Corrigé du DM n°25

Problème

Partie I. Préliminaires

1 Puisque $S_2 = \{\mathrm{Id}\,; (1\,2)\}$ et que $(1\,2)$ est de signature -1 (c'est une transposition),

$$\boxed{A_2 = \{\mathrm{Id}\,\}}$$

Parmi les éléments de S_3 donnés en classe, seuls Id et les deux 3-cycles sont de signature 1 (rappelons qu'un p-cycle est de signature $(-1)^{p-1}$ et qu'une transposition est de transposition -1). Dès lors,

$$\boxed{A_3 = \{\mathrm{Id}\,; (1\,2\,3); (1\,3\,2)\}}$$

2 Un noyau est un sous-groupe donc

$$\boxed{A_n \text{ est un sous-groupe de } S_n.}$$

> Comme pour S_n, certains puristes utilisent le gothique et notent cet ensemble $\mathfrak{A}_n$.

3 Quand on demande de montrer que φ est bien définie, on demande de prouver que φ est bien à valeurs dans $S_n \backslash A_n$. Or, pour toute permutation $\sigma \in A_n$, $\varepsilon(\sigma) = 1$ et puisque ε est un morphisme,

$$\begin{aligned}\varepsilon(\varphi(\sigma)) &= \varepsilon((1\,2)) \times \varepsilon(\sigma)\\ &= -1\end{aligned}$$

et donc on a bien $\varphi(\sigma) \notin A_n$. Montrons à présent que φ est bijective. Soient σ_1 et σ_2 deux éléments de A_n tels que $\varphi(\sigma_1) = \varphi(\sigma_2)$. Alors

$$(1\,2)\sigma_1 = (1\,2)\sigma_2$$

En composant à gauche par $(1\,2)^{-1} = (1\,2)$, on obtient que $\sigma_1 = \sigma_2$ donc φ est injective.

> Attention, on ne peut pas dire que φ est injective entre deux ensembles de même cardinal fini puisqu'on cherche précisément le cardinal de A_n.

Montrons enfin que φ est surjective. Soit $s \in S_n \backslash A_n$ et soit $\sigma = (1\,2) \circ s$. De même que ci-dessus, ε étant un morphisme, $\varepsilon(\sigma) = -\varepsilon(s) = 1$ puisque $\varepsilon(s) = -1$ (car $s \notin A_n$). Enfin, puisque $(1\,2)^2 = \mathrm{Id}$, $\varphi(\sigma) = s$: φ est surjective.

$$\boxed{\varphi \text{ est bien définie et bijective.}}$$

4 Deux ensembles finis en bijection ont le même cardinal donc $\mathrm{Card}\,(A_n) = \mathrm{Card}\,(S_n \backslash A_n)$. Or, S_n est l'union disjointe de ces deux ensembles donc

$$\begin{aligned}\mathrm{Card}\,(S_n) &= \mathrm{Card}\,(A_n) + \mathrm{Card}\,(S_n \backslash A_n)\\ &= 2\,\mathrm{Card}\,(A_n)\end{aligned}$$

En conclusion

$$\boxed{\mathrm{Card}\,(A_n) = \frac{\mathrm{Card}\,(S_n)}{2} = \frac{n!}{2}}$$

> On aurait aussi pu utiliser l'exercice 32 du chapitre 18 : si G est un groupe fini, H un groupe (pas forcément fini) et si $f : G \to H$ est un morphisme de groupes, alors $\mathrm{Card}\,(G) = \mathrm{Card}\,(\mathrm{Ker}\,(f)) \times \mathrm{Card}\,(\mathrm{Im}\,(f))$. Or, la signature est surjective dans $\{\pm 1\}$ donc son image est de cardinal 2, donc on obtient le même résultat en appliquant l'exercice 32 du chapitre 18 à la signature.

5 On a :

$$\boxed{\mathrm{A}_4 = \{\mathrm{Id}\,;(1\,2)(3\,4);(1\,3)(2\,4);(1\,4)(2\,3);(1\,2\,3);(1\,3\,2);(1\,2\,4);(1\,4\,2);(1\,3\,4);(1\,4\,3);(2\,3\,4);(2\,4\,3)\}}$$

Il suffit de voir que les cycles $(1\,2\,3)$ et $(1\,2\,4)$ ne commutent pas : en effet,

$$(1\,2\,3)(1\,2\,4) = (1\,3)(2\,4) \qquad \text{et} \qquad (1\,2\,4)(1\,2\,3) = (1\,4)(3\,2)$$

et donc $\boxed{\mathrm{A}_4 \text{ n'est pas abélien.}}$

Partie II. A_n et les 3-cycles

1 D'après le cours, un 3-cycle est de signature $(-1)^2 = 1$ donc

$$\boxed{\text{Les 3-cycles sont bien des éléments de } \mathrm{A}_n.}$$

A_n étant un groupe, il est stable par produit (rappelons que, quand on parle de produit, on parle en fait de composition de bijections).

$$\boxed{\text{Un produit de 3-cycles est un élément de } \mathrm{A}_n.}$$

2 Toute permutation de S_n peut s'écrire comme produit de transpositions, et on sait que la signature d'une transposition est égale à (-1) à la puissance le nombre de transpositions dans cette écriture (le nombre de transpositions peut varier, pas sa parité). Le résultat en découle :

$$\boxed{\text{Une permutation est un élément de } \mathrm{A}_n \text{ ssi elle peut s'écrire comme produit d'un nombre pair de transpositions.}}$$

3 Le cardinal de cette intersection peut valoir 0, 1 ou 2.

- Si ce cardinal vaut 2, c'est que les deux ensembles sont égaux donc $(a\,b) = (c\,d)$ donc $(a\,b) \circ (c\,d) = (a\,b) \circ (a\,b) = \mathrm{Id}$ donc on peut dire que c'est un produit vide de 3-cycles ou simplement $(1\,2\,3)^3$.
- Si ce cardinal vaut 1, alors ces ensembles ont un seul élément en commun : sans perte de généralité, supposons que $b = c$ donc a, b et d sont deux à deux distincts. On en déduit que $(a\,b) \circ (c\,d) = (a\,b) \circ (b\,d) = (a\,b\,d)$ (on trouve facilement que a est envoyé sur b qui est envoyé sur d qui est envoyé sur a).
- Supposons enfin que ce cardinal soit nul, alors les quatre entiers a, b, c, d sont deux à deux distincts. La permutation $(a\,b)\circ(c\,d)$ n'est pas un 3-cycle, pas la peine de rêver, mais en tâtonnant un peu, on trouve que $(a\,b)\circ(c\,d) = (a\,c\,d)\circ(a\,b\,d)$.

Dans tous les cas $\boxed{(a\,b) \circ (c\,d) \text{ est un produit de 3-cycle.}}$

4 Il suffit de combiner les résultats des trois premières questions : d'une part, tout produit de 3-cycles est un élément de A_n, et d'autre part, tout élément de A_n s'écrit comme produit d'un nombre pair de transpositions, donc comme produit de permutations du type $(a\,b) \circ (c\,d)$ qui sont, comme on l'a vu, des produits de 3-cycles.

$$\boxed{\mathrm{A}_n \text{ est exactement l'ensemble des permutations qui peuvent s'écrire comme produit de 3-cycles.}}$$

Partie III. A_n est le seul sous-groupe de S_n d'indice 2

1 Tout d'abord, H étant un sous-groupe de S_n, H est stable par produit (la composition) donc $x^2 \in \mathrm{H}$. Supposons à présent que $x \notin \mathrm{H}$. Alors S_n est l'union disjointe de H et de $x\mathrm{H}$. En effet :

- H et $x\mathrm{H}$ sont disjoints. Supposons en effet qu'il existe $h \in \mathrm{H} \cap x\mathrm{H}$. Puisque $h \in x\mathrm{H}$, alors il existe h_1 tel que $h = xh_1$ et donc $x = hh_1{}^{-1} \in \mathrm{H}$ car H est un sous-groupe de S_n ce qui est absurde car $x \notin \mathrm{H}$.
- H et $x\mathrm{H}$ ont même cardinal. En effet, l'application

$$f : \begin{cases} \mathrm{H} \longrightarrow x\mathrm{H} \\ h \longmapsto xh \end{cases}$$

est surjective par définition de $x\mathrm{H}$, et également injective : s'il existe h_1 et h_2 tels que $xh_1 = xh_2$ alors $h_1 = h_2$ car tout élément d'un groupe est régulier (ou, ce qui revient au même, en multipliant à gauche par x^{-1}).

On en déduit que H et xH ont même cardinal, $n!/2$, et puisqu'ils sont disjoints,

$$\text{Card}\,(\text{H} \cup x\text{H}) = \text{Card}\,(\text{H}) + \text{Card}\,(x\text{H}) = n! = \text{Card}\,(\text{S}_n)$$

d'où le résultat annoncé. Il en découle que $x^2 \in \text{H}$ ou $x^2 \in x\text{H}$. Si $x^2 \in x\text{H}$ alors il existe $h \in \text{H}$ tel que $x^2 = xh$ donc (comme précédemment, tout élément est régulier) $x = h \in \text{H}$ ce qui est absurde : $x^2 \in \text{H}$.

H contient tous les carrés.

2 Il suffit de voir que, si a, b, c sont deux à deux distincts, $(a\,b\,c) = (a\,c\,b) \circ (a\,c\,b)$.

Un 3-cycle est un carré.

3 D'après les deux questions précédentes, les 3-cycles sont dans H et H est un sous-groupe de S_n donc est stable par produit si bien que H contient tous les produits de 3-cycles, donc contient A_n d'après la question 4 de la partie précédente. Or, H et A_n ont même cardinal donc sont égaux.

A_n est le seul sous-groupe de S_n d'indice 2.

Partie IV. Simplicité de A_n pour $n \geqslant 5$

1 Soit $x \in \text{G}$. Alors

$$xex^{-1} = e$$

ce qui signifie que $\{e\}$ est distingué dans G. Enfin, le fait que G soit distingué est immédiat : pour tous $x \in \text{G}$ et $h \in \text{G}, xhx^{-1} \in \text{G}$.

$\{e\}$ et G sont toujours distingués dans G.

> Un groupe est dit « simple » s'il n'admet pas d'autre sous-groupe distingué. Les groupes distingués sont très utiles car on peut « quotienter » » par un sous-groupe distingué et munir l'ensemble quotient (cf. partie hors programme du chapitre 16) d'une structure de groupe. En clair, les groupes distingués permettent de « dévisser » un groupe à l'aide de groupes plus petits (voir par exemple l'exercice sur le produit semi-direct dans le chapitre 18). Un groupe simple est donc un groupe qu'on ne peut pas dévisser en sous-groupes plus petits.

2 L'ensemble $\text{C} = \{$ nombre de points fixes de $\sigma \,|\, \sigma \in \text{H}\backslash\{\text{Id}\}\}$ est une partie non vide (car $\text{H} \neq \{\text{Id}\}$) finie donc majorée de $\mathbb{N}$ donc admet un plus grand élément : en d'autres termes, parmi les éléments de H distincts de Id, il existe une permutation (pas forcément unique) σ ayant un nombre de points fixes maximal.

Une telle permutation σ existe bien.

$\sigma \neq \text{Id}$ donc son support a au moins deux éléments : en effet, il existe i tel que $\sigma(i) \neq i$ car $\sigma \neq \text{Id}$ et σ est injective donc $\sigma(\sigma(i)) \neq \sigma(i)$ donc $\sigma(i)$ est un autre élément du support de σ. Enfin, si ce sont les deux seuls, alors σ est une transposition donc sa signature vaut -1, ce qui est absurde car on travaille dans $\text{H} \subset \text{A}_n$.

Le support de σ a au moins 3 éléments.

3.(a) Puisque ce sont des éléments de A_n, ils s'écrivent comme produit d'un nombre pair de transpositions d'après la partie II (ou on dit simplement que s'il n'y a qu'une transposition, alors sa signature vaut -1, ce qui est absurde).

σ est le produit d'au moins deux transpositions.

3.(b) Par hypothèse, $n \geqslant 5$.

Il existe $k \neq i, j, r, s$.

3.(c) $\sigma \in \text{H}$ et H est un sous-groupe de G donc $\sigma^{-1} \in \text{H}$. Or, H est de plus distingué dans G donc $\tau\sigma^{-1}\tau^{-1} \in \text{H}$. Enfin, $\sigma \in \text{H}$ donc

$$\sigma' = \sigma \times \tau\sigma^{-1}\tau^{-1} \in \text{H}$$

3.(d) Rappelons que $\sigma^{-1}(x)$ est l'unique antécédent de x par σ, c'est-à-dire x puisque x est un point fixe de σ, et donc $\sigma(x) = x$.

Si x est un point fixe de σ, alors x est un point fixe de σ^{-1}.

3.(e) On sait que $\tau^{-1}(k) = s$ (précisons que $\tau^{-1} = \tau^2 = (r\,k\,s)$), $\sigma^{-1}(s) = r$ puis $\tau(r) = s$ et enfin $\sigma(s) = r$ donc $\sigma'(k) = r$: on a prouvé que $\sigma' \neq \mathrm{Id}$ (et en particulier k n'est pas un point fixe de σ').

$\sigma'(k) = r$: en particulier, $\sigma' \neq \mathrm{Id}$ et k n'est pas un point fixe de σ'.

3.(f) Soit f un point fixe de σ. Alors $f \neq i, j, r, s$ car ceux-ci sont dans le support de σ. On ne sait pas si k est un point fixe de σ ou non, donc on supposera également $f \neq k$. Dès lors, $\tau(f) = f$ et puisque f est fixe par σ, il est aussi fixe par σ^{-1} d'après la question précédente, et donc$\sigma^{-1} \circ \tau^{-1}(f) = f$, puis vient le tour de τ qui laisse f stable, puis σ qui laisse stable f. On en déduit que tous les points fixes de σ (sauf peut-être k si c'est un point fixe) sont aussi points fixes de f.

Calculons à présent $\sigma'(i)$ et $\sigma'(j)$. Puisque i est distinct de k, r, s, i est fixe par τ^{-1}. Par conséquent, $\sigma^{-1}\circ\tau^{-1}(i) = \sigma^{-1}(i) = j$ (puisque i est dans la transposition $(i\,j)$) et j est laissé stable par τ donc on arrive à σ et $\sigma(j) = i$ si bien que $\sigma'(i) = i$: i est point fixe de σ', et on prouve de même que j est point fixe de σ'.

En conclusion, σ' a au moins deux points fixes qui ne sont pas des points fixes de σ, et tous les points fixes de σ (sauf peut-être un : k) sont points fixes de σ' donc σ' a au moins un point de fixe de plus que σ.

σ' a strictement plus de points fixes que σ.

Cependant $\sigma' \neq \mathrm{Id}$ et $\sigma' \in \mathrm{H}$ d'après la question 3.(c) ce qui contredit la définition de σ (une permutation distincte de Id ayant un nombre maximal de points fixes). On en déduit que l'hypothèse selon laquelle tous les cycles de σ sont de longueur 2 est absurde.

Un des cycles de σ a une longueur supérieure ou égale à 3.

4.(a) $\sigma(j) = k$, $j \neq k$ et σ est injective.

$\sigma(k) \neq k$

4.(b) Par hypothèse, σ n'est pas un 3-cycle donc son support a au moins 4 éléments, donc est un soit un 4-cycle soit le produit de deux transpositions à supports disjoints. Le premier cas est exclu car un 4-cycle a une signature égale à -1 et le deuxième cas est exclu d'après la question 3.

Le support de σ a au moins 5 éléments.

4.(c) Notons $\tau = (r\,s\,k)$ et posons de même $\sigma' = \sigma\tau\sigma^{-1}\tau^{-1}$. De même que précédemment, $\sigma' \in \mathrm{H}$. Si f est un point fixe de σ, alors $f \neq i, j, k, r, s$ donc f est point fixe de σ et τ donc est aussi fixe par σ'. On montre de même que $\sigma'(k) = \sigma(k) \neq k$ (inconnu mais on sait que ce n'est pas k d'après la question 4.(a)) donc σ' n'est pas l'identité. Enfin, de même, i est point fixe de σ' (ainsi que j mais ici un seul suffit) et on conclut à une absurdité de la même façon.

5.(a) D'après l'exercice 13, des cycles de même longueur sont conjugués.

Il existe $\rho \in \mathrm{S}_n$ tel que $\rho\sigma\rho^{-1} = \sigma'$.

5.(b) Immédiat puisque $n \geqslant 5$.

5.(c) Toujours d'après l'exercice 13, $\rho\sigma\rho^{-1} = (\rho(i)\,\rho(j)\,\rho(k)) = (i'\,j'\,k')$ et si on pose $\tau = \rho\circ(r\,s)$, alors $\tau\sigma\tau^{-1} = (\tau(i)\,\tau(j)\,\tau(k))$. Or, i, j, k sont distincts de r et s donc i, j, k sont laissés fixes par $(r\,s)$ si bien que $\tau(i) = \rho(i)$ et idem pour les autres. On en déduit que

$$\rho\sigma\rho^{-1} = \tau\sigma\tau^{-1} = (i'\,j'\,k')$$

Or, parmi ρ et τ, on passe de l'un à l'autre en multipliant par une transposition donc la signature est multipliée par -1 : au moins un des deux appartient à A_n, ce qui permet de conclure.

Il existe $s \in \mathrm{A}_n$ tel que $\sigma' = s \circ \sigma \circ s^{-1}$.

5.(d) H étant distingué, $\sigma' \in \mathrm{H}$, et σ' étant quelconque, tous les 3-cycles sont dans H. H étant un groupe, il est stable par produit, donc contient tous les produits de 3-cycles, donc contient A_n, mais H est un sous-groupe de A_n donc $\mathrm{H} = \mathrm{A}_n$.

A_n est simple : ses seuls sous-groupes distingués sont $\{\mathrm{Id}\}$ et lui-même.

6.(a) On a évidemment $\mathrm{H} \cap \mathrm{A}_n$ qui est un sous-groupe de A_n (sous-groupe de S_n car intersection de sous-groupes de S_n et inclus dans A_n). Soit $h \in \mathrm{H} \cap \mathrm{A}_n$, soit $x \in \mathrm{A}_n$. Alors, en particulier, $x \in \mathrm{S}_n$ et puisque H est distingué dans S_n, alors $xhx^{-1} \in \mathrm{H}$. De plus, A_n est un groupe donc stable par produit et par inverse donc $xhx^{-1} \in \mathrm{A}_n$ si bien que $xhx^{-1} \in \mathrm{H} \cap \mathrm{A}_n$:

$\mathrm{H} \cap \mathrm{A}_n$ est un sous-groupe distingué de A_n.

6.(b) Puisque $\mathrm{H} \cap \mathrm{A}_n = \mathrm{A}_n$, alors $\mathrm{A}_n \subset \mathrm{H}$ donc A_n est un sous-groupe de H. D'après le théorème de Lagrange, le cardinal de A_n divise le cardinal de H. Si $\mathrm{Card}\,(\mathrm{A}_n) = \mathrm{Card}\,(\mathrm{H})$, puisque $\mathrm{A}_n \subset \mathrm{H}$, alors $\mathrm{A}_n = \mathrm{H}$. Sinon, $\mathrm{Card}\,(\mathrm{H}) \geqslant 2\,\mathrm{Card}\,(\mathrm{A}_n) = \mathrm{Card}\,(\mathrm{S}_n)$ mais H est un sous-groupe de S_n donc $\mathrm{H} = \mathrm{S}_n$.

Si $\mathrm{H} \cap \mathrm{A}_n = \mathrm{A}_n$ alors $\mathrm{H} = \mathrm{A}_n$ ou S_n.

6.(c) On montre comme en algèbre linéaire que $\mathrm{Ker}\,(\varepsilon_{|\mathrm{H}}) = \mathrm{H} \cap \mathrm{A}_n = \{\mathrm{Id}\}$ donc $\varepsilon_{|\mathrm{H}}$ est injective, donc ε est une bijection de H sur son image, qui est incluse dans $\{\pm 1\}$. On en déduit que H admet un ou deux éléments. Si H admet un élément, alors $\mathrm{H} = \{\mathrm{Id}\}$, et si H admet deux éléments, alors l'autre élément σ vérifie : $\forall s \in \mathrm{S}_n, s \circ \sigma \circ s^{-1} \in \mathrm{H}$ car H est distingué, ce qui est impossible car on obtient de cette façon toutes les transpositions (car elles sont toutes conjuguées d'après la question 3 de l'exercice 12). Finalement :

Si $\mathrm{H} \cap \mathrm{A}_n = \{\mathrm{Id}\}$ alors $\mathrm{H} = \{\mathrm{Id}\}$.