

Autour du groupe symétrique

Travaux dirigés du 7 et du 10 octobre 2025

✂ Préambule. Actions k -transitives

Soient G un groupe agissant sur un ensemble X , $k \geq 1$ un entier, et $x \in X$.

1. Montrer que G agit $(k+1)$ -transitivement sur X si, et seulement si, G agit transitivement sur X et G_x agit k -transitivement sur $X - \{x\}$.

Posons $Y = X - \{x\}$. Alors G_x agit naturellement sur Y . On a clairement $|X| \geq k+1 \iff |Y| \geq k$. Supposons que G agit $(k+1)$ -transitivement sur X . Alors G agit transitivement sur X . Soient $(x_1, \dots, x_k)$ et $(y_1, \dots, y_k)$ deux k -uplets d'éléments distincts de Y . Alors $(x, x_1, \dots, x_k)$ et $(x, y_1, \dots, y_k)$ sont des $(k+1)$ -uplets d'éléments distincts de X . Par $(k+1)$ -transitivité de l'action de G , il existe $g \in G$ avec $g(x) = x$ et $g(x_i) = y_i$ pour $i = 1, \dots, k$. On a donc $g \in G_x$, et G_x est bien k -transitif sur Y . Réciproquement supposons que G agit transitivement sur X , et que G_x agit k -transitivement sur Y . Soient $(x_1, \dots, x_{k+1})$ et $(y_1, \dots, y_{k+1})$ des $(k+1)$ -uplets d'éléments distincts dans X . Par transitivité de G sur X , il existe $g, h \in G$ tels que $g(x_1) = x$ et $h(y_1) = x$. Les k -uplets $(g(x_2), \dots, g(x_{k+1}))$ et $(h(y_2), \dots, h(y_{k+1}))$ sont bien constitués d'éléments distincts de Y . Par k -transitivité de G_x sur Y , il existe $\sigma \in G_x$ vérifiant $\sigma(g(x_i)) = h(y_i)$ pour tout $2 \leq i \leq k+1$. Ainsi, l'élément $h^{-1}\sigma g$ envoie x_i sur y_i pour $2 \leq i \leq k+1$, et aussi pour $i = 1$.

2. En déduire que si G est fini et agit k -transitivement sur X , alors l'entier $|X|(|X|-1)(|X|-2)\cdots(|X|-k+1)$ divise $|G|$.

On a $|G| = |X||G_x|$ par la formule orbite stabilisateur car G agit transitivement sur X . On raisonne par récurrence sur k . Le cas $k = 1$ est simplement la formule que l'on vient d'écrire. Pour $k > 1$ on sait que G_x agit $(k-1)$ -transitivement sur $Y = X - \{x\}$, et donc $|G_x|$ est multiple de $|Y|(|Y|-1)\cdots(|Y|-k+2)$. On conclut par $|G| = |X||G_x|$ et $|Y| = |X| - 1$. Deuxième méthode : notons $A_{X,k}$ l'ensemble des k -uplets d'éléments de X deux à deux distincts. Alors G agit transitivement sur $A_{X,k}$ donc $|A_{X,k}|$ divise $|G|$ (c'était la question 1 de l'exercice 1 du TD n°2, conséquence de la formule orbite-stabilisateur lorsqu'il n'y a qu'une orbite) et on conclut en calculant $|A_{X,k}| = |X|(|X|-1)(|X|-2)\cdots(|X|-k+1)$.

✂ Exercice 1. Quelques faits sur S_n

1. Montrer que le centre de S_n est trivial pour $n > 2$.

Soit σ dans le centre de S_n . Écrivons que σ commute à la transposition $(i \ j)$. On a $(i \ j) = \sigma(i \ j)\sigma^{-1} = (\sigma(i) \ \sigma(j))$, i.e. $\sigma(\{i, j\}) = \{i, j\}$. Ainsi, si σ préserve toutes les parties à 2 éléments de $\{1, \dots, n\}$. Comme on a $n \geq 3$, pour tout $i \in \{1, \dots, n\}$ on peut trouver $j, k \in \{1, \dots, n\}$ avec i, j, k distincts. On a alors $\{i\} = \{i, j\} \cap \{i, k\}$ puis $\sigma(i) = i$: σ est l'identité.

2. Soit $n \geq 2$ un entier. Montrer, sans utiliser la classification des sous-groupes distingués de S_n , qu'il existe un unique morphisme non trivial $S_n \rightarrow \{\pm 1\}$. En déduire que A_n est le seul sous-groupe d'indice 2 de S_n .

Un morphisme de groupes $f : G \rightarrow G'$ avec G' abélien est constant sur les classes de conjugaison de G : si on a $g, x \in G$ alors $f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g)f(g)^{-1}f(x) = f(x)$. Comme deux transpositions sont conjuguées dans S_n , tout morphisme $S_n \rightarrow \{\pm 1\}$ prend la même valeur $\varepsilon \in \{\pm 1\}$ sur chaque transposition. Comme les transpositions engendrent S_n , il y a donc au plus deux morphismes $S_n \rightarrow \{\pm 1\}$. Pour $\varepsilon = 1$, le morphisme est nécessairement trivial (et existe bien). Pour $\varepsilon = -1$, il existe encore : c'est la signature. Ensuite, pour tout sous-groupe H d'indice 2 d'un groupe G on a vu en cours qu'il existe un morphisme $G \rightarrow \{\pm 1\}$ de noyau H . En effet, on sait que H est distingué, et on regarde alors la composée de la projection canonique $G \rightarrow G/H$ et de l'unique isomorphisme $G/H \simeq \{\pm 1\}$. Comme il n'y a qu'un morphisme non trivial $S_n \rightarrow \{\pm 1\}$ par ce qui précède, à savoir la signature, A_n est le seul sous-groupe d'indice 2 de S_n .

3. Montrer que si un sous-groupe $G \subseteq S_n$ agit $(n-2)$ -transitivement sur $\{1, \dots, n\}$, alors on a $G = A_n$ ou $G = S_n$.

Le fait que S_n et A_n agissent respectivement n -transitivement et $(n-2)$ -transitivement sur $\{1, \dots, n\}$ est du cours. Réciproquement, si $G \subseteq S_n$ agit $(n-2)$ -transitivement sur $\{1, \dots, n\}$ on a que $\frac{n!}{2}$ divise $|G|$ par le second point du préambule. On en déduit que G est d'indice 1 ou 2. Mais on a vu à la question précédente que A_n est l'unique sous-groupe d'indice 2 de S_n .

✂ Exercice 2. Quelques contre-exemples avec A_4

1. Montrer que A_4 ne possède pas de sous-groupe d'ordre 6.

On a $|A_4| = 12$. Si A_4 admet un sous-groupe H d'ordre 6, ce sous-groupe est donc d'indice 2, puis le noyau d'un morphisme surjectif $A_4 \rightarrow \{\pm 1\}$. Or il n'y a pas de tel morphisme (soit on invoque le cours, soit on dit que A_n est

engendré par les 3-cycles et si c est un 3-cycle et $f : A_n \rightarrow \{\pm 1\}$ un morphisme, on a $f(c) = 1$ puisque $f(c^3) = f(c)^3 = 1$ d'une part et $f(c) = \pm 1$ d'autre part (plus généralement, si on a un morphisme $f : G \rightarrow G'$ et $g \in G$ tels que l'ordre de g est premier à $|G'|$, alors on a $f(g) = 1$). C'est le contre-exemple à la réciproque naïve du théorème de Lagrange.

- Soient G, H, K trois groupes avec $H \triangleleft K$ et $K \triangleleft G$. En examinant A_4 , vérifier que l'on n'a pas nécessairement $H \triangleleft G$. Montrer que si H est caractéristique dans K (c'est-à-dire stable par tout automorphisme de K), alors on a $H \triangleleft G$. On pose $G = A_4$ et $K = K_4$. On a $K \triangleleft G$. Soit H le sous-groupe $\langle (1\ 2)(3\ 4) \rangle$ de K_4 . C'est un sous-groupe d'ordre 2 et distingué dans K_4 , ce dernier étant abélien. Mais il n'est pas distingué dans A_4 , car $(1\ 2\ 3)(1\ 2)(3\ 4)(1\ 2\ 3)^{-1} = (2\ 3)(1\ 4) \notin H$. Pour la deuxième partie de la question, soit $g \in G$. Alors l'automorphisme $\alpha := \text{int}_g$ de G vérifie $\alpha(K) = K$ car K est distingué dans G , de sorte que l'on a $\alpha|_K \in \text{Aut}(K)$. Comme H est caractéristique dans K , on a $\alpha|_K(H) = H$, i.e. $gHg^{-1} = H$. On a montré que H est distingué dans G .

Exercice 3. Classes de conjugaison de A_n

Soit $\sigma \in A_n$. On dira que σ est *non spécial* s'il existe $\tau \in S_n$ avec $\tau\sigma = \sigma\tau$ et $\varepsilon(\tau) = -1$, et qu'il est *spécial* sinon.

- Montrer que σ est non spécial si, et seulement si, il existe une σ -orbite de cardinal pair ou deux σ -orbites de même cardinal impair.

Supposons que σ possède un cycle c de cardinal pair. Alors $\tau = c$ convient. Supposons que σ possède deux cycles de même cardinal m impair, disons $(i_1\ i_2\ \dots\ i_m)$ et $(j_1\ j_2\ \dots\ j_m)$. Alors $\tau = (i_1\ j_1)(i_2\ j_2)\dots(i_m\ j_m)$ est de signature $(-1)^m = -1$ et vérifie $\tau\sigma\tau^{-1} = \sigma$. Si σ a deux points fixes i et j alors $\tau = (i\ j)$ convient aussi. Supposons enfin $\sigma = c_1 c_2 \dots c_r$ avec les c_i de longueur impaires distinctes, et au plus un point fixe. Soient C le centralisateur de σ dans S_n et $\tau \in C$. On sait que les cycles de $\tau\sigma\tau^{-1} = \sigma$ sont les $\tau c_i \tau^{-1}$. Par unicité des longueurs des cycles, on a donc $\tau c_i \tau^{-1} = c_i$ pour tout i . En particulier, τ préserve le support S_i de chaque c_i , ainsi que l'éventuel point fixe de σ . Quitte à multiplier τ par un élément du sous-groupe $H = \langle c_1, c_2, \dots, c_r \rangle \subseteq C$, on peut supposer que τ admet un point fixe dans chacun des S_i . La formule $\tau c_i \tau^{-1} = c_i$ montre alors $\tau|_{S_i} = \text{id}_{S_i}$, puis $\tau = 1$. On a montré $C = H$. On conclut car $\varepsilon(c_i) = 1$ pour tout i , et donc $\varepsilon(C) = \{1\}$.

- Montrer que si σ est non spécial, on a $\text{Conj}_{S_n}(\sigma) = \text{Conj}_{A_n}(\sigma)$.

Supposons $\sigma \in A_n$ non spécial. Soit $\tau \in S_n$ avec $\tau\sigma = \sigma\tau$ et $\varepsilon(\tau) = -1$. Pour tout $g \in S_n - A_n$ on a $g\sigma g^{-1} = g\tau\sigma(g\tau)^{-1}$ avec $g\tau \in A_n$. L'inclusion évidente $\text{Conj}_{A_n}(\sigma) \subset \text{Conj}_{S_n}(\sigma)$ est donc une égalité.

- On suppose σ spécial et $s \in S_n - A_n$. Montrer $\text{Conj}_{S_n}(\sigma) = \text{Conj}_{A_n}(\sigma) \sqcup \text{Conj}_{A_n}(s\sigma s^{-1})$.

Supposons $\sigma \in A_n$ spécial et fixons $s \in S_n - A_n$. On a $S_n = A_n \sqcup A_n s$ car A_n est d'indice 2 dans S_n . On en déduit que pour $g \in S_n - A_n$, on a $g = hs$ pour un certain $h \in A_n$, puis $g\sigma g^{-1} = hs\sigma s^{-1}h^{-1}$. Cela montre $\text{Conj}_{S_n}(\sigma) = \text{Conj}_{A_n}(\sigma) \cup \text{Conj}_{A_n}(s\sigma s^{-1})$. Supposons enfin que l'on a $g\sigma g^{-1} = hs\sigma s^{-1}h^{-1}$ avec g, h dans A_n . Alors l'élément $s^{-1}h^{-1}g \in S_n$ commute avec σ et il est de signature -1 : absurde.

- En déduire des représentants des classes de conjugaison de A_4 et A_5 .

Par le cours, des représentants des classes de conjugaison de S_4 incluses dans A_4 sont 1, $(1\ 2)(3\ 4)$, $(1\ 2\ 3)$. Les éléments 1 et $(1\ 2)(3\ 4)$ sont non spéciaux dans S_4 , mais $(1\ 2\ 3)$ y est spécial. Des représentants des classes de conjugaison de A_4 sont donc 1, $(1\ 2)(3\ 4)$, $(1\ 2\ 3)$ et $(2\ 1\ 3)$ (on a pris $s = (1\ 2)$). De même, des représentants des classes de conjugaison de S_5 incluses dans A_5 sont 1, $(1\ 2)(3\ 4)$, $(1\ 2\ 3)$ et $(1\ 2\ 3\ 4\ 5)$. Les éléments 1, $(1\ 2)(3\ 4)$, $(1\ 2\ 3)$ sont non spéciaux dans S_5 , mais $(1\ 2\ 3\ 4\ 5)$ y est spécial. Des représentants des classes de conjugaison de A_4 sont donc 1, $(1\ 2)(3\ 4)$, $(1\ 2\ 3)$, $(1\ 2\ 3\ 4\ 5)$ et $(2\ 1\ 3\ 4\ 5)$.

Exercice 4. Une présentation de S_n

Pour $n \geq 2$ et $1 \leq i \leq j < n$ on définit $m_{i,j}$ en posant $m_{i,i} = 2$, $m_{i,j} = 3$ pour $j = i + 1$, et $m_{i,j} = 0$ sinon. Soit G un groupe engendré par des éléments $s_1, \dots, s_{n-1}$ vérifiant $(s_i s_j)^{m_{i,j}} = 1$ pour tout $1 \leq i \leq j < n$.

- Vérifier que pour tout $1 \leq i, j < n$ on a $s_i^2 = 1$, $s_i s_j = s_j s_i$ pour $|j - i| > 1$, ainsi que $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$ (relation de tresse) pour $i < n - 1$.

Pour $i = j$ on a $s_i^2 = 1$. Mais si on a $s_i^2 = s_j^2 = 1$, les relations $s_i s_j s_i s_j = 1$ et $s_i s_j s_i s_j s_i s_j = 1$ s'écrivent respectivement $s_i s_j = s_j s_i$ et $s_i s_j s_i = s_j s_i s_j$.

- On pose $f_i = s_i s_{i+1} \dots s_n$ pour $1 \leq i < n$, et $f_n = 1$. Montrer que pour tout $g \in G$, il existe $1 \leq i \leq n$ et $h \in \langle s_1, \dots, s_{n-2} \rangle$ vérifiant $g = f_i h$.

On raisonne par récurrence sur n . Le cas $n = 1$ est trivial, car on a $G = \{1, s_1\}$. On suppose $n > 1$. Soit $g \in G$. Utilisant $s_n^2 = 1$ on peut écrire

$$g = h_1 s_n h_2 s_n \dots s_n h_k, \quad (\star)$$

pour un certain $k \geq 1$ et des éléments $h_1, \dots, h_k$ dans $H := \langle s_1, \dots, s_{n-1} \rangle$. Si on a $k = 1$, alors g est dans H , et il n'y a rien à démontrer. Sinon, l'élément h_2 s'écrit par récurrence $h_2 = s_i s_{i+1} \dots s_{n-1} h'_2$ avec $1 \leq i \leq n$ et $h'_2 \in \langle s_1, \dots, s_{n-2} \rangle$. Supposons d'abord $k > 2$. Comme s_n commute aux s_i avec $i < n-1$ par hypothèse, on a donc

$$s_n h_2 s_n = s_i s_{i+1} \dots s_n s_{n-1} s_n h'_2$$

La relation de tresse permet de remplacer $s_n s_{n-1} s_n$ par $s_{n-1} s_n s_{n-1}$. Le nombre k d'occurrences de s_n dans l'écriture $(\star)$ de g a donc chuté de 1. Par récurrence sur k , on peut donc supposer $k = 2$, i.e. $g = h_1 s_n h_2$. Écrivons $h_1 = s_j s_{j+1} \dots s_{n-1} h'_1$ avec $1 \leq j \leq n$ et $h'_1 \in \langle s_1, \dots, s_{n-2} \rangle$. Comme s_n commute aux s_j avec $j < n-1$ on a donc

$$g = h_1 s_n h_2 = s_j s_{j+1} \dots s_{n-1} s_n h'_1 h_2 = f_j h'_1 h_2 \in f_j H$$

3. En déduire que G est fini de cardinal $\leq n!$.

On raisonne par récurrence sur n . C'est évident pour $n = 1$ car alors $G = \{1, s_1\}$ est de cardinal ≤ 2 . Le sous-groupe H de G engendré par les s_i avec $i < n$ satisfait l'hypothèse de récurrence, et donc vérifie $|H| \leq n!$. On a donc $|G| \leq (n+1)n! = (n+1)!$ par la question précédente.

4. Montrer $S_n \cong \langle s_1, \dots, s_{n-1} | (s_i s_j)^{m_{i,j}} = 1, 1 \leq i \leq j < n \rangle$.

On constate que les n transpositions $t_i := (i \ i+1)$ de S_{n+1} , avec $1 \leq i \leq n$, satisfont $(t_i t_j)^2 = 1$ pour $i = j$ et $|i - j| > 1$, et que l'élément $t_i t_{i+1} = (i \ i+1 \ i+2)$, pour $i < n$, vérifie aussi $(t_i t_{i+1})^3 = 1$. Soit Γ le groupe de droite défini par les générateurs s_i avec $1 \leq i \leq n$, et les relations $(s_i s_j)^{m_{i,j}} = 1$ pour tout $1 \leq i \leq j \leq n$. Par la propriété universelle de Γ , on a un unique morphisme de groupes

$$f : \Gamma \rightarrow S_{n+1}$$

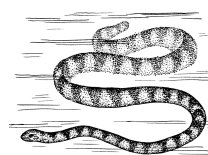
vérifiant $f(s_i) = t_i$ pour tout $i = 1, \dots, n$. Mais les t_i engendrent S_{n+1} par le cours, donc f est surjectif. On a aussi $|\Gamma| \leq (n+1)!$ par la question précédente. Le morphisme f est donc un isomorphisme.

Exercice 5. Taquin et serpents (A. E. Archer, "A modern treatment of the 15-puzzle" (1999))

Le taquin est un jeu constitué d'un carré 4×4 , lui-même constitué de 15 cases 1×1 mobiles numérotées de 1 à 15, et d'une case vide. Partant de la configuration initiale E_0 indiquée à gauche ci-dessous, et en déplaçant d'une case autant de fois qu'on le souhaite la case vide, on se trouve donc dans un état du jeu comme l'état E_1 représenté juste à droite de E_0 . On se propose d'étudier les états possibles du jeu et de déterminer si A , B et C ci-dessous en font partie.

E_0				E_1				A				B				C			
1	2	3	4	5	1	2	3	1	2	3	4		1	2	3		1	2	3
5	6	7	8	6	10	7	4	5	6	7	8	4	5	6	7	4	5	6	7
9	10	11	12	9		11	8	9	10	11	12	8	9	10	11	8	9	10	11
13	14	15		13	14	15	12	13	15	14		12	13	14	15	12	13	15	14

Notons $\mathcal{E}$ l'ensemble des états possibles du taquin. À chaque état $E \in \mathcal{E}$ on associe son serpent $s(E)$ qui est la suite $(x_1, x_2, \dots, x_{15})$ de tous les nombres de 1 à 15 obtenue en lisant le taquin dans l'ordre indiqué par le serpent de mer ci-contre et en omettant la case vide. Par exemple, le serpent de l'état initial $E_0 \in \mathcal{E}$ du jeu est la suite $s(E_0) = (1, 2, 3, 4, 8, 7, 6, 5, 9, 10, 11, 12, 15, 14, 13)$. Pour $E \in \mathcal{E}$ et $s(E) = (x_1, x_2, \dots, x_{15})$, on note aussi $\sigma(E)$ l'unique élément de S_{15} tel que $x_i = \sigma(i)$.



1. Soient $E, F \in \mathcal{E}$ tels que F est obtenu à partir de E et d'un seul déplacement de la case vide. Vérifier que l'élément $\sigma(E)^{-1} \sigma(F) \in S_{15}$ ne dépend que des positions originale et finale de la case vide (et non de E), et donner son type.

Si la case vide est déplacée horizontalement pour passer de E à F , ou plus généralement en suivant le serpent, on a $s(E) = s(F)$ et donc $\sigma(F) = \sigma(E)$. Sinon nous allons voir que $\sigma(E)^{-1} \sigma(F)$ est un cycle de longueur 3, 5 ou 7 qui ne dépend pas de E . En effet, supposons par exemple que la case vide se trouve à la i -ème case de la deuxième ligne et monte verticalement en première ligne. Écrivons $s(E) = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, \dots)$. Alors selon que l'on a $i = 1, 2, 3$, l'élément $s(F)$ vaut $(x_2, x_3, x_4, x_5, x_6, x_7, x_1, \dots)$, $(x_1, x_3, x_4, x_5, x_6, x_2, x_7, \dots)$ et $(x_1, x_2, x_4, x_5, x_3, x_6, x_7, \dots)$ respectivement. On constate donc que l'on a $\sigma(F) = \sigma(E) \circ \sigma_i$ avec

$$\sigma_1 = (1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7), \sigma_2 = (2 \ 3 \ 4 \ 5 \ 6) \text{ et } \sigma_3 = (3 \ 4 \ 5).$$

En étudiant de même la montée de la case vide en partant des lignes 3 et 4, on trouve les permutations suivantes (conjuguées de celles ci-dessus par $x \mapsto x+4$ et $x \mapsto x+8$) :

(7 8 9), (6 7 8 9 10), (5 6 7 8 9 10 11), (9 10 11 12 13 14 15), (10 11 12 13 14) et (11 12 13).

Bien entendu, lorsque l'on descend la case vide au lieu de la monter, on obtient les cycles inverses à ceux ci-dessus.

2. (Problème de Loyd) Le dessin A est-il un état du taquin ?

Soient $E = E_1, \dots, E_n = F$ une suite d'états du taquin obtenus par mouvements élémentaires successifs. On a

$$\sigma(E)^{-1} \sigma(F) = (\sigma(E_1)^{-1} \sigma(E_2)) (\sigma(E_2)^{-1} \sigma(E_3)) \dots (\sigma(E_{n-1})^{-1} \sigma(F)). \quad (\star)$$

Ainsi, on constate que $\sigma(E)^{-1} \sigma(F)$ est un produit de $n-1$ éléments parmi les 9 cycles ci-dessus et leurs inverses. Comme tous ces cycles sont de longueur impaire, il est dans A_{15} . Si le taquin A donné était dans $\mathcal{E}$ on aurait donc $\sigma(E_0)^{-1} \sigma(A) = (13\ 14) \in A_{15}$, une contradiction. (Le créateur de casse-têtes Sam Loyd avait promis mille dollars à qui trouverait comment obtenir l'état A sur le taquin !)

3. Déterminer $\{\sigma(E)^{-1} \sigma(F) \mid E, F \in \mathcal{E}\} \subseteq S_{15}$. En déduire quel dessin, parmi B et C, est un état du taquin.

La formule $(\star)$ de la question précédente ainsi que la question 1 montrent que l'ensemble G de l'énoncé est un sous-groupe de S_{15} inclus dans A_{15} . Mieux, c'est le sous-groupe de A_{15} engendré par les 9 cycles indiqués plus haut. On constate que G agit 3-transitivement sur $\{1, \dots, 15\}$. En effet, la transitivité est claire rien que grâce aux trois 7-cycles. La transitivité du stabilisateur G_1 sur $\{2, \dots, 15\}$ est aussi claire à cause de $(2\ 3\ 4\ 5\ 6)$, $(5\ 6\ 7\ 8\ 9\ 10\ 11)$ et $(9\ 10\ 11\ 12\ 13\ 14\ 15)$. Enfin, la transitivité du stabilisateur $(G_1)_2$ sur $\{3, \dots, 15\}$ est encore claire à cause de $(3\ 4\ 5)$, $(5\ 6\ 7\ 8\ 9\ 10\ 11)$ et $(9\ 10\ 11\ 12\ 13\ 14\ 15)$. On conclut par le premier point du préambule. Comme G contient le 3-cycle $(3\ 4\ 5)$, il contient par conjugaison tous les $(\sigma(3)\sigma(4)\sigma(5))$ avec $\sigma \in G$ et donc tous les 3-cycles par 3-transitivité de G . On a montré $G = A_{15}$. Pour la deuxième partie de la question, on a $\sigma(C)^{-1} \sigma(B) = (13\ 14)$ donc un seul de B ou C est un état du taquin par ce qui précède. On a $s(B) = (1, 2, 3, 7, 6, 5, 4, 8, 9, 10, 11, 15, 14, 13, 12)$, et donc on constate

$$\sigma(E_0)^{-1} \sigma(B) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 1 & 2 & 3 & 6 & 7 & 8 & 4 & 5 & 9 & 10 & 11 & 13 & 14 & 15 & 12 \end{bmatrix},$$

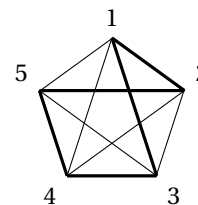
qui vaut aussi $(4\ 6\ 8\ 5\ 7)(12\ 13\ 14\ 15)$. Il n'est pas dans A_{15} : c'est donc le C qui est un état du taquin.

4. Montrer $|\mathcal{E}| = \frac{16!}{2} = 10\ 461\ 394\ 944\ 000$.

Il est clair que l'on a $s(F) = s(F')$ si, et seulement si, F' est obtenu à partir de F et d'un déplacement de la case vide le long du serpent. Il y a donc exactement 16 tels F' à F donné. Il est équivalent de se donner $s(F)$ et $\sigma(F)$, ou encore son translaté $\sigma(E_0)^{-1} \sigma(F)$. L'application $\mathcal{E} \rightarrow G, F \mapsto \sigma(E_0)^{-1} \sigma(F)$, est donc surjective, et toutes ses fibres ont 16 éléments. On en déduit $|\mathcal{E}| = 16 |A_{15}| = 16!/2$.

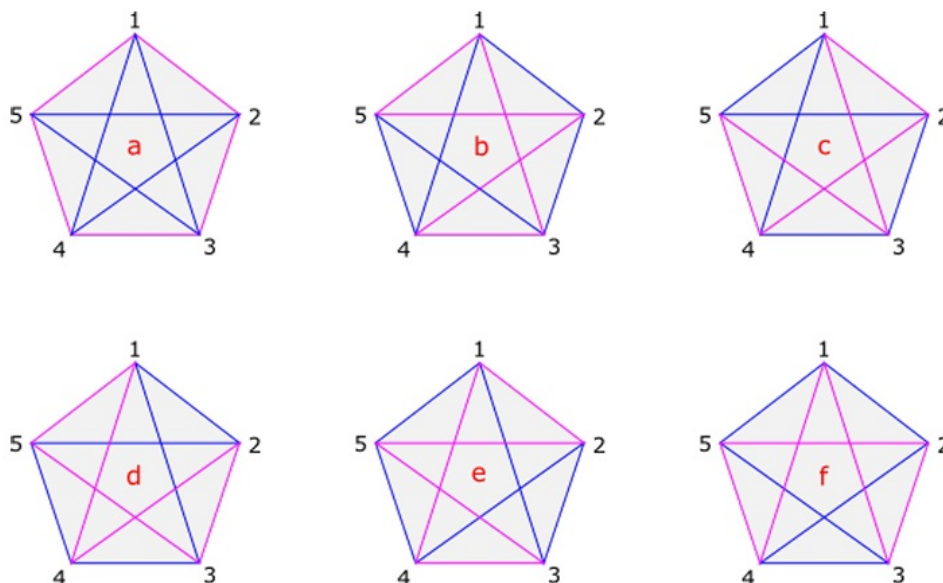
✂ Exercice 6. Une action exotique de S_5

Dans cet exercice, on va décrire de deux manières différentes une action transitive de S_5 sur un ensemble à 6 éléments. On commence par le point de vue développé dans l'article "A description of the outer automorphism of S_6 and the invariants of 6 points in the projective space" publié en 2007 par Howard, Millson, Snowden et Vakil. Soit $\mathcal{G}$ le graphe non orienté et complet de sommets $\{1, 2, 3, 4, 5\}$. Ce graphe a exactement 10 arêtes.



1. Un *circuit hamiltonien* sur $\mathcal{G}$ est un circuit de longueur 5 passant une et une seule fois par chaque sommet (voir ci-contre, en gras). Montrer qu'il existe exactement 6 partitions des 10 arêtes de $\mathcal{G}$ en réunion disjointe de deux circuits hamiltoniens.

Il existe $4! = 24$ circuits hamiltoniens orientés (on choisit l'ordre des 4 sommets distincts de $\{2, 3, 4, 5\}$ qui suivent le sommet 1), donc $24/2 = 12$ circuits hamiltoniens et $12/2 = 6$ partitions en deux circuits hamiltoniens. Les voici :



Hormis dans le cas du pentagone a , on constate que chaque pentagone est formé d'un poisson et d'une chauve-souris ! Notons $\{a, b, c, d, e, f\}$ l'ensemble de ces 6 partitions de $\mathcal{G}$.

2. Notons X l'ensemble de ces 6 partitions de $\mathcal{G}$ (on les appelle les 6 *pentagones mystiques*). L'action naturelle de S_5 sur $\{1, \dots, 5\}$ induit une action de S_5 sur X . Montrer que cette action est transitive.

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 $(2\ 1\ 5\ 3\ 4)$ (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 autre description de l'action ci-dessus. Soit Y l'ensemble des sous-groupes d'ordre 5 de S_5 .

3. Montrer que $|Y| = 6$ et que l'action de S_5 sur Y , via $(\sigma, H) \mapsto \sigma H \sigma^{-1}$, est transitive.

On a $|Y| = 6$ car 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 $\{a, b, c\} = \{3, 4, 5\}$. L'action est transitive car deux 5-cycles quelconques sont conjugués dans S_5 .

4. Montrer que cette action de S_5 est isomorphe à celle sur les pentagones mystiques.

Tout sous-groupe $H = \langle c \rangle$ d'ordre 5 de S_5 définit un unique pentagone $p(H)$ donné par les deux chemins non orientés $c^{\pm 1}$ et $c^{\pm 2}$. L'application $p : Y \rightarrow X, H \mapsto p(H)$, est manifestement bijective. Enfin, pour $\sigma \in S_5$ et $c = (i_1\ i_2\ i_3\ i_4\ i_5)$ on a $\sigma c \sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \sigma(i_3)\ \sigma(i_4)\ \sigma(i_5))$. On a donc $p(\sigma H \sigma^{-1}) = \sigma \cdot p(H)$ pour tout $H \in Y$: c est un isomorphisme d'action.

On va voir avec cette deuxième description que l'action est fidèle et 3-transitive. Soit G le sous-groupe de S_6 engendré par $(1\ 2\ 3\ 4\ 5)$ et $(1\ 2)(3\ 6)(5\ 4)$.

5. Montrer que l'action naturelle de G sur $\{1, 2, \dots, 6\}$ est 3-transitive.

On pose $c = (1\ 2\ 3\ 4\ 5)$, $t = (1\ 2)(3\ 6)(5\ 4)$. L'orbite de 6 sous l'action de G contient $3 = t(6)$, puis $\{1, 2, 3, 4, 5\} = \{c^i(3) \mid i \in \mathbb{Z}\}$, ainsi bien sûr que 6 : l'action en question de G est donc transitive. Pour montrer qu'elle est 2-transitive, on utilise le premier point du préambule. Il suffit de voir que G_6 agit transitivement sur $\{1, 2, 3, 4, 5\}$, mais c'est clair car on a $c \in G_6$. On constate enfin que l'on a

$$ct = (1\ 2\ 3\ 4\ 5)(1\ 2)(3\ 6)(5\ 4) = (1\ 3\ 6\ 4)$$

Mais toujours par le premier point du préambule, l'action de G est 3-transitive si, et seulement si, celle de $G_2 \cap G_5$ est transitive sur $\{1, 3, 4, 6\}$. On conclut car on vient de voir $(1\ 3\ 6\ 4) \in G_2 \cap G_5$.

6. En déduire que l'action de S_5 sur les pentagones mystiques est fidèle, et que l'on a $G \simeq S_5$.

On déduit de la question précédente et du second point du préambule que $|G|$ est divisible par $6 \cdot 5 \cdot 4 = 120$. Mais on a construit au début du présent exercice un morphisme $\phi : S_5 \rightarrow S_X$ avec $X = \{a, b, c, d, e, f\}$ envoyant $(1\ 2)$ sur $(a\ d)(b\ c)(e\ f)$ et $(1\ 2\ 3\ 4\ 5)$ sur $(b\ c\ d\ e\ f)$. Identifiant X à $\{1, \dots, 6\}$ en envoyant respectivement a, b, c, d, e, f sur $6, 1, 2, 3, 4, 5$, et donc S_X à S_6 , on a alors $t = \phi((1\ 2))$ et $c = \phi((1\ 2\ 3\ 4\ 5))$. On a donc $G \subseteq \phi(S_5)$. Mais on a à la fois $|\phi(S_5)| = |\ker \phi| = |S_5| = 120$ et $|G| \geq 120$. Cela montre $\ker \phi = \{1\}$ (donc l'action correspondante est fidèle) et $G = \phi(S_5) \simeq S_5$.

Cette action est à l'origine de nombreuses autres constructions autour de la géométrie des ensembles de petit cardinal. Elle permet notamment de construire un automorphisme non intérieur de S_6 . Elle est très spécifique : on peut montrer qu'elle est unique à isomorphisme près, que S_n n'admet pas d'action transitive sur un ensemble à $n+1$ éléments pour $n \neq 5$, et que tout automorphisme de S_n est intérieur pour $n \neq 6$.

Exercice 7. Le groupe de Mathieu M_{11} (J. Conway, "Three lectures on exceptional groups" (1993))

Soit M_{11} le sous-groupe de A_{11} engendré par les éléments $a = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11)$ et $b = (3\ 7\ 11\ 8)(4\ 10\ 5\ 6)$.

1. Montrer que M_{11} possède des éléments de type 11 , $1\ 2\ 8$, $1\ 5^2$, $1^2\ 3^3$ et $1^3\ 4^2$. Pour cela, on pourra vérifier les égalités $b^2 a = (1\ 2\ 11)(3\ 5\ 10)(6\ 8\ 9)$, $aba^{-1}b^{-1} = (1\ 9\ 4\ 7\ 3)(5\ 10\ 8\ 6\ 11)$ et $aba = (1\ 3\ 11\ 2\ 8\ 10\ 9\ 6)(4\ 7)$.

Les égalités données se vérifient immédiatement en appliquant l'algorithme donnant la décomposition en cycle d'une permutation. Étant donné la notation pour les types discutée en cours, les éléments $a, b, b^2 a, [a, b]$ et aba sont respectivement de type $11, 1^3\ 4^2, 1^2\ 3^3, 1\ 5^2$ et $1\ 2\ 8$.

2. En déduire (sans calcul) que M_{11} agit 3-transitivement sur $\{1, \dots, 11\}$.

Comme $G := M_{11}$ possède un 11 -cycle, il agit transitivement sur $E = \{1, 2, \dots, 11\}$. On va appliquer de nombreuses fois le critère de multiple transitivité du préambule. Observons que si G possède un élément g ayant un point fixe x dans E , alors pour tout $y \in E$, il existe $h \in G$ de même type que g , et avec en outre $h(y) = y$. En effet, comme G agit transitivement sur E , il existe $\sigma \in G$ avec $\sigma(x) = y$, et $h = \sigma g \sigma^{-1}$ convient. On déduit de cela que pour tout $x \in E$, le stabilisateur G_x de x dans G , qui agit naturellement sur $E' = E - \{x\}$, possède des éléments de type $1^2\ 4^2$, $1\ 3^3$, 5^2 et $2\ 8$ vus dans $S_{E'}$. La présence de $2\ 8$ et 5^2 par exemple montre que G_x agit transitivement sur E' .

Rappliquant l'observation ci-dessus à G_x agissant sur E' , on en déduit que pour tout $y \in E'$, $(G_x)_y = G_x \cap G_y$ possède des éléments de types $1\ 4^2$ et 3^3 vus comme éléments de $S_{E''}$ avec $E'' = E - \{x, y\}$. Cela force la transitivité de $(G_x)_y$ sur E'' . En effet, on peut dire qu'une orbite de ce dernier doit être de cardinal à la fois multiple de 3, et égal à 1, 4, 1+4, 4+4 ou 1+4+4. La seule possibilité est le cardinal 9.

Soit $E = \{1, \dots, 11\}$. Pour $F \subseteq E$ on pose $G_F = \{g \in M_{11} \mid g(F) = F\}$.

3. Montrer (sans calcul) que si $F \subseteq E$ a trois éléments, alors G_F agit transitivement sur $E - F$. En déduire que M_{11} agit transitivement sur l'ensemble des parties à 4 éléments de E .

On a vu que G agit 3-transitivement sur E . En particulier, il permute transitivement les parties à 3 éléments de E . Soit F une telle partie. Noter que G_F préserve F et son complémentaire $E - F$, mais que G_F n'agit pas nécessairement trivialement sur F . D'après la première question, observons que G_F contient des éléments de type 4^2 , $1^2\ 3^2$ et 8 vus comme éléments de S_{E-F} (c'est une variante de l'observation de la question 2). Il suffit de voir que si G possède un élément g ayant une partie stable $S \subseteq E$ à 3 éléments, alors il existe $h \in G_F$ tel que $h|_F$ a même type que $g|_S$ et $h|_{E-F}$ a même type que $g|_{E-S}$. Mais comme l'action de G permute transitivement les parties à 3 éléments de E , il existe $\sigma \in G$ avec $\sigma(S) = F$, et $h = \sigma g \sigma^{-1}$ convient. Cela conclut l'observation. Comme G_F possède un élément qui agit comme un 8-cycle sur $E - F$, il agit bien transitivement sur $E - F$, puis transitivement sur les parties à 4 éléments de E .

4. Soient $F \subseteq E$ avec $|F| = 4$, et $f : G_F \rightarrow S_F$ le morphisme naturel. Montrer (sans calcul) que $f(G_F)$ contient un 4-cycle et un 3-cycle. En déduire $f(G_F) = S_F$.

Comme G agit transitivement sur les parties à 4 éléments de E , l'argument ci-dessus et la question 1 montrent que G_F contient des éléments de type $1\ 3$ et 4 vus comme permutations de F . Il reste à voir qu'un sous-groupe H de S_4 engendré par un 4-cycle et un 3-cycle est S_4 . On peut le faire à la main, ou observer que le cardinal de H serait multiple de $3 \cdot 4 = 12$ par Lagrange, donc H serait d'indice 1 ou 2. Mais A_4 est l'unique sous-groupe d'ordre 12 de S_4 (c'était la question 2 de l'exercice 1), et H contient un 4-cycle, non dans A_4 , on a donc bien $H = S_4$.

5. Montrer que M_{11} agit 4-transitivement sur $\{1, 2, \dots, 11\}$, puis montrer que $|M_{11}|$ est multiple de $\frac{11!}{7!} = 7\ 920$.

La seconde assertion découle de la première et du second point du préambule. Pour la première, soient (x_1, x_2, x_3, x_4) et (y_1, y_2, y_3, y_4) des 4-uplets d'éléments distincts de E . On pose $X = \{x_1, x_2, x_3, x_4\}$ et $Y = \{y_1, y_2, y_3, y_4\}$. Par la question 3, il existe $g \in M_{11}$ avec $g(X) = Y$. Posons $x'_i = g(x_i)$ pour tout $1 \leq i \leq 4$. Par la question 4, il existe $h \in G_Y$ avec $h(x'_i) = y_i$ pour tout $1 \leq i \leq 4$. L'élément $gh \in G$ envoie bien x_i sur y_i pour tout $1 \leq i \leq 4$.

Mathieu a démontré l'égalité $|M_{11}| = 7\,920$ et que M_{11} est simple : c'est le plus petit des groupes simples dits sporadiques. Mathieu a en fait construit explicitement, entre 1861 et 1873, 5 groupes simples $M_n \subseteq S_n$, pour $n = 11, 12, 22, 23$ et 24 . La détermination de leur cardinal fut un temps controversée, ou même simplement le fait qu'ils ne sont pas égaux à A_n .