

Fiche d'exercices n° 3 - Corrigés

Groupes et géométrie

Groupes symétriques

Exercice 1.

$$\begin{aligned}
 \sigma_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 6 & 2 & 1 \end{pmatrix} \\
 &= (1346)(25) \text{ décomposition canonique} \\
 &= (13)(34)(46)(25) \text{ une décomp. en prod. de transpo.} \\
 &= (13)(13)(14)(13)(46)(25) \\
 &= (14)(13)(46)(25) \text{ une autre décomp. en prod. de transpo.} \\
 &= (14)(13)(14)(16)(14)(12)(15)(12) \text{ une décomp. en prod. de transpo. du type } (1 \ i)
 \end{aligned}$$

Pour avoir la décomposition en produit de transpositions du type $(i \ i+1)$, remarquons que $(p \ q) = (q-1 \ q)(p \ q-1)(q-1 \ q)$ (où $q-p \geq 2$)

$$\begin{aligned}
 \sigma_1 &= (14)(13)(46)(35) \\
 &= (34)(13)(34).(23)(12)(23).(56)(45)(56).(45)(24)(45) \\
 &= (34)((23)(12)(23))(34).(23)(12)(23).(56)(45)(56).(45)((34)(23)(34))(45)
 \end{aligned}$$

Les $(i \ i+1)$ engendrent les transpositions, qui engendrent les cycles, qui engendrent le groupe symétrique S_n .

$\sigma_1 = (1346)(25)$ est décomposé en produit de cycles à supports disjoints, donc qui commutent.

$o(1346) = 4$ et $o(25) = 2$ donc $o(\sigma_1) = \text{ppcm}(2, 4) = 4$.

De plus, il y a deux σ_1 -orbites, donc $\varepsilon(\sigma_1) = (-1)^{6-2} = 1$.

Enfin,

$$\begin{aligned}
 \sigma_1^{50} &= (1346)^{50}(25)^{50} \\
 &= ((1346)^4)^{12} (1346)^2 ((25)^2)^{25} \\
 &= e^{12}(14)(63)e^{25} \\
 &= (14)(63)
 \end{aligned}$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 9 & 7 & 2 & 5 & 8 & 1 & 3 \end{pmatrix} = (1478)(265)(39)$$

(1478) est d'ordre 4, (265) est d'ordre 3, et (39) est d'ordre 2.

Donc $o(\sigma_2) = \text{ppcm}(4, 3, 2) = 12$.

Il y a trois σ_2 -orbites, donc $\varepsilon(\sigma_2) = (-1)^{9-3} = 1$
 De plus, on peut décomposer σ_2 en produit de (1 i) :

$$\begin{aligned}\sigma_2 &= (1478)(265)(39) \\ &= (14)(47)(78)(26)(65)(39) \\ &= (14)(14)(17)(14)(17)(18)(17)(12)(16)(12)(16)(15)(16)(13)(19)(13) \\ &= (17)(14)(17)(18)(17)(12)(16)(12)(16)(15)(16)(13)(19)(13)\end{aligned}$$

Enfin,

$$\begin{aligned}\sigma_2^{100} &= (1478)^{100}(265)^{100}(39)^{100} \\ &= ((1478)^4)^{25} \circ (265)^1 \circ ((39)^2)^{50} \\ &= (265)\end{aligned}$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 4 & 2 & 1 & 8 & 7 & 9 & 11 & 12 & 10 & 5 & 6 \end{pmatrix} = (1324)(58\ 11)(679\ 12)$$

(1324) est d'ordre 4, (58 11) est d'ordre 3, et (679 12) est d'ordre 4.

Donc $o(\sigma_3) = \text{ppcm}(4, 3, 4) = 12$.

Il y a quatre σ_3 -orbites (10 forme une orbite ponctuelle),

donc $\varepsilon(\sigma_3) = (-1)^{12-4} = 1$.

De plus, $\sigma_3 = (13)(32)(24)(58)(8\ 11)(67)(79)(9\ 12)$ est une décomposition en produit de transpositions.

Enfin,

$$\begin{aligned}\sigma_3^{10} &= ((1234)^4)^2 (1234)^2 ((58\ 11)^3)^3 (58\ 11)^1 ((679\ 12)^4)^2 (679\ 12)^2 \\ &= (1234)^2 (58\ 11)^1 (679\ 12)^2 \\ &= (12)(34)(58\ 11)(69)(7\ 12)\end{aligned}$$

Exercice 2.

Soit $\gamma = (x_0 \dots x_{k-1})$ un k -cycle dans S_n .

Déterminons pour quelles valeurs de p entier tel que $1 \leq p \leq k-1$, γ^p est un cycle.

- Si p est un entier premier à k vérifiant $1 \leq p \leq k-1$,
 alors $\gamma^p = (x_0 x_p x_{2p} \dots x_{(r-1)p})$.
 En supposant que cet ensemble a r éléments et $x_{rp} = x_0$,
 on a $rp \equiv 0[k]$.
 $k \mid rp$ et $\text{pgcd}(k, p) = 1$ donc, d'après le théorème de Gauß, $k \mid r$.
 Mais $r \leq k$, donc $r = k$, et γ^p est un k -cycle.
- Maintenant, si p et k ne sont pas premiers entre eux, on note $d = \text{pgcd}(p, k)$,
 et on a $p = dp'$ et $k = dk'$, avec $\text{pgcd}(p', k') = 1$.

$\gamma^p = (x_0 x_p \dots x_{(r-1)p}) \circ (\dots) \circ (\dots)$ est un produit de plus d'un cycle à supports disjoints, donc c'est PAS un cycle.

En fait, γ^p est composé de d cycles de longueur $r = k' = \frac{k}{d} = \frac{k}{pgcd(p, k)}$.

Remarque :

(i) On se souvient (exo 4, fiche 2) que la classe de p dans $\mathbb{Z}/k\mathbb{Z}$ engendre le sous-groupe d'ordre $\frac{k}{pgcd(p, k)}$.

(ii) Prenons un exemple : $(x_0 \dots x_{12})^8 = (x_0 x_8 x_4)(x_1 x_9 x_5)(x_2 x_{10} x_6)(x_3 x_{11} x_7)$
est composé de 4 cycles d'ordre $3 = \frac{12}{4} = \frac{12}{pgcd(8, 12)}$.

Exercice 3.

Soit $n \geq 3$ un entier, $\sigma \in S_n$, et γ un r -cycle dans S_n tel que :

$$\gamma = (j_1, j_2, \dots, j_r)$$

Démontrons que $\sigma \circ \gamma \circ \sigma^{-1}$ est le r -cycle $(\sigma(j_1), \sigma(j_2), \dots, \sigma(j_r))$.

Par la permutation $\sigma \circ \gamma \circ \sigma^{-1}$:

$\sigma(j_1)$ est envoyé sur j_1 puis j_2 puis $\sigma(j_2)$

$\sigma(j_2)$ est envoyé sur j_2 puis j_3 puis $\sigma(j_3)$

...

$\sigma(j_r)$ est envoyé sur j_r puis j_1 puis $\sigma(j_1)$

Si $\alpha \neq \sigma(j_i)$, alors $\sigma^{-1}(\alpha) \neq j_i \notin \text{supp}(\gamma)$.

Donc $\sigma \circ \gamma \circ \sigma^{-1}(\alpha) = \sigma \circ \sigma^{-1}(\alpha) = \alpha$.

Autrement dit, $\sigma \circ \gamma \circ \sigma^{-1}$ est exactement le r -cycle $(\sigma(j_1), \sigma(j_2), \dots, \sigma(j_r))$.

Exercice 4.

Démontrons que, pour $n \geq 3$, le groupe $\text{Int}(S_n)$ des automorphismes intérieurs de S_n est isomorphe à S_n .

Soit $f \in \text{Int}(S_n)$. Il existe $\sigma \in S_n$ tel que : $f = f_\sigma : \gamma \mapsto \sigma \circ \gamma \circ \sigma^{-1}$.

On a naturellement une application :

$$\begin{aligned} \varphi : S_n &\longrightarrow \text{Int}(S_n) \\ \sigma &\longmapsto f_\sigma \end{aligned}$$

- si $\sigma, \sigma' \in S_n$,

$$\begin{aligned}
 (f_\sigma \circ f_{\sigma'}) (\gamma) &= f \circ f_{\sigma'} (\gamma) \\
 &= \sigma \left(\sigma' \gamma \sigma'^{-1} \right) \sigma^{-1} \\
 &= \sigma \sigma' \gamma \left(\sigma \sigma' \right)^{-1} \\
 &= f_{\sigma \sigma'} (\gamma)
 \end{aligned}$$

Donc φ est un morphisme, qui de plus vérifie :

$$\varphi(id)(\gamma) = \gamma, \text{ pour tout } \gamma \in S_n.$$

- φ est surjective par définition de $I_n(S_n)$.
- Supposons $f_\sigma = id$, c'est à dire $f_\sigma(\gamma) = \sigma \circ \gamma \circ \sigma^{-1} = \gamma$, pour tout $\gamma \in S_n$.
En particulier, pour $1 \leq r \leq n$ quelconque, si $\gamma = (j_1 \dots j_r)$ est un r -cycle, $\sigma \circ \gamma \circ \sigma^{-1} = (\sigma(j_1) \dots \sigma(j_r))$ est un r -cycle.
En utilisant ce résultat avec $\gamma_1 = (1i)$,
 $\sigma \circ \gamma \circ \sigma^{-1} = \gamma \Leftrightarrow (\sigma(1)\sigma(i)) = (1i)$, donc $\sigma(i) = 1$ ou i .
Mais le même raisonnement avec $\gamma_2 = (2i)$ nous amène à $\sigma(i) = 2$ ou i , et donc nécessairement $\sigma(i) = i$.
Comme notre raisonnement est valable pour tout $i \in \{1, \dots, n\}$, c'est que $\sigma = id$.
Donc φ est injective.
- Finalement, φ est un isomorphisme, et $I_n(S_n) \simeq S_n$, pour $n \geq 3$.

Exercice 5. Systèmes minimaux de générateurs de S_n .

- a.** Les transpositions $(1, i)$ pour $2 \leq i \leq n$ engendrent S_n .
 $(x_1 \dots x_k) = (1x_1)(1x_k)(1x_{k-1}) \dots (1x_2)(1x_1)$, si $x_i \neq 1, \forall i$
 $(1x_2 \dots x_k) = (1x_k)(1x_{k-1}) \dots (1x_2)$ sinon
(ou bien écrire $(x_1 \dots x_k) = (x_1x_2)(x_2x_3) \dots (x_{k-1}x_k)$ et $(x_i x_{i+1}) = (1x_i)(1x_{i+1})(1x_i)$)
De plus, si on oublie la transposition $(1i)$, on ne peut obtenir que des permutations qui laissent fixe i , donc pas S_n tout entier.
Les $(1i)$ forment un système minimal de générateurs.
- b.** Les transpositions $(i, i+1)$ pour $1 \leq i \leq n-1$ engendrent S_n .
 $(1i) = (12)(23) \dots (i-2 \ i-1)(i-1 \ i)(i-2 \ i-1) \dots (23)(12)$
donc les $(1i)$ sont dans le sous-groupe engendré par les $(i \ i+1)$.
Mais d'après la question précédente, $\langle (1i), i \in \{1, \dots, n\} \rangle = S_n$, donc les $(i \ i+1)$ engendrent S_n .
De plus si on oublie la transposition $(i \ i+1)$, l'ensemble $\{1, \dots, n\}$ est laissé (globalement) stable par toute permutation du groupe engendré et ne peut donc être S_n tout entier. Les $(i \ i+1)$ forment un système minimal de générateurs.

- c. Le cycle $(1, 2, \dots, n)$ et la transposition $(1, 2)$ engendrent S_n . On a en effet $(i \ i+1) = \sigma^{i-1} \tau \sigma^{1-i}$.

Explicitons :

L'image de i est $i+1-i=1$ puis 2 puis $2+i-1=i+1$.

L'image de $i+1$ est $i+1+1-i=2$ puis 1 puis $1+i-1=i$.

L'image de j ($j \neq i$ et $i+1$) est $j+1-i$ ($\neq 1$ et 2) puis $j+1-i$ puis $j+1-i+i-1=j$.

σ et τ forment un système minimal (clairement) de générateurs.

- d. Si n est premier, le cycle $(1, 2, \dots, n)$ et n'importe quelle transposition engendrent S_n . En effet, posons $a = j-i$, on a $\sigma^{1-i} \circ (ij) \circ \sigma^{i-1} = (1 \ i+i+1) = (1 \ a+1) = \tau$.

Puis, $\sigma^{ka} \tau \sigma^{-ka} = (ka+1 \ (k+1)a+1) = \tau_k$

et $(1 \ ka+1) = \tau \tau_1 \tau_2 \dots \tau_{k-2} \tau_{k-1} \tau_{k-2} \dots \tau_2 \tau_1 \tau$

et ce pour tout $k \geq 1$ (les entiers sont à comprendre modulo n).

Comme $a \neq 0[n]$ et n est premier,

$\exists k \geq 1$ tel que $ka \equiv 1[n]$ (a est inversible dans $(\mathbb{Z}/2p\mathbb{Z})^\times$)

On a donc montré que (12) appartient au groupe engendré, qui est donc S_n d'après la question précédente.

Pour n premier, $\sigma = (1 \dots n)$ et τ transposition quelconque forment un système minimal (clairement) de générateurs.

Remarque : pour aider à comprendre, explicitons un peu :

$\tau = (1 \ a+1)$ $\tau_1 = (a+1 \ 2a+1)$ $\tau_2 = (2a+1 \ 3a+1)$ $\tau_{k-2} = ((k-2)a+1 \ (k-1)a+1)$ $\tau_{k-1} = ((k-1)a+1 \ la+1)$	$\tau \tau_1 \tau_2 \dots \tau_{k-2} \tau_{k-1} \tau_{k-2} \dots \tau_2 \tau_1 \tau$ envoie : 1 sur $(a+1)$ puis $(2a+1)$ puis ... puis $ka+1$ $(ka+1)$ sur rien puis $((k-1)a+1)$ puis ... puis 1 pour $j \neq ka+1$, où $l \in \{0; 1; \dots; k\}$, j est envoyé sur j
---	--

Groupes alternés

Exercice 6. *Systèmes de générateurs de $\mathcal{A}_n$.*

Soit $n \geq 4$ un entier.

1. On rappelle que les produits d'un nombre pair de transpositions engendrent $\mathcal{A}_n$ (et même $= \mathcal{A}_n$).
2. Soient i, j, k, l distincts dans $\{1, 2, \dots, n\}$ avec $n \geq 4$. Vérifions les relations :

$$(i, j)(j, k) = (i, j, k) \text{ et } (i, j)(k, l) = (i, j, k)(j, k, l)$$

$(ij)(jk)$ envoie :

k sur i

j sur k

i sur j

et fixe le reste

donc $\boxed{(ij)(jk) = (ijk)}$

$(ij)(kl)$ envoie :

i sur j

j sur i

k sur l

l sur k

et $(ijk)(jkl)$ envoie :

i sur j

j sur i

k sur l

l sur k

donc $\boxed{(ij)(kl) = (ijk)(jkl)}$

3. Déduisons en que le groupe alterné $\mathcal{A}_n$ est engendré par :

a. l'ensemble des 3-cycles de S_n :

Les transpositions engendrent S_n , mais $\mathcal{A}_n$ est formé des produits d'un nombre pair de transpositions.

→ Tout produit d'un nombre pair de transpositions est dans $\mathcal{A}_n$ (signature), et est le produit d'un certain nombre de "transpo $\times$ transpo" (car le total est pair).

→ $\mathcal{A}_n$ est engendré par les produits de deux transpositions.

Or, on vient de voir à la question précédente, que tout produit de deux transpositions ($(ij)(jk)$ ou $(ij)(kl)$) s'obtient à partir de 3-cycles.

Donc les 3-cycles engendrent $\mathcal{A}_n$.

b. l'ensemble des 3-cycles de la forme $(1\ i\ j)$ pour $2 \leq i, j \leq n$:

En remarquant que $(ijk) = (1ij)(1jk)$, $\mathcal{A}_n$ est engendré par les 3-cycles de la forme $(1\ i\ j)$ pour $2 \leq i, j \leq n$.

c. l'ensemble des 3-cycles de la forme $(1\ 2\ i)$ pour $3 \leq i \leq n$:

En remarquant que $(1ij) = (12j)(12i)(12i)$, $\mathcal{A}_n$ est engendré par les 3-cycles de la forme $(1\ 2\ i)$ pour $3 \leq i \leq n$.

d. l'ensemble des 3-cycles $(i, i+1, i+2)$ pour $1 \leq i \leq n-2$:

Remarquons que $(124) = (123)(234)$,

et pour $i \geq 3$, $(1\ 2\ i+2) = (i\ i+2\ i+1)(12i)(i\ i+1\ i+2)$, où $(i\ i+2\ i+1)$ est l'inverse de $(i\ i+1\ i+2)$

Autrement dit :

(123)

$(124) = (123)(234)$

pour $i = 3$, $(1\ 2\ i+2) = (1\ 2\ 5) = (354)(123)(345) = (345)^{-1}(123)(345)$
 pour $i = 4$, $(1\ 2\ i+2) = (1\ 2\ 6) = (465)(124)(456) = (456)^{-1}(123)(234)(456)$
 pour $i = 5$, $(1\ 2\ i+2) = (1\ 2\ 7) = (576)(125)(567) = (567)^{-1} \circ$
 voir plus haut $\circ (567)$
 Bref, tous les $(12i)$ s'obtiennent à partir de $(i\ i+1\ i+2)$, et
 $\mathcal{A}_n$ est engendré par les 3-cycles de la forme $(i, i+1, i+2)$ pour $1 \leq i \leq n-2$.

4. Montrons que le troisième système est minimal, mais pas les autres si $n \geq 5$.
- Si on oublie $(12i)$, on n'obtient que des permutations qui laissent i fixe, donc pas $\mathcal{A}_n$ tout entier.
 Le système générateur $(12i)$ est minimal.
 - En revanche on remarque que :

$$\begin{aligned}(234) &= (345)(123)(354)(123) \\ &= (345)(123)^{-1}(345)^{-1}(123)\end{aligned}$$

Le système $(i\ i+1\ i+2)$ n'est pas minimal.

Remarque : Une autre démo. du fait que les $(12i)$, $3 \leq i \leq n$ engendrent $\mathcal{A}_n$.

Pour tout $\sigma \in \mathcal{A}_n$, notons $m(\sigma)$ le plus grand entier m tel que

$$\sigma(m) = k \neq m (\sigma \neq id).$$

Montrons par récurrence sur $m(\sigma)$ que σ s'écrit comme produit de $\sigma_i = (12i)$.

- si $m(\sigma) \leq 2$, comme σ est paire, $\sigma = id$.
- on suppose que $m = m(\sigma) > 2$

On considère $\tau = (12m)(12k)\sigma$ où $k = \sigma(m) > 2$

$\tau = (12m)\sigma$ si $k = 2$ (forcément $k \leq$)

$\tau = (1m2)\sigma$ si $k = 1$

Dans tous les cas, $\tau(m) = m$, et on a $\sigma(\tau) < \sigma(m)$.

L'hypothèse de récurrence s'applique : τ se décompose avec des $(12i) \dots$ et donc σ aussi.

Exercice 7.

Dans S_4 on pose :

$$K = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\} = \{e, a, b, c\}$$

- a. K ne contient que des produits de deux transpositions, donc des permutations paires, donc $K \subset \mathcal{A}_4$.
- b. Ecrivons sa table de multiplication :

$$\begin{array}{l|l|l} (13)(24) \ (12)(34) = (14)(23) & (12)(34) \ (14)(23) = (13)(24) & (13)(24) \ (14)(23) = (12)(34) \\ (12)(34) \circ (13)(24) = (23)(14) & (14)(23) \circ (12)(34) = (13)(24) & (14)(23) \circ (13)(24) = (12)(34) \\ a \times b = b \times a = c & a \times c = c \times a = b & b \times c = c \times b = a \end{array}$$

- c. On reconnaît le seul groupe abélien d'ordre 4 non cyclique : $V_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Il y a trois isomorphismes possibles.

Signature

Exercice 8. *Partition de n et permutations régulières.*

On appelle partition de n une suite $k_1, k_2, \dots, k_n$ d'entiers naturels tels que :

$$\sum_{i=1}^n i k_i = n$$

On rappelle que toute permutation $\sigma \in S_n$ se décompose de façon unique en cycles de supports disjoints, et on lui fait correspondre une partition $k = k(\sigma)$ de la façon suivante : k_i est le nombre de i -cycles qui interviennent dans cette décomposition. En particulier k_1 est le nombre de points fixes de σ .

- a. Montrons que deux permutations sont conjuguées dans S_n si, et seulement si elles ont même partition associée.

- Soient $\sigma, \tau \in S_n$.

On écrit $\sigma = (x_1^1 \dots x_{i_1}^1)(x_1^2 \dots x_{i_2}^2) \dots (x_1^j \dots x_{i_j}^j)$ sa décomposition canonique.

On a vu que $\tau\sigma\tau^{-1} = (\tau(x_1^1) \dots \tau(x_{i_1}^1)) \dots (\tau(x_1^j) \dots \tau(x_{i_j}^j))$

En fait, on a vu l'égalité pour σ un r -cycle, mais remarquons que :

$$\tau\sigma\tau^{-1} = \tau \circ (x_1^1 \dots x_{i_1}^1) \circ \tau^{-1} \circ \tau \circ \dots \circ \tau^{-1} \tau \circ (x_1^j \dots x_{i_j}^j) \circ \tau^{-1}$$

On voit que les longueurs des cycles de σ et $\tau\sigma\tau^{-1}$ sont les mêmes.

Deux permutations conjuguées ont même partition.

- Réciproquement, si σ et σ' ont même partition, écrivons : $\sigma = (x_1^1 \dots x_{i_1}^1) \dots (x_1^j \dots x_{i_j}^j)$

$$\sigma' = (x_1'^1 \dots x_{i_1}'^1) \dots (x_1'^j \dots x_{i_j}'^j)$$

On crée alors τ en associant x_k^i à $x_k'^i$, pour tout i et pour tout k .

On prolonge τ arbitrairement pour obtenir un élément de S_n .

On a alors σ et σ' conjugués par la relation $\sigma' = \tau\sigma\tau^{-1}$.

- b. Montrons que la signature de σ est :

$$\epsilon(\sigma) = (-1)^{n-t} \text{ où } t \text{ est le nombre d'orbites}$$

$$\text{On a } t = \sum_i k_i \text{ d'où } \epsilon(\sigma) = (-1)^{n-\sum_i k_i} = (-1)^{n+\sum_i k_i}.$$

Sinon, la signature d'un i -cycle est $(-1)^{i-1}$,

$$\text{d'où } \epsilon(\sigma) = \prod_i ((-1)^{k_i-1})^{k_i} = (-1)^{\sum_i k_i(i-1)} = (-1)^{n-\sum_i k_i} = (-1)^{n+\sum_i k_i}$$

- c. On appelle *exposant* d'un groupe fini G le plus petit nombre k tel que $g^k = 1$ pour tout élément $g \in G$. Déterminons les exposants de $\mathcal{A}_5$ et S_5 .

On rappelle que :

- l'ordre d'un cycle est égal à sa longueur
- l'ordre d'un produit de cycles à supports disjoints est le *ppcm* des ordres.

Il s'agit donc d'énumérer les partitions de 5 puis de calculer les ordres associés, et enfin leur *ppcm*.

$$5 = 5 \longrightarrow \text{ordre } 5 \text{ (5-cycles)}$$

$$5 = 4 + 1 \longrightarrow \text{ordre } 4 \text{ (4-cycles)}$$

$$5 = 3 + 2 \longrightarrow \text{ordre } 6$$

$$5 = 3 + 1 + 1 \longrightarrow \text{ordre } 3$$

$$5 = 2 + 2 + 1 \longrightarrow \text{ordre } 2$$

$$5 = 2 + 1 + 1 + 1 \longrightarrow \text{ordre } 2$$

$$5 = 1 + 1 + 1 + 1 + 1 \longrightarrow \text{ordre } 1 \text{ (identité)}$$

Enfin, l'exposant de S_5 est $\text{ppcm}(5; 4; 6; 3; 2) = 60$.

Pour $\mathcal{A}_5$, on ne garde que les partitions associées à des permutations paires, c'est à dire les partitions où apparaissent un nombre pair de chiffres pairs.

Soit : $5 = 5$; $5 = 3 + 1 + 1$; $5 = 2 + 2 + 1$; $5 = 1 + 1 + 1 + 1 + 1$,

et l'exposant de $\mathcal{A}_5$ est $\text{ppcm}(5; 3; 2) = 30$.

- d.** Une permutation de S_n est dite *régulière* si sa partition associée a un coefficient non nul et un seul.

Montrons qu'une permutation est régulière si, et seulement si c'est une puissance d'un n -cycle.

Une permutation circulaire est conjuguée à $\sigma = (1 \dots n)$ (et donc les n -cycles ont même partition).

Limitons nous à l'étude du cas des puissances de $(1 \dots n)$.

σ^k envoie x sur $x + k[n]$. Or $\bar{k}$ engendre, dans $\mathbb{Z}/n\mathbb{Z}$ le sous-groupe d'ordre

$$d = \frac{n}{\text{pgcd}(n; k)}.$$

σ^k est composé de $\text{pgcd}(n, k)$ cycles dont les supports sont les classes modulo $\langle \bar{k} \rangle$.

Il y a $\text{pgcd}(n; k)$ supports de taille d . Donc σ^k est régulière.

(il y a $r = \frac{n}{d}$ d -cycles disjoints), on pose $\sigma = (x_1^1 x_1^2 \dots x_1^r x_2^1 \dots x_2^r \dots x_d^1 \dots x_d^r)$ permutation circulaire telle que... $\sigma^r = \tau$...

Exercice 9.

On conserve les notations de l'exercice précédent.

- a.** Montrons qu'une permutation τ de S_n commute avec un n -cycle si, et seulement si τ est une puissance de σ .

- τ puissance de $\sigma \implies \tau$ commute avec σ . OK

- Supposons que τ commute avec σ .

Si $\sigma = (x_1 \dots x_n)$ est un n -cycle, $\sigma\tau\sigma^{-1} = (\tau(x_1) \dots \tau(x_n))$ est aussi un n -cycle.

Dire que σ et τ commutent signifie que $(\tau(x_1) \dots \tau(x_n)) = (x_1 \dots x_n)$.

Les éléments $\tau(x_1), \dots, \tau(x_n)$ sont les éléments $x_1, \dots, x_n$ pris dans le même ordre, mais peut-être non pas à partir de l'élément numéro 1, mais à partir du numéro k .

Cela signifie exactement que $\tau = \sigma^k$.

- b.** Montrons que dans le cas général, le commutant de σ , c'est à dire le sous-groupe de S_n formé des permutations τ telles que $\sigma\tau = \tau\sigma$ a pour cardinal :

$$\prod_i i^{k_i} k_i!$$

Écrivons sur une ligne les cycles de σ , y compris les k_1 qui sont de longueur 1.

Pour que $\tau\sigma\tau^{-1} = \sigma$, il faut que τ permute les supports des cycles de σ .

Comme on ne peut permuter que les cycles de même longueur, il y a $k_i!$ choix possibles pour les cycles de longueur i ($k_i!$ permutations des k_i supports de longueur i).

Une fois la correspondance entre les cycles choisie, il y a i choix possibles pour chaque cycle de longueur i (on envoie un élément sur un des i autres, par τ , et les autres suivent).

Remarque :

En appliquant la formule avec I réduit à l'indice n et $k_n = 1$, on retrouve qu'il y a $n^1 = n$ éléments commutant avec un n -cycle : ses puissances.

Groupes diédraux

Exercice 10.

En notant P_n le polygone régulier à n côtés centré en $O(0;0)$ et $A_k(\cos(\frac{2ik\pi}{n}); \sin(\frac{2ik\pi}{n}))$ pour $0 \leq k \leq n-1$, et en considérant les notations du cours :

- a.** Montrons que toute isométrie $f \in \mathbb{D}_n$ est déterminée par les images de A_1 et A_2 .

Pour $n \geq 3$, soit f une isométrie affine du plan telle que $f(P_n) = P_n$ (globalement).

f transforme A_1 en l'un des n sommets $A_1, \dots, A_n$.

Lorsque $f(A_1)$ est fixé, comme f conserve les distances, il ne reste plus que deux positions pour $f(A_2)$.

Par suite, dès que $f(A_2)$ est fixé, les $f(A_i)$, pour $3 \leq i \leq n$ le sont également de façon unique.

Donc $\boxed{\#\mathbb{D}_n \leq 2n}$.

- b.** Montrons que $\mathbb{D}_n$ possède au moins $2n$ éléments.

- Notons r la rotation d'angle $\frac{2\pi}{n}$
 et r_k la rotation d'angle $\frac{2k\pi}{n}$, $0 \leq k \leq n-1$.
 On a $r_k = r^k$ et $(r_k)^{-1} = r_{n-k} = r^{n-k} = r^{-k}$.
 Pour tout α tel que $1 \leq \alpha \leq n$, on a $r_k(A_\alpha) = A_\beta$
 et $\beta = \alpha + k[n]$, $1 \leq \beta \leq n$.
 $\mathbb{D}_n$ contient donc l'ensemble Γ_n des rotations r_k , $0 \leq k \leq n-1$.
 De plus, pour $0 \leq j, k \leq n-1$, $r_k \circ r_j = r_j \circ r_k = r_l$ où $l = j + k[n]$.
 De plus, $(r_k)^{-1} = r_{n-k}$ et $\Gamma_n \leq \mathbb{D}_n$.
 On a un isomorphisme de groupe :

$$\begin{array}{ccc} \Gamma_n & \longrightarrow & \mathbb{U}_n \\ r_k & \longmapsto & e^{\frac{2ik\pi}{n}} \end{array}$$
 Γ_n est cyclique d'ordre n donc abélien et distingué dans $\mathbb{D}_n$.
 On peut voir Γ_n engendré par r_1 et alors $\Gamma_n = \{id, r, r^2, r^3, \dots, r^{n-1}\}$.
- Soit σ la symétrie par rapport à (Ox) dans le plan.
 $\sigma(A_1) = A_1$ et $\sigma(A_\alpha) = A_{n-\alpha+1}$, donc $\sigma \in \mathbb{D}_n$ et on remarque que $\sigma^2 = id$.
 De plus, $\sigma \notin \Gamma_n$ car $\sigma \neq id$, σ fixe A_1 alors que $r_k(A_1) = A_{1+k}$, ($1 \leq k \leq n-1$).
 Mais alors, $r_k \circ \sigma \in \Gamma_n$ impliquerait $\sigma \in \Gamma_n$ qui est faux. Donc $r_k \circ \sigma \notin \Gamma_n$.
 De plus, les n éléments $r_k \circ \sigma$, ($0 \leq k \leq n-1$) sont distincts.
 En effet, $r^k \circ \sigma = r^j \circ \sigma \implies r^k = r^j \implies k = j$.
 Donc, $\mathbb{D}_n$ contient au moins $2n$ éléments : $\boxed{\#\mathbb{D}_n \geq 2n}$.
Conclusion : $\boxed{\#\mathbb{D}_n = 2n}$.

Exercice 11.

Avec les notations du cours :

a. Décrivons $\mathbb{D}_2$.

Les isométries qui conservent A_1 et A_2 sont : id , σ symétrie par rapport à (Ox) , r_1 la rotation par rapport à O et d'angle π (c'est à dire la symétrie par rapport à O) et la symétrie par rapport à (Oy) qui coïncide avec $r_1 \circ \sigma = \sigma \circ r_1$.
 $\mathbb{D}_2 = \{id, \sigma, r, \sigma \circ r\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

b. Décrivons $\mathbb{D}_3$.

$\mathbb{D}_3$ s'injecte naturellement dans S_3 , mais comme ils ont même cardinal, $\mathbb{D}_3 \simeq S_3$.

Énumérons les éléments de $\mathbb{D}_3$:

- id
- r rotation d'angle $\frac{2\pi}{3}$, r^2 rotation d'angle $\frac{4\pi}{3}$ et inverse de r
- s la symétrie par rapport à (Ox)
- $s \circ r = r^{-1} \circ s = r^2 \circ s$ la symétrie par rapport à (d') hauteur issue de A_2
- $s \circ r^2 = r^{-2} \circ s = r \circ s$ la symétrie par rapport à (d'') hauteur issue de A_3

c. Montrons que, pour $n > 3$, $\mathbb{D}_n$ est un sous-groupe strict H de S_n .

En d'autres termes, $\mathbb{D}_n$ est une "réalisation géométrique" de H .

Pour $\mathbb{D}_n \subset Is(P)$, on a naturellement l'injection (morphisme) canonique :

$$\begin{aligned} \varphi : \mathbb{D}_n &\longrightarrow S_n \\ f &\longmapsto f|_{\{A_1, \dots, A_n\}} \end{aligned}$$

pour $n > 3$, $2n < n!$ donc $H = \text{Im}(\varphi) \neq S_n$.

H est un sous-groupe strict de S_n .

Exercice 12.

Avec les notations du cours :

- a.** Pour $0 \leq k \leq n-1$, $(r^k)^{-1} = r^{n-k}$.
b. Montrons que, dans $\mathbb{D}_n$, on a : $r^k \circ s$ est d'ordre 2, pour tout $0 \leq k \leq n-1$.

- si $\boxed{k=0}$, $r^k \circ s = s \neq id$ donc $r^k \circ s$ est d'ordre 2.
- si $\boxed{k=1}$,
 - si $n=2$ on a vu que $r \circ s$ est la symétrie par rapport à (Oy) donc $(r^1 \circ s)$ est d'ordre 2.
 - si $n \geq 3$, on considère $(r_circs)^2$ et on se souvient que $f \in \mathbb{D}_n$ est déterminée par $f(A_1)$ et $f(A_2)$.
 Or, $(r \circ s)^2(A_1) = A_1$ et $(r \circ s)^2(A_2) = A_2$, d'où $(r \circ s)^2 = id$.
 et donc, $o(r \circ s) = 2$ car $r \circ s \neq id$
- si $\boxed{k > 1}$, comme $s = s^{-1}$, on a $sr^k s = sr^k s^{-1}$
 d'où $sr^k s = (sr^k s^{-1})^k$ avec $sr s^{-1} = r^{-1}$
 d'où $sr^k s = r^{-k}$
 et donc $(r^k s)^2 = e$
 Mais comme $r^k \circ s \neq id$, c'est que $r^k \circ s$ est d'ordre 2.

- c.** On a montré au passage que, pour tout $0 \leq k \leq n-1$, $s \circ r^k = r^{-k} \circ s = r^{n-k} \circ s$.

Remarque :

$\overline{r^k s} = sr^{-k} = (r^k s)^{-1}$, et $r^k s$ est bien son propre inverse.

De même, $sr^k = r^{-k} s = (r^k)^{-1} s^{-1} = (sr^k)^{-1}$, et sr^k est bien son propre inverse.

Exercice 13.

$n > 2$ est un entier.

a. Décrivons la partition de $\mathbb{D}_n$ en classes de conjugaison en distinguant les cas n pair et n impair.

- $\{id\}$ est toujours seule
- si n impair :
 - Il y a $\frac{n-1}{2}$ classes de conjugaisons de rotations
 - Il y a une classe de conjugaison de symétries
- si n est pair :
 - Il y a $\frac{n-2}{2}$ classes de conjugaisons avec 2 rotations, et une classe avec 1 seule rotation.
 - Il y a deux classes de conjugaison de symétries : celles par rapport à une droite passant par deux sommets, et celles par rapport à une droite passant par deux milieux de segment

b. Déterminons le centre de $\mathbb{D}_n$ en distinguant les cas n pair et n impair.

- pour $n = 2$, $\mathbb{D}_2$ est abélien, et $Z(\mathbb{D}_2) = \mathbb{D}_2$.
- pour $n > 2$, $Z(\mathbb{D}_n) = \begin{cases} \{id\} & \text{si } n \text{ est impair} \\ \{id, r^{\frac{n}{2}}\} & \text{si } n \text{ est pair} \end{cases}$

On sait en effet que $\mathbb{D}_n$ contient un unique sous-groupe Γ cyclique d'ordre n .

De plus, pour tout $y \in \mathbb{D}_n \setminus \Gamma$, $o(y) = 2$ et $xyx^{-1} = x^{-1}$, $\forall x \in \Gamma$.

Soit a générateur de Γ . On a en particulier $yay^{-1} = a^{-1}$.

Puisque a est d'ordre $n \geq 3$, $a^{-1} \neq a$ donc y ne commute pas avec a .

Aucun élément de $\mathbb{D}_n \setminus \Gamma$ n'appartient donc au centre de $\mathbb{D}_n$.

Quels éléments de Γ sont dans le centre ?

Comme Γ est commutatif,

$x \in \Gamma$ est dans le centre si x commute avec $y \in \mathbb{D}_n \setminus \Gamma$.

Or, $xyx^{-1} = x^{-1}$ implique que $x \in Z(\mathbb{D}_n) \Leftrightarrow x = x^{-1}$ (c'est à dire $x^2 = e$ c'est à dire x est d'ordre 1 ou 2).

Si n est impair, Γ ne contient pas d'élément d'ordre 2, d'où $Z(\mathbb{D}_n) = \{id\}$.

Si n est pair, Γ est cyclique ne contenant qu'un seul sous-groupe d'ordre $2 \mid n$.

Il n'y a qu'un seul élément x d'ordre 2 qui engendre $\{x, id\} \simeq \mathbb{Z}/2\mathbb{Z}$.

D'où $Z(\mathbb{D}_n)$ est l'unique sous-groupe de Γ à deux éléments.

Exercice 14.

Tout groupe G engendré par deux éléments a et b tels que :

$$o(a) = n \ (n \geq 2), \ o(b) = 2, \ \text{et} \ o(ab) = 2$$

est isomorphe au groupe $\mathbb{D}_n$.

Rappel :

Si $H < G$ et $K < G$.

$HK < G \Leftrightarrow HK = KH$

Lemme

Si $HK < G$, alors $HK = \langle H \cup K \rangle$

Par hypothèse, , $G = \langle a, b \rangle$ donc tout élément de G est produit de puissances entières (positives, négatives ou nulles) de a et b . En fait on a aussi $G = \langle \langle a \rangle \cup \langle b \rangle \rangle$.

Par hypothèse : $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$ et $\langle b \rangle = \{e, b\}$.

On montre que :

- pour $0 \leq k \leq n-1$, les $a^k b$ sont deux à deux distincts. Et comme $b \notin \langle a \rangle$, aucun des $a^k b$ n'est dans $\langle a \rangle$.
- Comme $o(ab) = 2$, on a $ab = (ab)^{-1} = b^{-1}a^{-1} = ba^{-1}$ ($o(b) = 2$).

On a alors :

$$\begin{aligned}(a^k b)^2 &= a^k b a^k b \\ &= a^{k-1} (ab) a^k b \\ &= a^{k-1} b a^{k-1} b \\ &= \dots \\ &= e\end{aligned}$$

donc $a^k b$ est d'ordre 2.

et $ba^k = a^{n-k}b$, $\forall k \in \{0; \dots; n-1\}$ (voir exercice 12)

Ainsi, $\langle a \rangle \langle b \rangle = \langle b \rangle \langle a \rangle$ c'est d'après le lemme le sous groupe engendré par $\langle \rangle \cup \langle b \rangle$.

Ainsi, $G = \langle a \rangle \langle b \rangle = \{e, a, \dots, a^{n-1}, b, ab, \dots, a^{n-1}b\}$.

Le groupe G est donc d'ordre $2n$ et est parfaitement déterminée par :

a, b et les conditions $o(b) = 2$, $o(ab) = 2$ et $o(a) = n$.

Par suite, un morphisme $\varphi : \mathbb{D}_n \longrightarrow G$ tel que $\varphi(r) = a$ et $\varphi(s) = b$ est nécessairement un isomorphisme.

Exercice 15.

Soit $p \geq 2$ est un nombre premier.

Montrons qu'il n'existe, à isomorphisme près que deux groupes d'ordre $2p$:

$$\mathbb{D}_p \text{ et } \mathbb{Z}/2p\mathbb{Z}$$

Lemme (fiche 1, exo 4) :

Un groupe dans lequel tout élément est d'ordre 2 est commutatif.

Ceci étant acquis, soit $g \in G, g \neq e$. L'ordre de g est 2, p ou $2p$ d'après le théorème de Lagrange.

Si tous les éléments de G sont d'ordre 2, G est abélien et si $a, b \neq e \in G, \langle a; b \rangle = \{e, a, b, ab\}$.

Ainsi, $4 \mid 2p$ est exclu car p premier ($p \geq 3$) (on traite le cas $p = 2$ à part).

- (i) s'il existe $a \in G$ d'ordre $2p$, G est cyclique isomorphe à $\mathbb{Z}/2p\mathbb{Z}$
- (ii) s'il existe $a \in G$ d'ordre p et si $H = \{e, a, \dots, a^{p-1}\} \langle a \rangle$, $H \triangleleft G$ car d'indice 2. Donc $\exists b \in G \setminus H$ tel que $G = H \cup bH$.

Montrons que tout élément de $G \setminus H$ est d'ordre 2 (le montrer pour b suffira).

- $b^2 \in H$ car si $b^2 \in bH$, alors $b \in H$ ce qui est exclu.
- supposons $b^2 \neq e$, alors $\exists i \in \{1, \dots, p-1\}$, $b^2 = a^i$ et comme $p = 2q + 1$, on peut écrire $b^{2q} = a^{iq} = b^{p-1}$ ce qui entraîne $b^p = e = ba^{iq}$ ($o(b) = p$ car pas 2 et pas $2p$).

Ainsi $b = a^{-iq} \in H$ ce qui n'est pas vrai.

Donc b est d'ordre 2 et il en va de même de tout élément de $G \setminus H$.

Conclusion :

$G = \{e, a, \dots, a^{p-1}, b, ab, \dots, a^{p-1}b\}$ quelque soit $b \notin H$. On reconnaît $\mathbb{D}_p$.

Exercice 16. *Groupe diédral infini.*

Soit $\mathbb{R}$ considéré comme espace affine euclidien de dimension 1.

À tout $n \in \mathbb{Z}$, on associe la translation $\tau_n : \mathbb{R} \longrightarrow \mathbb{R}$ telle que $\tau_n(x) = x + n$

a. Vérifier que pour tout $n \in \mathbb{Z}$, on a $\tau_1^n = \tau_n$.

b. On pose $S_{\mathbb{R}}(\mathbb{Z}) = \{\varphi \in Is(1) ; \varphi(\mathbb{Z}) = \mathbb{Z}\}$
et σ_0 l'isométrie de $\mathbb{R}$ telle que $\sigma_0(x) = -x$.

Prouver que $S_{\mathbb{R}}(\mathbb{Z})$ est formé par l'ensemble des τ_1^n et des $\tau_1^n \circ \sigma_0$, pour $n \in \mathbb{Z}$.

En déduire que $S_{\mathbb{R}}(\mathbb{Z})$ est un sous-groupe de $Is(1)$.

Le groupe $S_{\mathbb{R}}(\mathbb{Z})$ est appelé *groupe diédral infini* et on le note généralement $\mathbb{D}_{\infty}$.

Exercice 17.

Soit $n \geq 3$ un entier. On pose $\alpha = \exp(\frac{2i\pi}{n}) \in \mathbb{C}$ Démontrons que le groupe multiplicatif engendré par les matrices complexes :

$$X = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \text{ et } Y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

est isomorphe au groupe diédral $\mathbb{D}_n$.

$$X^n = Id, \text{ et } X^k = \begin{pmatrix} \exp(\frac{2ik\pi}{n}) & 0 \\ 0 & \exp(\frac{-2ik\pi}{n}) \end{pmatrix} \neq Id \text{ pour } 1 \leq k \leq n-1.$$

Donc X est d'ordre n dans $M_n(\mathbb{C})$.

$Y^2 = Id$, Y est d'ordre 2 dans $M_n(\mathbb{C})$.

De plus $XY = \begin{pmatrix} 0 & \alpha \\ \alpha^{-1} & 0 \end{pmatrix}$ est tel que $(XY)^2 = Id$, donc XY est d'ordre 2.

Le groupe $G = \langle X; Y \rangle$ vérifie $o(X) = n$; $o(Y) = 2$; $o(XY) = 2$, donc d'après l'exercice 14, $G \simeq \mathbb{D}_n$.