Université M. Ismail – Faculté des Sciences – Département de Mathématiques

Travaux Dirigés d'Algèbre 6 - S4 / Corrigé de la Série 3 - (proposé par Pr. Rami) – 2020-2021

Exercice 1.

Pour la décomposition de σ en cycles disjoints, on remarque que :
–$\sigma(1) = 3,\ \sigma^2(1) = \sigma(3) = 5,\ \sigma^3(1) = \sigma(5) = 1$ et donc $c_1 = (1,\ 3,\ 5)$ est un cycle.
–$\sigma(2) = 9,\ \sigma^2(2) = \sigma(9) = 10,\ \sigma^3(2) = \sigma(10) = 4,\ \sigma^4(2) = \sigma(4) = 2$ et donc $c_2 = (2,\ 9,\ 10,\ 4)$ est un cycle.
$\sigma(7) = 8,\ \sigma^2(7) = \sigma(8) = 7$ et donc $c_3 = (7,\ 8)$ est un cycle.
Il reste 6 et 11 qui sont fixes pour σ. Par conséquent :

$$\sigma = c_1c_2c_3.$$

Pour la décomposition de σ' en cycles disjoints, on procède de la même façon et on obtient :

$$\sigma' = c_1c_2c_3$$

avec $c_1 = (1,\ 10,\ 13,\ 4,\ 11,\ 3,\ 7)$, $c_2 = (2,\ 5,\ 9,\ 6)$ et $c_3 = (8,\ 12,\ 14)$.

Pour calculer σ^{2020}, on détermine d'abord l'ordre de σ. Sachant que la décomposition de σ en cycles disjoints est $\sigma = c_1c_2c_3 = (1,\ 3,\ 5)(2,\ 9,\ 10,\ 4)(7,\ 8)$ donc $o(\sigma) = ppcm(o(c_1), o(c_2), o(c_3))$; Or, $o(c_1) = 3$, $o(c_2) = 4$ et $o(c_3) = 2$ d'où $o(\sigma) = 12$. Finalement, comme $2020 = 12 \times 18 + 4$ on a alors $\sigma^{2020} = (\sigma^{12})^{18}\sigma^4 = \sigma^4 = c_1^4c_2^4c_3^4 = c_1$.

Exercice 2. 1) Le produit $c_1c_2c_3$ dans $\mathcal{S}_4$ est donné par :

$$\begin{array}{c}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \\ 4 & 1 & 3 & 2 \\ 4 & 2 & 1 & 3 \end{pmatrix}\end{array} \begin{array}{c} \\ c_3 \\ c_2 \\ c_1 \end{array} = (1,\ 4,\ 3)$$

On peut aussi faire un calcul direct :

$$c_1c_2c_3(1) = 4,\ c_1c_2c_3(2) = 2,\ c_1c_2c_3(3) = 1,\ et\ c_1c_2c_3(4) = 3.$$

N. B. les cycles ne sont pas disjoints !

2) Soit $\tau_1,\ \tau_2$ deux transpositions de $\mathcal{S}_n$ avec $n \geq 3$. D'après la Proposition IV. 0. 2 du cours, puisque ce sont deux cycles de même longueur égale à 2, il existe $\sigma \in \mathcal{S}_n$ telle que $\tau_1 = \sigma\tau_2\sigma^{-1}$ par suite $\tau_1\tau_2 = \sigma\tau_2\sigma^{-1}\tau_2$ et comme $\tau_2 = \tau_2^{-1}$, alors $\tau_1\tau_2 = \sigma\tau_2\sigma^{-1}\tau_2^{-1} = [\sigma, \tau_2]$.

N.B ; Pour $n = 2$ il n'y a qu'une seule transposition et le résultat est évident.

Supposons que $Z(\mathcal{S}_n) \neq \{Id\}$. Il existe donc $Id \neq \sigma \in \mathcal{S}_n\ :\ \forall \sigma' \in \mathcal{S}_n,$ on a $\sigma\sigma' = \sigma'\sigma$. Seulement, puisque $n \geq 3$, on peut choisir $a, b, c \in I_n$ distincts deux à deux tels que $\sigma(a) = b$. On prend alors $\tau = (b, c)$. On remarque que $\sigma\tau(a) = \sigma(a) = b$ et $\tau\sigma(a) = \tau(b) = c$ et donc $\sigma\tau \neq \tau\sigma$. D'où la contradiction et donc $Z(\mathcal{S}_n) = \{Id\}$.

Exercice 3. S'il existe un homomorphisme surjectif $f : \mathcal{S}_3 \to \mathcal{A}_3$, on aurait alors, d'après le premier théorème d'isomorphisme, $\mathcal{S}_3/Ker(f) \cong \mathcal{A}_3$ et en particulier $Ker(f)$ serait un groupe (toujours) distingué de $\mathcal{S}_3$ qui est d'ordre 2 car $|\mathcal{S}_3/Ker(f)| = |\mathcal{S}_3|/|Ker(f)| = 3$. Or, les seuls sous-groupes d'ordre 2 sont $< \tau_1 >$, $< \tau_2 >$ ou $< \tau_3 >$. Mais en revenant à la table de multiplication de $\mathcal{S}_3$, on vérifie qu'aucun d'eux n'est disingué. Par conséquent il n'existe pas de homomorphisme surjectif $f : \mathcal{S}_3 \to \mathcal{A}_3$.

Exercice 4.

1. Générateurs de $\mathcal{S}_n$:
   (a) Par les transpositions simples $(i, i+1)$: il suffit de remarquer que toute transposition (i,j) avec $i < j$ s'écrit comme suit :

   $$(i,j) = (\mathbf{i}, \mathbf{i+1})(i{+}1, i{+}2)\dots(\mathbf{j-2}, \mathbf{j-1})(\mathbf{j-1}, \mathbf{j})(\mathbf{j-2}, \mathbf{j-1})\dots(i{+}1, i{+}2)(\mathbf{i}, \mathbf{i+1}).$$

   Et comme $\mathcal{S}_n$ est engendré par les transpositions (i,j), donc il est engendré par les transpositions $(i, i+1)$ qui forment l'ensemble $\{(1,2), (2,3)\dots(n-1,n)\}$.
   (b) Par la transposition $(1,2)$ et le cycle $c = (1, 2, \dots, n)$: pour cela, remarquons les faits successifs suivants (sachant que $c^{-1} = (n, n-1, n-2, \dots, 2, 1)$) :
   On vérifie par un simple calcul que $c(1,2)c^{-1} = (2,3)$, $c(2,3)c^{-1} = (3,4)$ (appliquer pour cela la permutation à tous les entiers $1 \leq i \leq n$). En supposant par récurrence que $c(i-1,i)c^{-1} = (i, i+1)$, on montre de la même façon que $c(i, i+1)c^{-1} = (i+1, i+2)$ et ainsi, on a $\forall 0 \leq k \leq n-2,\ c^k(1,2)c^{-k} = (k+1, k+2)$. Ce qui permet d'exprimer tous les générateurs obtenus en (a) en fonction de la transposition $(1,2)$ et du cycle $c = (1, 2, \dots, n)$ lesquels sont par conséquent des générateurs de $\mathcal{S}_n$.
   (c) Par les transpositions $(1,2)$, $(1,3)$, $\dots$, $(1,n)$: il suffit de vérifier la formule suivante pour tout couple (i,j) tel que $1 < i < j$: $(i,j) = (1,i)(1,j)(1,i)$. Ainsi en notant que les transpositions $(1,i)$ s'écrivent automatiquement en fonction des transpositions $(1,i)$! ! !, on conclut que $\mathcal{S}_n$ est engendré par les transpositions $(1,2)$, $(1,3)$, $\dots$, $(1,n)$.
2. On sait que $\mathcal{A}_n$ est engendré par les permutations paires et donc d'après la question précédente, il est engendré par les produits $(i, i+1)(i+1, i+2) = (i, i+1, i+2)$. Pour le vérifier, appliquer en premier $(i+1, i+2)$ puis ensuite $(i, i+1)$, on obtient :

   $$i \mapsto i \mapsto i{+}1;\ i{+}1 \mapsto i{+}2 \mapsto i{+}2;\ i{+}2 \mapsto i{+}1 \mapsto i;\ \forall l \notin \{i, i{+}1, i{+}2\},\ l \mapsto l \mapsto l.$$

   On a ainsi montré que $\mathcal{A}_n$ est engendé par les cycles de la forme $(i, i+1, i+2)$, $\forall 1 \leq i \leq n-1$.

Exercice 5. Montrons que $V_4 = \{id_{I_4},\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\}$ est distingué dans $\mathcal{S}_4$. Remarquons en premier lieu que les éléments de V_4 autres que l'identité sont les produits de deux transpositions (a,b) et (c,d) avec $\{a,b,b,c,d\} = I_4$. Soit donc $\forall \sigma \in \mathcal{S}_4$, on a alors $\sigma(a,b)(c,d)\sigma^{-1} = \sigma(a,b)\sigma^{-1}\sigma(c,d)\sigma^{-1} = (\sigma(a,b)\sigma^{-1})(\sigma(c,d)\sigma^{-1}) = (\sigma(a), \sigma(b))(\sigma(c), \sigma(d)) \in V_4$.
Puisque $\{\sigma(a), \sigma(b), \sigma(c), \sigma(d)\} = I_4$, il en résulte que $V_4 \trianglelefteq \mathcal{S}_4$.

Puisque les éléments de V_4 sont des produits de deux transpositions, il est évidemment un sous-groupe de $\mathcal{A}_4$ et puisqu'il est distingué dans $\mathcal{S}_4$, il est aussi distingué dans $\mathcal{A}_4$. On en déduit immédiatement que $\mathcal{A}_4$ n'est pas simple.

N.B. Pour voir que V_4 est un sous-groupe de $\mathcal{S}_4$, il suffit de remarquer que ses éléments sont tous d'ordre 2 et que le produit de deux d'entre-eux reste dans V_4.

De la même manière, on montre que H est un sous-groupe de V_4. Pour montrer que $H \trianglelefteq V_4$, notons $\sigma_1 = (1,2)(3,4) \in H$ et $\sigma_2 = (1,3)(2,4)$, $\sigma_3 = (1,4)(2,3) \in V_4$. On a vu auparavant que

$$\sigma(a,b)(c,d)\sigma^{-1} = (\sigma(a),\sigma(b))(\sigma(c),\sigma(d)).$$

En l'appliquant à $\sigma_1 = (1,2)(3,4) \in H$ et $\sigma = \sigma_2$ ou $\sigma = \sigma_3$, on trouve que $\sigma\sigma_1\sigma^{-1} \in H$ et par suite $H \trianglelefteq V_4$. D'autre part, en prenant maintenant $\sigma\tau = (1,4) \notin V_4$, on trouve que $\tau\sigma_1\tau^{-1} = (4,2)(3,1) \notin H$ et donc $H \not\trianglelefteq \mathcal{S}_4$ (n'est pas distingué).

Exercice 6. On a vu à la fin de la série 2 que $\mathcal{S}_3$ est résoluble : $\{Id\} \trianglelefteq \mathcal{A}_3 \trianglelefteq \mathcal{S}_3$ et $\mathcal{S}_3/\mathcal{A}_3$ est cyclique, donc commutatif.

Pour $\mathcal{S}_4$, en utilisant l'exercice précédent, on a la suite :

$$\{Id\} \trianglelefteq H \trianglelefteq V_4 \trianglelefteq \mathcal{A}_4 \trianglelefteq \mathcal{S}_4$$

qui en plus vérifie $\mathcal{S}_4/\mathcal{A}_4$ est d'ordre 2 et donc cyclique et c'est le cas pour $\mathcal{A}_4/V_4$ qui est d'ordre 3, V_4/H qui est d'ordre 2 et enfin $H/\{Id\} = H$ qui est d'ordre 2. En conclusion, $\mathcal{S}_4$ est résoluble.

Exercice 7. Supposons que $\mathcal{A}_4$ contient un sous-groupe K d'ordre 6 ; il est donc d'indice $[\mathcal{A}_4, K] = 2$ et pas suite (voir l'exercice 3 de la série 2) il est distingué dans $\mathcal{A}_4$. D'autre part, d'après le Théorème de Cauchy -$6 = 3 \times 2$- il contient un élément d'ordre 3 qui est donc un 3-cycle. Enfin, d'après le cours, (le Lemme 3 page 35) on a alors $H = \mathcal{A}_4$ ce qui est absurde et par conséquent, $\mathcal{A}_4$ ne contient aucun sous-groupe K d'ordre 6.

Exercice 8. Soit $n \geq 3$ et $D(\mathcal{S}_n)$ le sous-groupe dérivé de $\mathcal{S}_n$. On rappelle que

$$D(\mathcal{S}_n) =< [\sigma,\sigma'],\ \ \sigma,\ \sigma' \in \mathcal{S}_n >$$

le sous-groupe engendré par les commutateurs. Il est distingué dans $\mathcal{S}_n$ dû à la relation

$$\sigma"[\sigma,\sigma']\sigma"^{-1} = [\sigma"\sigma\sigma"^{-1}, \sigma"\sigma'\sigma"^{-1}],\ \forall\sigma" \in \mathcal{S}_n.$$

D'autre part, $\forall\sigma,\ \sigma' \in \mathcal{S}_n$ $\varepsilon([\sigma,\sigma']) = \varepsilon(\sigma)\varepsilon(\sigma')\varepsilon(\sigma^{-1})\varepsilon(\sigma'^{-1}) = \varepsilon(\sigma)^2\varepsilon(\sigma')^2 = +1$ et par suite $D(\mathcal{S}_n) \subseteq \mathcal{A}_4$. Montrons ensuite l'autre inclusion. Pour cela, on va utiliser le fait que $\mathcal{A}_4$ est engendré par les 3-cycles (cours). Soit donc (i,j,k) un 3-cycle ; comme il est d'ordre 3 et $(i,j,k)^{-1} = (i,k,j)$, on a $(i,j,k)^3 = Id \Rightarrow (i,j,k) = (i,j,k)^{-2} = (i,k,j)^2$. Il en résulte que

$$(i,j,k) = (i,k,j)^2 = ((i,j)(i,k))^2 = (i,j)(i,k)(i,j)(i,k) = (i,j)(i,k)(i,j)^{-1}(i,k)^{-1} = [(i,j),(i,k)].$$

Par suite $(i,j,k) \in D(\mathcal{S}_n)$ et $\mathcal{A}_n \subseteq D(\mathcal{S}_n)$. D'où le résultat $\mathcal{A}_n = D(\mathcal{S}_n)$.

Exercice 9. Soit $n \geq 5$ et H un sous-groupe distingué de $\mathcal{S}_n$.

1. Comme $\mathcal{A}_n \trianglelefteq \mathcal{S}_n$, on a aussi $H \cap \mathcal{A}_n \trianglelefteq \mathcal{S}_n$. Mais $\forall\sigma \in \mathcal{S}_n$ et $\forall\sigma' \in H \cap \mathcal{A}_n$ on a $\varepsilon(\sigma\sigma'(\sigma)^{-1}) = \varepsilon(\sigma)^2\varepsilon(\sigma') = +1$, donc $\sigma\sigma'(\sigma)^{-1} \in \mathcal{A}_n$ et par suite $H \cap \mathcal{A}_n \trianglelefteq \mathcal{A}_n$.
   Comme $n \geq 5$, $\mathcal{A}_n$ est simple, on en déduit alors que $H \cap \mathcal{A}_n = \mathcal{A}_n$ et donc que $\mathcal{A}_n \subseteq H$ ou bien que $H \cap \mathcal{A}_n = \{Id_{I_n}\}$.

2. On suppose que $H \cap \mathcal{A}_n = \{Id_{I_n}\}$. Soit $\varepsilon_{|H} : H \to \{-1, +1\}$ la restriction de ε à H. $\forall \sigma \in H$, $\varepsilon(\sigma) = +1 \Rightarrow \sigma \in H \cap \mathcal{A}_n \Rightarrow \sigma = Id_{I_n}$ et donc $\ker(\varepsilon) = \{Id_{I_n}\}$ c. à. d. $\varepsilon_{|H}$ est injective.
   Soit maintenant $\sigma \in H$ et $\sigma' \in \mathcal{S}_n$, on a déjâ vu que $\varepsilon([\sigma, \sigma']) = +1$ et donc $[\sigma, \sigma'] = \sigma\sigma'\sigma^{-1}\sigma'^{-1} \in \mathcal{A}_n$. Mais, comme $H \trianglelefteq \mathcal{S}_n$, on a alors $\sigma'\sigma^{-1}\sigma'^{-1}) \in H$ ce qui entraine que $\sigma\sigma'\sigma^{-1}\sigma'^{-1} = \sigma(\sigma'\sigma^{-1}\sigma'^{-1}) \in H$, et par suite $[\sigma, \sigma'] \in H \cap \mathcal{A}_n$. Ainsi, on a $[\sigma, \sigma'] = Id_{I_n}$ et donc $\sigma \in Z(\mathcal{S}_n)$ et $H \subseteq Z(\mathcal{S}_n)$.

   Montrons ensuite que $Z(\mathcal{S}_n) = \{Id_{I_n}\}$ (une autre preuve à été donnée à l'exercice 2). Pour cela, soit $\sigma \in Z(\mathcal{S}_n)$ et $k \in I_n$. Puisque $n \geq 3$, il existe $\sigma' \in \mathcal{S}_n$ tel que $\sigma'(k) = k$ et $\sigma'(i) \neq i$, $\forall i \neq k$. On a alors $\forall k \in I_n$:

   $$\sigma \in Z(\mathcal{S}_n) \Rightarrow \sigma'\sigma = \sigma\sigma' \Rightarrow \sigma'\sigma(k) = \sigma\sigma'(k) \Rightarrow \sigma'(\sigma(k)) = \sigma(k) \Rightarrow \sigma(k) = k$$

   (car le seul élément fixé par σ' est k ! ! !). Par suite $\sigma = Id_{I_n}$ et donc $Z(\mathcal{S}_n) = \{Id_{I_n}\}$.
   En conclusion $H = \{Id_{I_n}\}$.

3. On suppose maintenant que $\mathcal{A}_n \subseteq H$. Comme $\mathcal{A}_n \trianglelefteq \mathcal{S}_n$ on a aussi $\mathcal{A}_n \trianglelefteq H$ et donc $[\mathcal{S}_n : \mathcal{A}_n] = [\mathcal{S}_n : H][H : \mathcal{A}_n] = 2$ et donc $[H : \mathcal{A}_n] = 1$ ou $[H : \mathcal{A}_n] = 2$ ce qui entraine que $H = \mathcal{A}_n$ ou bien $H = \mathcal{S}_n$.

4. D'après ce qui précède, les sous-groupes distingués de $\mathcal{S}_n$ sont uniquement $\{Id_{I_n}\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$.

   Il en résulte que pour tout $n \geq 5$, $\mathcal{S}_n$ n'est pas résoluble ! ! !.