2. Groupes symétrique et alterné

On rappelle que pour $n \geq 1$, S_n désigne le groupe des bijections, aussi appellées *permutations*, de l'ensemble $\{1, \ldots, n\}$. C'est un groupe d'ordre $n!$. Un élément σ de S_n est parfois noté sous la forme de la matrice $2 \times n$

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

On note $\mathrm{Fix}\,\sigma$ l'ensemble des $i \in \{1, \ldots, n\}$ tels que $\sigma(i) = i$ (*points fixes* de σ), et $\mathrm{Supp}\,\sigma$ le complémentaire de $\mathrm{Fix}\,\sigma$ dans $\{1, \ldots, n\}$ (*support* de σ). Deux permutations à supports disjoints commutent (mais la réciproque est fausse !) : si σ est de support S et τ de support T avec $S \cap T = \emptyset$, alors $\sigma\tau$ et $\tau\sigma$ coincident avec σ sur S, avec τ sur T, et valent l'identité sur $\{1, \ldots, n\} \smallsetminus (S \cup T)$.

Si $2 \leq k \leq n$ est un entier, on appelle *k-cycle*, ou cycle de longueur k, une permutation σ dont le support est une partie à k éléments de la forme $\{i_1, i_2, \ldots, i_k\}$, avec $\sigma(i_m) = i_{m+1}$ pour $m = 1, \ldots, k-1$ et $\sigma(i_k) = i_1$. On note alors $\sigma = (i_1\, i_2 \cdots i_k)$, et on a aussi $\sigma = (i_2\, i_3 \cdots i_k\, i_1)$, etc... Un k-cycle est d'ordre exactement k : on a $\sigma^n(i_m) = i_{n+m}$, les indices étant pris modulo k. Dans le cas particulier $k = 2$, on parle de *transposition* : une transposition $(i\, j)$, avec $i \neq j$, échange i et j et fixe tous les autres éléments. Les cycles engendrent S_n. Beaucoup plus précisément, on a :

Proposition 2.1. (Décomposition en cycles d'une permutation) *Pour tout élément $\sigma \in \mathrm{S}_n$, il existe une unique famille de cycles $\{c_i\}_{i \in I}$ à supports disjoints et tels que $\sigma = \prod_i c_i$.*

Noter que deux cycles à supports disjoints commutent, donc il n'est pas nécessaire de préciser l'ordre dans le produit ci-dessus. De plus, dans le cas $\sigma = 1$ tous les points de $\{1, \ldots, n\}$ sont fixés donc la famille de cycles associée est vide ! et on utilise la convention usuelle qu'un produit vide vaut 1 dans un groupe.

Exemple 2.2. Par exemple, on a la décomposition en cycles suivante dans S_8

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

Attention, on a $(1\,2\,3) = (1\,2)\,(2\,3)$ dans S_3 mais ce n'est pas *la* décomposition en cycles car les supports de $(1\,2)$ et $(2\,3)$ ne sont pas disjoints.

Pour démontrer la proposition on considère l'action naturelle du sous-groupe $\langle\sigma\rangle \subset \mathrm{S}_n$ sur $\{1, \ldots, n\}$. La relation d'équivalence sur $\{1, \ldots, n\}$ associée à ce sous-groupe n'est rien d'autre que celle étudiée à l'Exemple 1.8 Chap. 1, appliqué à la bijection $f = \sigma$ de $X = \{1, \ldots, n\}$. Ses classes, *i.e.* les orbites de $\langle\sigma\rangle$ pour cette action, sont simplement appelées *orbites* de σ. Les orbites de cardinal 1 sont les points fixes de σ, ils sont ignorés dans la décomposition [2] ci-dessus. Notons $\{C_i\}_{i \in I}$ les autres orbites, dont ont sait qu'elles sont disjointes. Pour tout i, on constate que σ préserve C_i et en permute circulairement les éléments (comme déjà mis en évidence dans l'Exemple 1.8 Chap. 1), ce qui définit le cycle c_i recherché. On a alors bien $\sigma = \prod_i c_i$, car sur C_j ces deux permutations valent toutes deux c_j, et hors des C_j elles valent l'identité. Cette observation montre aussi l'unicité de la décomposition.

2. Nous aurions pu autoriser les cycles de longueur 1, mais comme ils sont tous égaux à l'identité, il faudrait ajouter leur support dans la définition, ce qui est lourd.

Une première application de la décomposition en cycles concerne la détermination (efficace algorithmiquement !) de l'ordre d'une permutation.

PROPOSITION 2.3. *Soit $\sigma \in \mathrm{S}_n$ de décomposition en cycles $\sigma = \prod_i c_i$. Alors l'ordre de σ est le ppcm des longueurs des c_i.*

DÉMONSTRATION — Soit $k \in \mathbb{Z}$. On a $\sigma^k = \prod_i c_i^k$ car les c_i commutent. Comme $\mathrm{Supp}(c_i^k) \subset \mathrm{Supp}(c_i)$ et que les $\mathrm{Supp}\, c_i$ sont disjoints, on constate σ^k coincide avec c_i^k sur $\mathrm{Supp}(c_i)$, et donc $\sigma^k = 1 \Leftrightarrow c_i^k = 1$ pour tout i. On conclut car l'ordre d'un cycle est sa longueur. □

REMARQUE 2.4. *On prendra garde qu'une puissance d'un cycle n'est pas forcément un cycle. Par exemple on a $(1\,2\,3\,4)^2 = (1\,3)\,(2\,4)$. En revanche, si c est un k-cycle et si n est premier à k, alors c^n est encore un k-cycle (Exercice 4.4).*

La Proposition 2.1 montre que S_n est engendré par les cycles. Pour une partie $\{i_1, \ldots, i_k\}$ à k éléments, la relation

$$(i_1\, i_2 \ldots i_k) \;=\; (i_1 i_2)\,(i_2\, i_3 \ldots i_k) \;=\; (i_1 i_2)\,(i_2\, i_3) \cdots (i_{k-1} i_k) \tag{18}$$

(immédiate !) montre aussi que :

PROPOSITION 2.5. *Les transpositions engendrent S_n.*

Le groupe S_n a beaucoup d'autres systèmes de générateurs intéressants. Avant d'en donner deux autres, montrons lemme important suivant, qui évite souvent bien des calculs !

LEMME 2.6. (Conjugué d'un cycle) *Soient $\sigma \in \mathrm{S}_n$ et $c = (i_1, i_2, \ldots, i_k)$ un k-cycle. Alors $\sigma c \sigma^{-1}$ est le k-cycle $(\sigma(i_1)\,\sigma(i_2)\,\ldots\,\sigma(i_k))$.*

DÉMONSTRATION — On a $\sigma c \sigma^{-1}(\sigma(i_m)) = \sigma c(i_m) = \sigma(i_{m+1})$. Soit $C = \{i_1, i_2, \ldots, i_m\}$. Pour $j \notin \sigma(C)$, on a $\sigma^{-1}(j) \notin C$ et donc $c(\sigma^{-1}(j)) = \sigma^{-1}(j)$, puis $\sigma c \sigma^{-1}(j) = j$. □

PROPOSITION 2.7. *(i) Les*[3] *$(i\ i+1)$ avec $1 \leq i < n$ engendrent S_n.*

(ii) La transposition $(1\,2)$ et le n-cycle $(1\,2 \ldots n)$ engendrent S_n.

En particulier, on a $\min(\mathrm{S}_n) = 2$ pour $n > 2$.

DÉMONSTRATION — Soit H le sous-groupe de S_n engendré par les $(i\ i+1)$. Fixons $1 \leq i < j \leq n$. En conjuguant $(1\,2) \in H$ successivement par $(2\,3)$, $(3\,4)$, …, $(j-1\ j)$, on a $(1\,j) \in H$. En conjuguant $(1\,j)$ successivement par $(1\,2)$, $(3,4)$, …, $(i-1\,i)$, on a $(i\,j) \in H$. Ainsi, H contient toutes les transpositions, puis $H = \mathrm{S_n}$. Le (ii) se déduit du (i) et de la relation $c^{i-1}(1\,2)c^{1-i} = (i\ i+1)$, où $c = (1\,2 \ldots n)$, elle-même conséquence du Lemme 2.6 ci-dessus. □

3. Les $s_i = (i\,i+1)$ sont appelés *générateurs de Coxeter* de S_n. Ils vérifient $s_i^2 = 1$, $s_i s_j = s_j s_i$ pour $|i-j| > 1$ et $(s_i s_{i+1})^3 = 1$, ou ce qui revient au même, $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$ (on a en fait $s_i s_{i+1} = (i\ i{+}1\ i{+}2)$). On peut montrer que « toute relation entre les s_i se déduit de ces identités.

Notre but est maintenant de décrire les classes de conjugaison dans S_n.

DÉFINITION 2.8. *(i) Une partition de l'entier n est la donnée d'une suite décroissante $n_1 \geq n_2 \geq \cdots \geq n_r$ d'entiers > 0 tels que $n = n_1 + n_2 + \cdots + n_r$.*

(ii) Le type de $\sigma \in \mathrm{S}_n$ est la partition de l'entier n définie par les cardinaux[4] *des orbites de σ dans $\{1, \ldots, n\}$.*

Les partitions de 4 sont par exemple 4, $3+1$, $2+2$, $2+1+1$ et $1+1+1+1$. La partition $n = n_1 + \cdots + n_r$ est souvent notée symboliquement $1^{l_1} 2^{l_2} \cdots n^{l_n}$ où l_i est le nombre de $1 \leq j \leq r$ tels que $n_j = i$; on omet alors le symbole i^{l_i} quand $l_i = 0$, et on écrit i pour i^1. Par exemple, les partitions de 4 deviennent 4, $1\,3$, 2^2, $1^2\,2$ et 1^4. Ainsi, la permutation $(1\,4)(2\,3)(5\,7\,6)$ de S_8 est de type $1\,2^2\,3$.

PROPOSITION 2.9. *Deux éléments de S_n sont conjugués si, et seulement si, ils ont même type.*

DÉMONSTRATION — Pour $\sigma, \tau, \tau' \in \mathrm{S}_n$ on a $\sigma\tau\tau'\sigma^{-1} = \sigma\tau\sigma^{-1}\sigma\tau'\sigma^{-1}$. Soit $\sigma \in \mathrm{S}_n$ de décomposition en cycles $\sigma = c_1 \cdots c_r$, avec $C_i \subset \{1, \ldots, n\}$ le support de c_i. Pour $\tau \in \mathrm{S}_n$ on a donc $\tau\sigma\tau^{-1} = (\tau c_1 \tau^{-1}) \cdots (\tau c_r \tau^{-1})$. Les $\tau c_i \tau^{-1}$ sont des cycles de support les $\tau(C_i)$ par le Lemme 2.6, encore disjoints : c'est la décomposition en cycles de $\tau\sigma\tau^{-1}$. En particulier, σ et $\tau\sigma\tau^{-1}$ ont même type. Réciproquement, supposons σ et σ' de même type, disons décomposés respectivement en produits de cycles c_i et c'_i pour $i = 1, \ldots, r$, avec c_i et c'_i de même longueur pour tout i. Les supports I_i (resp. I'_i) et des c_i (resp. c'_i) sont disjoints et de même cardinal. Par le Lemme 2.6, on peut trouver $\tau \in \mathrm{S}_n$ avec $\tau(I_i) = I'_i$ et même $\tau c_i \tau^{-1} = c'_i$ pour tout i, puis $\tau\sigma\tau^{-1} = \sigma'$. □

Mettons en évidence une propriété de S_n que l'on vient d'utiliser pour affirmer l'existence de τ dans la dernière phrase de cette démonstration.

DÉFINITION 2.10. *Pour $k \geq 1$ entier, et G agissant sur X avec $|X| \geq k$, on dit que G agit k-transitivement sur X si pour $(x_1, \ldots, x_k)$ et $(y_1, \ldots, y_k)$ deux k-uples d'éléments distincts de X il existe $g \in G$ tel que $gx_i = y_i$ pour tout $i = 1 \ldots k$.*

Par définition 1-transitif équivaut à transitif, et k+1-transitif implique k-transitif.

EXEMPLE 2.11. *(i) $\mathrm{GL}(V)$ agit 2-transitivement sur $\mathbb{P}(V)$ si $\dim V > 1$. Il agit même 3-transitivement si $\dim V = 2$ comme on le verra plus tard !*

(ii) S_n agit n-transitivement sur $\{1, \ldots, n\}$ (c'est ce que l'on a utilisé ci-dessus).

(iii) Pour $n \geq 4$, S_n agit transitivement, mais pas 2-transitivement, sur l'ensemble des parties à 2 éléments de $\{1, \ldots, n\}$.

Un sous-groupe de S_n particulièrement important est le *groupe alterné*. Il est relié à la notion de *signature* d'un permutation σ. Elle est définie par la formule[5]

$$\varepsilon(\sigma) = \prod_{\{i,j\}} \frac{\sigma(j) - \sigma(i)}{j - i},$$

le produit étant pris sur toutes les parties $\{i, j\}$ à deux éléments de $\{1, 2, \ldots, n\}$.

4. Autrement dit, par les longueurs des cycles intervenant dans la décomposition en cycles de σ, et où chaque point fixe est vu comme un cycle de longueur 1.

5. Pour $n = 1$, ce produit "vide" vaut 1 par convention.

PROPOSITION 2.12. *La signature ε est un morphisme de groupes $\mathrm{S}_n \to \{\pm 1\}$. On a $\varepsilon(\tau) = -1$ pour toute transposition τ.*

En particulier, $\varepsilon(\sigma)$ est un signe ± 1 : c'est donc $(-1)^{\mathrm{n}(\sigma)}$ où $\mathrm{n}(\sigma)$ est le nombre de couples $\{i, j\}$ avec $i < j$ et $\sigma(j) < \sigma(i)$ (nombre d'*inversions* de σ).

DÉMONSTRATION — Le groupe S_n agit naturellement sur l'ensemble des parties à 2 éléments de $\{1, \dots, n\}$. On en déduit $\prod_{i<j}(\sigma(j) - \sigma(i)) = \pm \prod_{i<j}(i - j)$, et donc $\varepsilon(\sigma) = \pm 1$, pour $\sigma \in \mathrm{S}_n$. On en déduit aussi, pour tout $\sigma, \tau \in \mathrm{S}_n$, l'égalité

$$\varepsilon(\sigma) = \prod_{\{i,j\}} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} = \varepsilon(\sigma\tau)/\varepsilon(\tau)$$

ce qui prouve la première assertion. Pour la seconde, soit $\tau = (a\, b)$ une transposition. On peut écrire $\tau = \sigma(1\, 2)\sigma^{-1}$ où σ est n'importe quelle permutation envoyant 1 sur a et 2 sur b. On a alors $\varepsilon(\tau) = \varepsilon(\sigma)\varepsilon((1\, 2))\varepsilon(\sigma)^{-1} = \varepsilon((1\, 2))$ (des signes commutent...). On peut donc supposer $a = 1$ et $b = 2$. Mais dans ce cas, on constate que $\mathrm{n}((1\, 2)) = 1$: la seule inversion de $(1\, 2)$ est $\{1, 2\}$. On a donc $\varepsilon((1\, 2)) = (-1)^1 = -1$. □

DÉFINITION 2.13. *Le* groupe alterné A_n *est le sous-groupe des éléments $\sigma \in \mathrm{S}_n$ tels que $\varepsilon(\sigma) = 1$ (permutations* paires*). C'est un sous-groupe distingué, et on a $|\mathrm{A}_n| = n!/2$ pour $n \geq 2$.*

REMARQUE 2.14. (Groupe alterné et jeu de taquin) La notion de permutation paire, bien qu'élémentaire, n'est pas si intuitive que cela ! Elle permet par exemple comprendre pourquoi le challenge à 1000 dollars posé par Sam Loyd au 19ème siècle concernant les positions accessibles du populaire *jeu de Taquin* était impossible : voir ce billet de Michel Coste et l'Exercice 4.9.

Si $c = (i_1\, i_2 \dots i_k)$ est un k-cycle, la formule (18) montre $\varepsilon(c) = (-1)^{k-1}$. Ainsi, un k-cycle est dans A_n si, et seulement si, on a $k \equiv 1 \bmod 2$. Donnons quelques générateurs de A_n.

PROPOSITION 2.15. *(i) Les produits de deux transpositions engendrent A_n.*
(ii) Les 3-cycles engendrent A_n.

DÉMONSTRATION — On a vu que les transpositions engendrent S_n. Écrivons $\sigma \in \mathrm{S}_n$ comme produit $\sigma = \tau_1 \cdots \tau_n$ de transpositions. On alors $\varepsilon(\sigma) = (-1)^n$, donc $\sigma \in \mathrm{A}_n$ si, et seulement si, n est pair : le (i) s'en déduit.

On a $(a\, b)(a\, b) = 1$, $(a\, b)(b\, c) = (a\, b\, c)$ pour a, b, c distincts, et $(a\, c)(b\, d) = (a\, b\, c)(a\, b\, d)$ pour a, b, c, d distincts. Ainsi, tout produit de 2 transpositions est un produit de 3-cycles. Le (i) implique donc le (ii). □

REMARQUE 2.16. Un produit de deux transpositions à supports disjoints est appelé *double transposition*. On parle de même de *triple tanspositions* etc...

Les classes de conjugaison de A_n sont légèrement plus subtiles à classer que celles de S_n (voir l'Exercice 4.12).

PROPOSITION 2.17. *Pour $n \geq 3$, le groupe A_n agit $(n-2)$-transitivement sur $\{1, \ldots, n\}$. En particulier, pour $2 \leq k \leq n-2$, les k-cycles de S_n sont conjugués sous l'action de A_n.*

DÉMONSTRATION — En effet, soient $(x_1, \ldots, x_{n-2})$ et $(y_1, \ldots, y_{n-2})$ deux $(n-2)$-uples d'éléments distincts de $\{1, \ldots, n\}$. On peut trouver $\sigma \in \mathrm{S}_n$ avec $\sigma(x_i) = y_i$ pour tout $1 \leq i \leq n-2$, par n-transitivité de S_n. Le complémentaire des y_i dans $\{1, \ldots, n\}$ est une partie à 2 éléments, disons $\{a, b\}$. On a encore $(a\,b)\sigma(x_i) = y_i$ pour tout $1 \leq i \leq n-2$. On conclut car une (et une seule) des deux permutations σ et $(a\,b)\sigma$ est dans S_n. La dernière assertion découle du Lemme 2.6. □

3. Les cas $n \leq 5$

On a évidemment $\mathrm{A}_1 = \mathrm{S}_1 \simeq 1$ (groupe trivial), et aussi $\mathrm{S}_2 = \{1, (1\,2)\} \simeq \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{A}_2 \simeq 1$. Examinons la structure du groupe S_3. Ses $3! = 6$ éléments sont 1, les trois transpositions $(1\,2)$, $(1\,3)$ et $(2\,3)$, ainsi que les deux 3-cycles $c = (1\,2\,3)$ et $c^2 = (1\,3\,2) = c^{-1}$. On a en particulier

$$\mathrm{A}_3 = \langle c \rangle \simeq \mathbb{Z}/3\mathbb{Z}.$$

Posons $\tau = (1\,3)$. On a $\tau c \tau^{-1} = (3\,2\,1) = c^2$ (Lemme 2.6) et donc $\tau c = c^2 \tau$. Un petit calcul montre en fait $\tau c = c^2 \tau = (1\,2)$ et $c\tau = \tau c^2 = (2\,3)$. En particulier, S_3 n'est pas commutatif[6] et on a

$$\mathrm{S}_3 = \langle \tau, \sigma \rangle.$$

Au final, tout élément de S_3 s'écrit sous la forme (unique) $c^k \tau^q$ avec $0 \leq k < 2$ et $0 \leq q < 1$. D'autre part, le produit de deux tels éléments se déduit simplement des relations $c^3 = 1$, $\tau^2 = 1$ et $\tau c = c^{-1}\tau$, cette dernière entraînant $\tau c^k = c^{-k}\tau$ pour tout $k \in \mathbb{Z}$. On en déduit la *table de multiplication* de S_3 (Table 1).

$\cdot$	1	c	c^2	τ	τc	τc^2
1	1	c	c^2	τ	τc	τc^2
c	c	c^2	1	τc^2	τ	τc
c^2	c^2	1	c	τc	τc^2	τ
τ	τ	τc	τc^2	1	c	c^2
τc	τc	τc^2	τ	c^2	1	c
τc^2	τc^2	τ	τc	c	c^2	1

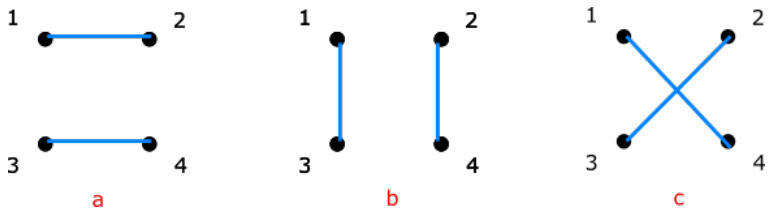
TABLE 1. Table de multiplication de S_3

En fait, une analyse similaire s'applique à tout groupe non abélien d'ordre 6 et permet de montrer que tout groupe non abélien d'ordre 6 est isomorphe à S_3 (voir le complément 9). La structure dégagée ci-dessus de S_3 ne s'étend pas du tout à S_n

6. On en déduit que S_X n'est pas abélien pour $|X| \geq 3$, car alors S_X admet des sous-groupes isomorphes à S_3.

pour $n \geq 4$, mais conduit plutôt à la notion de groupe diédral, que nous verrons plus loin.

Considérons maintenant le cas du groupe S_4, qui a 24 éléments. Il se trouve qu'il existe un morphisme un peu surprenant $\mathrm{S}_4 \to \mathrm{S}_3$, qui permet largement de ramener la structure de S_4 à celle de S_3, et que l'on va décrire maintenant. Observons que l'ensemble $\{1,2,3,4\}$ possède exactement 3 partitions en parties à 2 éléments :



On a donc $a = \{\{1,2\},\{3,4\}\}$, $b = \{\{1,\ 3\},\{2,4\}\}$ et $c = \{\{1,4\},\{2,3\}\}$. Le groupe S_4 agit naturellement sur l'ensemble $\mathscr{P} = \{a,b,c\}$ de ces 3 partitions, ce qui fournit un morphisme de groupes

$$f : \mathrm{S}_4 \to \mathrm{S}_{\mathscr{P}}, \quad \text{avec} \quad \mathrm{S}_{\mathscr{P}} \simeq \mathrm{S}_3.$$

Par exemple, on constate que $f((1\,3)) = f((2\,4))$ est la transposition $(a\,c)$ de $\mathscr{P}$, et on a de même $f((2\,3\,4)) = (a\,b\,c)$.

PROPOSITION 3.1. *Le morphisme f ci-dessus est surjectif, de noyau*

$$\mathrm{K}_4 := \{1,\ (1\,3)(2\,4), (1\,2)(3\,4),\ (1\,4)(2\,3)\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Noter que $(1\,2)(3\,4)$ et $(1\,3)(2\,4)$ commutent, même s'ils ne sont pas à support disjoint.

DÉMONSTRATION — Comme $(a\,c) = f((1\,3))$ et $(a\,b\,c) = f((2\,3\,4))$ engendrent $\mathrm{S}_{\mathscr{P}}$ par l'étude de S_3, on a montré que f est surjectif. Son noyau a donc 4 éléments, et les éléments de $\{1,\ (1\,3)(2\,4), (1\,2)(3\,4),\ (1\,4)(2\,3)\}$ conviennent manifestement. C'est un groupe d'ordre 4 dont tous les éléments sont de carré 1 (donc commutatif !), il est donc isomorphe au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

On a clairement $\mathrm{K}_4 \subset \mathrm{A}_4$ et f induit de même morphisme surjectif $\mathrm{A}_4 \to \mathrm{A}_{\mathscr{P}} \simeq \mathrm{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$ (un 3-cycle est envoyé sur un 3 cycle) de noyau K_4. Nous verrons au §5 que ces dévissages non triviaux de S_n et A_n pour $n \leq 4$ cessent pour $n \geq 5$. En revanche, un phénomène remarquable supplémentaire se produit pour $n = 5$.

THÉORÈME 3.2. *Il existe une action transitive de S_5 sur un ensemble à 6 éléments.*

Nous verrons plus tard que cette action est unique à isomorphisme près, et aussi qu'elle est fidèle et 3-transitive ! (Voir l'Exercice 4.19) Nous allons en donner deux descriptions ci-dessous.

La première, d'apparence assez magique mais particulièrement esthétique, est issue d'un article de Howard-Millson-Snowden-Vakil [7]. On considère le graphe complet $\mathscr{G}$ (non orienté) de sommets $\{1,2,3,4,5\}$. Ce graphe a exactement 10 arêtes. On se

7. *A description of the outer automorphism of* S_6 *and the invariants of* 6 *points in the projective space.*

convainc aisément qu'il existe exactement 6 manières de partitionner ces 10 arêtes en réunion disjointe de deux circuits hamiltoniens [8] de $\mathscr{G}$: ce sont les 6 "*pentagones mystiques*", représentés ci-dessous :

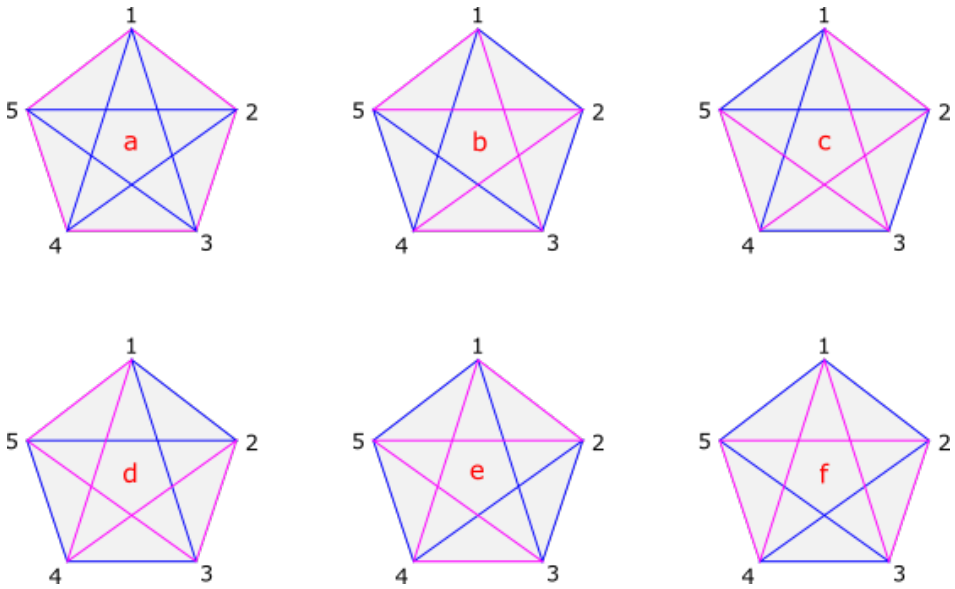


FIGURE 1. Les 6 « pentagones mystiques »

Hormis dans le cas du pentagone a, on constate que chaque pentagone est formé d'un *poisson* et d'une *chauve-souris* ! Notons $X = \{a, b, c, d, e, f\}$ l'ensemble de ces 6 partitions de $\mathscr{G}$. L'action évidente de S_5 agit sur $\{1, \ldots, 5\}$ induit naturellement une action de S_5 sur X, et fournit donc un morphisme de groupes

$$\phi : \mathrm{S}_5 \to \mathrm{S}_X \simeq \mathrm{S}_6.$$

Il est aisé d'étudier l'action de chaque élément de S_5 sur X. Un exemple particulièrement simple est celui de la permutation $(1\,2\,3\,4\,5)$ de S_5, qui fixe manifestement le pentagone a et permute cycliquement les 5 autres, via $(b\,c\,d\,e\,f)$. On a donc $\phi((1\,2\,3\,4\,5)) = (b\,c\,d\,e\,f)$. Autre exemple : on a $\phi((1\,2)) = (a\,d)(b\,c)(e\,f)$. En effet, $(1\,2)$ envoie le « contour » $(1\,2\,3\,4\,5)$ du a sur $(2\,1\,3\,4\,5)$ (poisson du d), le poisson $(1\,2\,3\,5\,4)$ du b sur $(2\,1\,3\,5\,4)$ (chauve-souris du c), et la chauve-souris $(1\,2\,5\,4\,3)$ du e sur $(2\,1\,5\,3\,4)$ (poisson du f). Cela démontre que l'action de S_5 sur X est transitive, comme annoncé. De même, on verrait que le 3-cycle $(1\,2\,3)$ agit comme $(a\,f\,c)(b\,e\,d)$ et le 4-cycle $(1\,2\,3\,4)$ comme $(a\,c\,e\,b)$.

Donnons maintenant une seconde description, à la fois plus classique et plus naturelle, de l'action ci-dessus. Notons Y l'ensemble des sous-groupes d'ordre 5 de S_5. On a $|Y| = 6$. En effet, un sous-groupe d'ordre 5 est engendré par un 5-cycle, et contient en fait un unique 5-cycle envoyant 1 sur 2, *i.e.* de la forme $(1\,2\,a\,b\,c)$ avec $\{a, b, c\} = \{3, 4, 5\}$. Le groupe S_5 agit par conjugaison sur Y, via $(\sigma, H) \mapsto \sigma H \sigma^{-1}$. Cette action est transitive car deux 5-cycles quelconques sont conjugués dans S_5 : elle répond bien au théorème. Mieux, cette description rend évident le fait que le sous-groupe de S_5 isomorphe à S_3 fixant 1 et 2 agit 3-transitivement sur Y !

Vérifions enfin que les actions ci-dessus de S_5 sur X et Y sont isomorphes. En effet, tout sous-groupe $H = \langle c \rangle$ d'ordre 5 de S_5 définit un unique pentagone $\mathrm{p}(H)$

8. *i.e.* de circuit de longueur 5 passant une et une seule fois par chaque sommet.