École Normale Supérieure, Année 2021-2022

1e année, Algèbre 1

TD n° 5 : Notes et corrections

Exercice 1.

Montrer que le centre de S_n est trivial pour $n \geqslant 3$. On pourra commencer par montrer que si un élément est dans le centre, alors il fixe les paires de points.

Correction exercice 1

Soit $\sigma \in \mathrm{Z}(\mathrm{S}_n)$, montrons que $\sigma = \mathrm{id}$. Soit $i, j \in \mathbb{N}$ des entiers tels que $1 \leqslant i < j \leqslant n$, alors $\sigma(i\,j)\sigma^{-1} = (\sigma(i)\ \sigma(j))$ mais comme σ est central $(\sigma(i)\ \sigma(j)) = (i\ j)$. Ainsi, $\{\sigma(i), \sigma(j)\} = \{i, j\}$ et donc en l'appliquant pour $j_1, j_2 \neq i$ tels que $1 \leqslant j_1 \neq j_2 \leqslant n$ on obtient que $\sigma(i) = i$, c'est-à-dire que σ agit trivialement sur $\{1, 2, \ldots, n\}$, donc $\sigma = \mathrm{id}$ l'identité.

Exercice 2.

1. Montrer qu'il existe un unique morphisme non trivial $\mathrm{S}_n \to \mathbb{Z}/2\mathbb{Z}$.
2. Soit $H \subset \mathrm{S}_n$ un sous-groupe d'indice 2. Montrer $H = \mathrm{A}_n$.
3. Montrer que tout morphisme $\mathrm{A}_n \to \mathbb{Z}/2\mathbb{Z}$ est trivial.
4. Déduire de la question précédente que A_4 ne possède pas de sous-groupe d'ordre 6.

Correction exercice 2

1. Soit $f\colon \mathrm{S}_n \to \mathbb{Z}/2\mathbb{Z}$ un morphisme. On veut raisonner sur l'image des transpositions. Comme $\mathbb{Z}/2\mathbb{Z}$ est abélien, f est constant sur les classes de conjugaison, mais alors l'ensemble des transpositions est d'image 1 ou 0. Les transpositions engendrent S_n donc les deux alternatives précédentes déterminent le morphisme. Si l'image des transpositions est 0, le morphisme est trivial. Ainsi, on a un unique morphisme non trivial qui est nécessairement la signature : c'est bien un morphisme $\mathrm{S}_n \to \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$ non trivial.
2. Comme $H \subset \mathrm{S}_n$ est d'indice 2, il est distingué et on peut former le quotient S_n/H qui est un groupe d'ordre 2 donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Le morphisme quotient $\mathrm{S}_n \to \mathrm{S}_n/H \cong \mathbb{Z}/2\mathbb{Z}$ n'est pas trivial puisque H n'est pas d'indice 1 et la première question nous assure qu'un tel morphisme est la signature. On en déduit que le noyau du morphisme quotient est A_n donc $H = \mathrm{A}_n$.
3. Soit $f\colon \mathrm{A}_n \to \mathbb{Z}/2\mathbb{Z}$ un morphisme. Rappelons que A_n est engendré par ses 3-cycles. Un 3-cycle est d'ordre 3 donc son image par f est soit d'ordre 3, soit l'élément neutre. Comme $\mathbb{Z}/2\mathbb{Z}$ ne contient pas d'élément d'ordre 3, l'image par f d'un 3-cycle est le neutre donc f est trivial.
4. Un sous-groupe de A_4 est d'ordre 6 si, et seulement s'il est d'indice 2. Comme pour la deuxième question de l'exercice, la donnée d'un sous-groupe d'indice 2 est équivalente à la donnée d'un morphisme non trivial $\mathrm{A}_4 \to \mathbb{Z}/2\mathbb{Z}$, donc il n'existe pas de sous-groupe d'ordre 6 dans A_4.

Exercice 3. Générateurs de S_n

Soit $n \geqslant 2$ un entier.

1. Montrer que les transpositions $\tau_i \coloneqq (i\ i+1)$ avec $1 \leqslant i \leqslant n-1$ engendrent S_n.
2. Montrer que la transposition $\tau_1 = (1\,2)$ et le n-cycle $c = (1\,2\,\ldots\,n)$ engendrent S_n.

Correction exercice 3

1. On raisonne par récurrence sur n : le cas $n = 2$ est clair. Soit $H_n \coloneqq \langle \tau_1, \tau_2, \dots, \tau_{n-1} \rangle \subset \mathrm{S}_n$, supposons $H_{n-1} = \mathrm{S}_{n-1}$. Soit $\sigma \in \mathrm{S}_n$, montrons que $\sigma \in H_n$. Posons $i \coloneqq \sigma(n)$, on définit la permutation $\sigma' \in \mathrm{S}_n$ par

$$\sigma' \coloneqq \begin{cases} \tau_{n-1}\tau_{n-2}\dots\tau_i\sigma & \text{si } i \neq n \\ \sigma & \text{sinon, } i = n \end{cases}$$

et on remarque que dans les deux cas, $\sigma'(n) = n$. Alors, σ' définit une permutation de $\{1, 2, \dots, n-1\}$, c'est-à-dire que $\sigma' \in \mathrm{S}_{n-1}$ par l'hypothèse de récurrence. On peut alors conclure puisque $\sigma' \in H_{n-1}$ et donc $\sigma \in H_n H_{n-1} \subset H_n$.

2. La formule de conjugaison donne $c\tau_i c^{-1} = \tau_{i+1}$, pour i entier tel que $1 \leqslant i \leqslant n-2$ et $c\tau_{n-1}c^{-1} = \tau_1$. Ainsi, toujours, pour i entier tel que $1 \leqslant i \leqslant n-1$, on a $c^{i-1}\tau_1 c^{1-i} = \tau_i$. On obtient $\langle \tau_1, \tau_2, \dots, \tau_{n-1} \rangle \subset \langle c, \tau_1 \rangle$ et donc $\langle \tau_1, c \rangle = \mathrm{S}_n$ d'après la première question.

Exercice 4. Simplcité de A_5

On s'intéresse aux classes de conjugaison dans A_5. On commence par faire agir S_5 par conjugaison sur lui même.

1. Justifier que A_5 est stable sous cette action et identifier les orbites. Donner le cardinal de chaque orbite.
2. Une des orbites ne peut pas être une classe de conjugaison[1] de A_5, laquelle ?
3. Montrer que les autres orbites sont bien des classes de conjugaison dans A_5.
4. Montrer que l'orbite de la question 2 est l'union de deux classes de conjugaison dans A_5.
5. Déduire de la description des classes de conjugaison que A_5 est un groupe *simple*.

Correction exercice 4

1. L'action par conjugaison de S_n sur S_n préserve la signature et donc, stabilise A_5. Rappelons les classes de conjugaison de S_5, déterminés par leurs types. Ces types sont les partitions de 5, soit $5^1 \sim 5,\ 1^1 4^1 \sim 1+4,\ 2^1 3^1 \sim 2+3,\ 1^2 3^1 \sim 1+1+3,\ 1^1 2^2 \sim 1+2+2,\ 1^3 2^1 \sim 1+1+1+2,\ 1^5 \sim 1+1+1+1+1$. Seulement les classes associées aux partitions $5^1,\ 1^2 3^1,\ 1^1 2^2,\ 1^5$ ont une intersection non triviale avec A_n. On calcul leurs cardinals
   - 1^5 correspond à l'élément neutre : **1** élément.
   - $1^1 2^2$ correspond aux doubles transpositions. Elles ont chacunes un unique point fixe et pour chaque $i \in \{1, 2, 3, 4, 5\}$ on compte 3 doubles transpositions qui fixent i : $5 \times 3 = \mathbf{15}$ éléments, les stabilisateurs dans S_n sont d'ordre 8.
   - $1^2 3^1$ correspond aux 3-cycles. Chaque 3-cycle à exactement 2 point fixe et pour tout sous-ensemble $\{i, j\} \subset \{1, 2, 3, 4, 5\}$ on compte 2 3-cycles qui fixent i et j : $\binom{5}{2} \times 2 = \mathbf{20}$ éléments, les stabilisateurs dans S_n sont d'ordre 6.
   - 5^1 correspond aux 5-cycles. Par ce qui précède, on devrait trouver 24 éléments. Un 5-cycle est déterminé par les images, distinctes, de 4 éléments distincts de $\{1, 2, 3, 4, 5\}$: $4! = \mathbf{24}$ éléments , les stabilisateurs dans S_n sont d'ordre 5.
2. On a obtenu que les 5-cycles forment une orbite de cardinal 24 sous l'action de S_5. Or $|\mathrm{A}_5| = 60$ qui n'est pas divisible par 24. Ainsi, cette partie n'est pas une orbite sous S_n.ne peut pas être une classe de conjugaison de A_5.
3. Rappelons que A_5 agit 2-transitivement sur $\{1, 2, 3, 4, 5\}$. Déterminons dans chaque point précédent les orbites sous la conjugaison par A_5.
   - Pour 1^5 la classe de conjugaison n'est que le neutre $\{e\}$.
   - Dans $1^1 2^2$ on a une unique classe de conjugaison sous A_5. En effet, par la 2-transitivité, tout élément est conjugué à un élément de la forme $(1\ 2)(a_1\ a_2)$ puis, comme les permutations paires de $\{3, 4, 5\}$ s'identifient à $\mathrm{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$, il suffit de conjuguer suffisamment de fois par $(3\,4\,5)$ pour obtenir que tout élément est conjugué à $(1\ 2)(3\ 4)$.
   - Dans $1^2 3^1$, la 2-transitivité permet d'appliquer la conjugaison par A_5 pour se ramener aux 3 cycles qui fixent 4 et 5. Il suffit donc d'obtenir que $(1\,2\,3)$ et $(1\,3\,2)$ sont conjugués dans A_5 et il le sont bien par $(2\,3)(4\,5)$. Rappelons que plus généralement, les 3-cycles sont conjugués dans A_n.

[1] *Indication* : Pour une raison de cardinal

4. D'après ce qu'on a obtenu dans la question 2, l'ensemble des 5-cycles, qui est stable par conjugaison, est l'union d'au moins deux classes de conjugaison. Il suffit donc de montrer que le stabilisateur d'un 5-cycle est engendré par celui-ci, puisqu'alors sa classe de conjugaison dans A_5 est de cardinal $12 = \frac{24}{2}$. Soit c un 5-cycle, comme le stabilisateur de c dans S_5 est d'ordre $5 = \frac{120}{24}$ et qu'il contient c , le stabilisateur de c est $\langle c\rangle \cong \mathbb{Z}/5\mathbb{Z}$. Ainsi, pour A_5, le stabilisateur de c est contenu dans $\langle c\rangle$ mais comme $c \in \mathrm{A}_n$ on obtient que ce stabilisateur est $\langle c\rangle$. On obtient de fait deux classes de conjugaison de 5-cycles dans A_5 : on peut vérifier par exemple que les classes de conjugaison de $(1\,2\,3\,4\,5)$ et $(2\,1\,3\,4\,5)$ sont distinctes dans A_5.

5. Soit $H \subset A_5$ un sous-groupe distingué. L'ordre de H divise $60 = 2^2 3^1 5$ donc $|H| = 1, 2, 3, 4, 5, 6, 12, 10, 15, 20, 24, 30, 60$. De plus, H est par définition l'union de classes de conjugaison et contient la classe du neutre :

   - il ne peut contenir une seule classe de conjugaison non-triviale puisqu'il serait d'ordre 16, 21, 13, qui ne figure pas parmi les diviseurs,
   - il ne peut pas non plus en contenir exactement 2 puisqu'il serait d'ordre 36, 28, 33, 25, qui ne sont pas non plus des diviseurs de 60,
   - finalement, ce n'est pas non plus possible pour 3, puisqu'il serait d'ordre 45, 48, 40, qui ne divisent pas 60.

   En définitive, on a montré que si H n'est pas trivial, alors $H = \mathrm{A}_5$. Les sous-groupes distingués de A_5 sont triviales où A_5 tout entier ce qui signifie que A_5 est simple.

Exercice 5.

1. Exhiber un sous-groupe transitif de S_6 isomorphe à S_3.
2. Exhiber un sous-groupe de S_8 isomorphe à H_8.
3. Montrer pour $n < 8$, qu'aucun sous-groupe de S_n n'est isomorphe à H_8.

Exercice 6. Générateurs de S_n II

Soit $n \geqslant 1$ un entier. Soit a, b deux entiers tels que $1 \leqslant a < b \leqslant n$. On se donne la transposition $\tau = (a\,b)$ et le n-cycle $\sigma = (1\,2\,3\,\ldots\,n)$. On se propose de montrer $\mathrm{S}_n = \langle\sigma, \tau\rangle \iff (b-a, n) = 1$.

1. Soit $d \coloneqq (b-a, n)$. Montrer[2] que l'action de $\langle\sigma, \tau\rangle$ sur $\{1, 2, \ldots, n\}$ préserve les classes de congruence modulo d. En déduire le sens direct.
2. Supposons que $(b-a, n) = 1$. Montrer σ^{b-a} est un n-cycle de la forme $\sigma^{b-a} = (a\ b\ \ldots)$. En déduire que $\langle\sigma, \tau\rangle$ est conjugué à $\langle(1\,2), (1\,2\,\ldots)\rangle$ puis conclure le sens réciproque.
3. Supposons $n = p$ un entier premier. Montrer qu'une transposition et un p-cycle quelconques engendrent S_p. Justifier que ce n'est pas le cas pour S_4 et S_6.

Exercice 7.

Soit $n \geqslant 1$ un entier.

1. Montrer que l'équation
$$\sum_{i=1}^{n} \frac{1}{m_i} = 1,$$
n'a qu'un nombre fini de solutions $(m_1, \ldots, m_n) \in (\mathbb{N} \setminus \{0\})^n$.
2. En déduire qu'il n'existe qu'un nombre fini de classes d'isomorphisme de groupes finis admettant exactement n classes de conjugaison.

Correction exercice 7

1. Soit $\mathrm{I} = \mathbb{R}_+^\times$, considérons S comme un sous-ensemble discret de I^n. L'application $f\colon \mathrm{I} \to \mathrm{I}$ donnée par $x \mapsto \frac{1}{\sqrt{x}}$ est un homéomorphisme. Ainsi, $F = (f, \ldots, f)\colon \mathrm{I}^n \to \mathrm{I}^n$ est un homéomorphisme et l'image de S est un sous-ensemble discret de la sphère $\mathbb{S}^n = \{(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n \mid x_1^2 + x_2^2 + \cdots + x_n^2 = 1\}$ qui est un sous-ensemble compact de $\mathbb{R}^n$. Comme un sous-ensemble discret et compacte est fini, l'image de S par F est finie et donc S est fini.

[2] Plus formellement, montrer $\forall g \in \langle\sigma, \tau\rangle$, $i \equiv j \bmod d \implies g(i) \equiv g(j) \bmod d$

2. Soit G un groupe, que l'on fait agir sur lui même par conjugaison. Supposons qu'il ait n classes de conjugaison que l'on note $C_1, \dots, C_n$. On peut supposer que C_1 est la classe de l'élément neutre dont le stabilisateur est G tout entier. Par la relation orbite-stabilisateur, on peut écrire la formule des classes comme

$$|G| = \sum_{k=1}^{n} \frac{|G|}{|G_k|}, \quad \text{où } G_k \coloneqq G_{C_k}.$$

On divise la relation par $|G|$ pour obtenir que $\sum_{k=1}^{n} \frac{1}{|G_k|} = 1$. On sait que cette relation n'a qu'un nombre fini de solution, en particulier on n'a qu'un nombre fini de valeurs possibles pour $|G_1| = |G|$. Or on sait qu'il n'existe qu'un nombre fini de groupes de cardinal fixé. Ainsi, il n'existe qu'un nombre fini de groupes à exactement n classes de conjugaison.

Exercice 8. Lemme de Ore

Soient G un groupe fini et p le plus petit facteur premier de $|G|$.

1. On suppose que G agit sur un ensemble X à p éléments. Montrer que G_x agit trivialement sur X pour tout $x \in X$.
2. En déduire que tout sous-groupe de G d'indice p est distingué.

Correction exercice 8

1. Soit $x \in X$, on fait agir G_x sur X. Notons que p est le plus petit facteur premier de $|G_x|$. Ainsi, pour $y \in X$ on a

$$\frac{|G_x|}{|G_x \cap G_y|} = |G_x \cdot y| \leqslant |X| = p.$$

Mais l'inégalité précédente est stricte car G_x admet un point fixe et donc nécessairement $G_x = G_x \cap G_y$. Ainsi, $G_x \subset G_y$ pour tout $y \in X$ et G_x agit trivialement sur X.

2. Soit $H \subset G$ un sous-groupe d'indice p. Considérons le G-ensemble des classes à gauche $X \coloneqq G/H$. D'après la question précédente, pour tout $x \in X$, G_x opère trivialement sur X. Rappelons que le stabilisateur de la classe de H est $H = G_H$. Comme $gHg^{-1} = G_x$ pour $x = gH \in X$ on déduit que gHg^{-1} agit trivialement sur X et en particulier fixe la classe de H i.e. $gHg^{-1} \subset H$ pour tout $g \in H$ et on a bien montré que H est distingué dans G.