*

Remarque 2.18 *Un groupe d'ordre* $2p$ *avec* p *premier est soit diédral, soit cyclique (voir Boyer, sol-chap4.pdf et exos-ch4.pdf).*

Exercice 2.31 *On se place dans un espace affine euclidien* $\mathcal{E}$ *de dimension* 3 *et on s'intéresse au groupe des isométries de* $\mathcal{E}$ *qui laissent globalement invariant les sommets d'un tétraèdre régulier* $\mathcal{T} = A_1A_2A_3A_4$. *On note* $Is(\mathcal{T})$ *ce groupe.*

1. *Montrer que* $Is(\mathcal{T})$ *est isomorphe à un sous-groupe de* $\mathcal{S}_4$.
2. *Montrer que* $Is(\mathcal{T})$ *est isomorphe à* $\mathcal{S}_4$ *et que le groupe* $Is^+(\mathcal{T})$ *des déplacements qui laissent globalement invariant les sommets de* $\mathcal{T}$ *est isomorphe à* $\mathcal{A}_4$.

Solution 2.31

1. *À toute isométrie* $\varphi \in Is(\mathcal{T})$, *on associe la permutation :*

$$\sigma = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ \varphi(A_1) & \varphi(A_2) & \varphi(A_3) & \varphi(A_4) \end{pmatrix}$$

de $E = \{A_1, A_2, A_3, A_4\}$ *et l'application* $\Phi : \varphi \mapsto \sigma$ *est un morphisme de groupes. Ce morphisme est injectif du fait que* (A_1, A_2, A_3, A_4) *est un repère affine de* $\mathcal{E}$ *et qu'une application affine est uniquement déterminée par ses valeurs sur un repère affine. Donc* $Is(\mathcal{T})$ *est isomorphe à un sous-groupe de* $\mathcal{S}_4$ *et son ordre divise* 24.

2. *Comme* $\mathcal{S}(E)$ *est engendré par les transpositions* (A_1, A_k) *avec* $k = 2, 3, 4$, *il suffit de montrer que* $\Phi(Is(\mathcal{T}))$ *contient ces transpositions. La transposition* (A_1, A_k) *est l'image de la réflexion par rapport au plan médiateur du segment* $[A_1, A_k]$ *(ce plan médiateur contient les deux autres sommet de* $\mathcal{T}$ *puisque ses faces sont des triangles équilatéraux). Donc* $\Phi(Is(\mathcal{T})) = \mathcal{S}(E)$.
Comme $Is^+(\mathcal{T})$ *est d'indice* 2 *dans* $Is(\mathcal{T})$, $\Phi(Is^+(\mathcal{T}))$ *est d'indice* 2 *dans* $\Phi(Is(\mathcal{T}))$ *et donc égal à* $\mathcal{A}(E)$.

Exercice 2.32 *On se place ici dans un espace affine euclidien* $\mathcal{E}$ *de dimension* 3 *et on s'intéresse au groupe* $Is(\mathcal{C})$ *des isométries affines de* $\mathcal{E}$ *qui laissent globalement invariant les sommets d'un cube* $\mathcal{C}$.

1. *Montrer que tout élément de* $Is(\mathcal{C})$ *induit une permutation de l'ensemble* $\mathcal{D} = \{[A_1, A_7], [A_2, A_8], [A_3, A$ *des grandes diagonales du cube et en déduire un morphisme de groupes* Φ *de* $Is(\mathcal{C})$ *dans* $\mathcal{S}(\mathcal{D})$.
2. *Déterminer le noyau de* Φ.
3. *Montrer que* Φ *est surjective.*
4. *En déduire que* $\operatorname{card}(Is(\mathcal{C})) = 48$ *et* $\operatorname{card}(Is^+(\mathcal{C})) = 24$.
5. *Montrer que* $Is^+(\mathcal{C})$ *est isomorphe à* $\mathcal{S}_4$.

Solution 2.32

1. *Par conservation des barycentres et des distances par une isométrie, une diagonale est transformée en diagonale de même longueur, donc* $\mathcal{D}$ *est globalement invariant par tout élément de* $Is(\mathcal{C})$ *et l'application* Φ *qui associe à* $\varphi \in Is(\mathcal{C})$ *la permutation correspondante des grandes diagonales réalise un morphisme de groupes de* $Is(\mathcal{C})$ *dans* $\mathcal{S}(\mathcal{D})$.
2. *Si* $\varphi \in \ker(\Phi)$, *elle conserve alors chaque diagonale. On a donc* $\varphi(A_1) = A_1$ *ou* $\varphi(A_1) = A_7$ *et même chose pour les autres grandes diagonales.*
Si $\varphi(A_1) = A_1$, *on a alors* $\varphi([A_1, A_2]) = [A_1, A_k]$ *avec* $k = 2, 4$ *ou* 5 *puisque les arêtes sont conservées et* $\varphi(A_2) = A_2$ *puisque la diagonale* $[A_2, A_8]$ *est conservée. De même, on a* $\varphi(A_4) = A_4$. *Comme* φ *conserve aussi le barycentre* O *des* A_k, *on a* $\varphi = Id$ *puisqu'elle laisse fixe le repère affine* (O, A_1, A_2, A_4).
Si $\varphi(A_1) = A_7$, *on a alors* $\varphi([A_1, A_2]) = [A_7, A_k]$ *avec* $k = 3, 6$ *ou* 8 *puisque les arêtes sont conservées et* $\varphi(A_2) = A_8$ *puisque la diagonale* $[A_2, A_8]$ *est conservée. De même, on a* $\varphi(A_4) = A_6$. *Donc* φ *est la symétrie* σ_O *de centre* O, *puisque ces deux applications affines coïncident sur le repère affine* (O, A_1, A_2, A_4).
En définitive, $\ker(\Phi) = \{Id, \sigma_O\}$.
3. *Notons* $D_1 = [A_1, A_7], \cdots, D_4 = [A_4, A_6]$ *les grandes diagonales. Comme* $\mathcal{S}(\mathcal{D})$ *est engendré par les transpositions* (D_1, D_k) *avec* $k = 2, 3, 4$, *il suffit de vérifier que ces transpositions sont dans* $\operatorname{Im}(\Phi)$. *Pour* $D_1 = [A_1, A_7]$ *et* $D_2 = [A_2, A_8]$, *la réflexion par rapport au plan* $(A_3A_4A_5)$ *qui contient les deux autres diagonales permute* D_1 *et* D_2. *De même pour les autres.*
4. *On a alors :*

$$\begin{aligned}\operatorname{card}(Is(\mathcal{C})) &= \operatorname{card}(\ker(\Phi))\operatorname{card}(\operatorname{Im}(\Phi)) = 2\operatorname{card}(\mathcal{S}(\mathcal{D}))\\ &= 2\operatorname{card}(\mathcal{S}_4) = 48.\end{aligned}$$

Comme $Is(\mathcal{C})$ *contient un l'anti-déplacement* σ_O, *on a* $\operatorname{card}(Is(\mathcal{C})) = 2\operatorname{card}(Is^+(\mathcal{C}))$ *et* $\operatorname{card}(Is^+(\mathcal{C})) = 24$.

5. *Le noyau de la restriction de* Φ *à* $Is^+(\mathcal{C})$ *est* $\{Id\}$, *donc* Φ *est injective et avec* $\operatorname{card}(Is^+(\mathcal{C})) = 24 = \operatorname{card}(\mathcal{S}_4)$, *on déduit que* Φ *est un isomorphisme de* $Is^+(\mathcal{C})$ *sur* $\mathcal{S}_4$.

2.8.5 Polynômes symétriques

$\mathbb{K}$ est un corps commutatif de caractéristique différente de 2.

Définition 2.8 *On dit qu'un polynôme* $P \in \mathbb{K}[X_1, \cdots, X_n]$ *est symétrique si* $P\left(X_{\sigma(1)}, \cdots, X_{\sigma(n)}\right) = P(X_1, \cdots, X_n)$ *pour toute permutation* $\sigma \in \mathcal{S}_n$.

Les polynômes $\Sigma_k = \sum_{i_1 < \cdots < i_k} X_{i_1} \cdots X_{ik}$ sont les polynômes symétriques élémentaires.

Théorème 2.16 *Si* $P \in \mathbb{K}[X_1, \cdots, X_n]$ *est symétrique, il existe alors un unique polynôme* $Q \in \mathbb{K}[X_1, \cdots, X_n]$ *tel que* $P(X_1, \cdots, X_n) = Q(\Sigma_1, \cdots, \Sigma_n)$.

Théorème 2.17 *Soient* H, F *deux* $\mathbb{K}$*-espaces vectoriels. Une application* n*-linéaire* $\varphi : E^n \to F$ *est alternée si, et seulement si,* $\varphi\left(x_{\sigma(1)}, \cdots, x_{\sigma(n)}\right) = \varepsilon(\sigma)\varphi(x_1, \cdots, x_n)$ *pour tout* $(x_1, \cdots, x_n) \in E^n$ *et toute permutation* $\sigma \in \mathcal{S}_n$.

Théorème 2.18 *Soit* $\mathbb{K}$ *un corps commutatif de caractéristique différente de* 2. *L'application* $\det : \mathcal{M}_n(\mathbb{K}) \to \mathbb{K}$ *définie par :*

$$\det(A) = \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$$

est une forme linéaire alternée.