EPFL Automne 2017

Geometrie, MATH-120

Solutions Série 5

Les exercices 1 a 6 ont ete corriges dans le cours. Nous ne donnons donc ici que la correction de l'Exercice 7.

Exercice 7. (Unicite de la signature) Soit

$$\mathfrak{S}_n = \mathfrak{S}_{\{1,2,\cdots,n\}} = \mathrm{Bij}(\{1,2,\cdots,n\})$$

le groupe symetrique de n elements (le groupe des permutations de l'ensemble $\{1,2,\cdots,n\}$, muni de la composition)

La "signature" est un morphisme de ce groupe vers le groupe multiplicatif $\{\pm 1\}$ qui est *non-trivial* (qui n'est pas le morphisme constant $\sigma \to 1$). On note ce morphisme

$$\varepsilon : (\mathfrak{S}_n, \circ) \to (\{\pm 1\}, \times).$$

On peut montrer l'existence d'un tel morphisme soit par des arguments de theorie des groupes, soit par des methodes d'algebre lineaire (a partir du determinant).

Dans cet exercice on va montrer qu'un tel morphisme (en admettant qu'il existe) est en fait unique.

Pour $l \geqslant 2$ et $n_i \in \{1,\cdots,n\}$ des entiers tous distincts on note

$$(n_1, n_2 \cdots, n_l) =$$

la permutation σ telle que

$$\sigma(n_1) = n_2,\ \sigma(n_2) = n_3, \cdots, \sigma(n_{l-1}) = n_l,\ \sigma(n_l) = n_1$$

et qui laisse fixe tous les elements $m \in \{1,2,\cdots,n\}$ differents des n_i ($\sigma(m) = m$). Une telle permutation est dite cyclique (ou est un cycle) de longueur l.

Une transposition est une permutation cyclique de longueur 2 : de la forme (n_1, n_2), c'est a dire qu'elle echange n_1 et n_2 et laisse tous les autres elements $\neq n_1, n_2$ fixes.

On admettra (et on montrera plus tard au deuxieme semestre) que toute permutation $\sigma \in \mathfrak{S}_n$ peut s'ecrire comme la composee de permutations cycliques.

1. Quel est l'ordre de $(n_1, n_2, \cdots, n_l)$?
2. Pour une permutation τ donnee calculer le conjugue par tau du cycle $(1, 2, \cdots, l)$:
$$\tau \circ (1, 2, \cdots, l) \circ \tau^{-1}$$
(que vaut $\tau \circ (1, 2, \cdots, l) \circ \tau^{-1}(\tau(1))$?).
3. Montrer que tous les cycles d'une longueur donnee sont conjugues entre eux : si $(n_1, n_2, \cdots, n_l)$ et $(m_1, m_2, \cdots, m_l)$ sont deux cycles de longueur l il existe un permutation τ telle que
$$(m_1, m_2, \cdots, m_l) = \mathrm{ad}_\tau(n_1, n_2, \cdots, n_l) = \tau \circ (n_1, n_2, \cdots, n_l) \circ \tau^{-1}.$$
4. Montrer par recurrence (sur la longueur) que tout cycle peut s'ecrire comme composee de transpositions. Montrer que $\mathfrak{S}_n$ est engendre par les $\frac{n(n-1)}{2}$ transpositions
$$(n_1, n_2),\ 1 \leqslant n_1 < n_2 \leqslant n.$$
5. Soit
$$\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$$
un morphisme de groupes ($\{\pm 1\}$ est muni de la multiplication). Montrer que ε prend la meme valeur pour toute les transpositions (cf. Exercice 1).
6. En deduire qu'il n'existe pas plus de deux morphismes de groupes $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$.

Solution 7. 1. Notons tout d'abord que dans $\mathrm{Bij}(\{1, 2, \cdots, n\})$, l'element neutre est l'identite Id et la loi de composition interne est la composee $\circ$. Ainsi, nous savons que l'ordre de $(n_1, n_2, \cdots, n_l)$ est le plus petit entier $m > 0$ tel que $(n_1, n_2, \cdots, n_l)^m = Id$. Il est facile de voir que, pour tout entier m strictement positif et $k \in \{1, 2, \cdots, l\}$,
$$(n_1, n_2, \cdots, n_l)^m(n_k) = n_{r_l(k+m)},$$
ou $r_l(k+m)$ est le reste de la division euclidienne de $k+m$ par l. Ainsi, $(n_1, n_2, \cdots, n_l)^m = Id$ si et seulement si $k = r_l(k+m)$ pour tout $k \in \{1, 2, \cdots, l\}$, i.e. si et seulement si $m = Ml$, pour $M \in \mathbb{N}$ et strictement positif. On en deduit donc que l'ordre de $(n_1, n_2, \cdots, n_l)$ est egal a l.

2. Notons tout d'abord que $\tau \circ (1, 2, \cdots, l) \circ \tau^{-1} \in \mathrm{Bij}(\{1, 2, \cdots, n\})$ etant donne que $\tau, \tau^{-1}, (1, 2, \cdots, l) \in \mathrm{Bij}(\{1, 2, \cdots, n\})$ et que la composee d'applications bijectives est bijective. En utilisant la definition de la composee de fonctions ainsi que celle de $(1, 2, \cdots, l)$, on a, pour tout $k \in \{1, 2, \cdots, l-1\}$,
$$\begin{aligned}(\tau \circ (1, 2, \cdots, l) \circ \tau^{-1})(\tau(k)) = \tau \circ (1, 2, \cdots, l)(\tau^{-1}(\tau(k)) &= \tau \circ (1, 2, \cdots, l)(k) \\ &= \tau((1, 2, \cdots, l)(k)) \\ &= \tau(k+1). \qquad (0.1)\end{aligned}$$

Le meme raisonnement nous donne que

$$(\tau \circ (1,2,\cdots,l) \circ \tau^{-1})(\tau(l)) = \tau(1). \tag{0.2}$$

Par ailleurs, pour tout $m \in \{1,2,\cdots,n\}$ different de tous les $\tau(k), k \in \{1,2,\cdots,l\}$, notons que $\tau^{-1}(m) \notin \{1,2,\cdots,l\}$. En effet, supposons que $\tau^{-1}(m) = k$ pour un $k \in \{1,2,\cdots,l\}$. Ainsi, on a $\tau(\tau^{-1}(m)) = \tau(k)$, i.e. $m = \tau(k)$, ce qui est absurde (car contredit la caracterisation de m). Ainsi, pour tout $m \in \{1,\cdots,n\}$ different de tous les $\tau(k), k \in \{1,2,\cdots,l\}$, on a

$$\tau \circ (1,2,\cdots,l) \circ \tau^{-1}(m) = \tau((1,2,\cdots,l)(\tau^{-1}(m))) = \tau(\tau^{-1}(m)) = m. \tag{0.3}$$

Finalement, en combinant (0.1), (0.2) et (0.3), on obtient que

$$\tau \circ (1,2,\cdots,l) \circ \tau^{-1} = (\tau(1),\tau(2),\cdots,\tau(l)).$$

3. Soient $(n_1,n_2,\cdots,n_l)$ et $(m_1,m_2,\cdots,m_l)$ deux cycles. En appliquant le meme raisonnement qu'a la question precedente, on obtient que pour tout $\tau \in \mathfrak{S}_n$,

$$\tau \circ (n_1,n_2,\cdots,n_l) \circ \tau^{-1} = (\tau(n_1),\tau(n_2),\cdots,\tau(n_l)).$$

Ainsi, en choisissant $\tau \in \mathrm{Bij}(\{1,2,\cdots,n\})$ tel que, pour tout $k \in \{1,2,\cdots,l\}$, $\tau(n_k) = m_k$, on obtient

$$\tau \circ (n_1,n_2,\cdots,n_l) \circ \tau^{-1} = (m_1,m_2,\cdots,m_l),$$

ce qui montre que $(n_1,n_2,\cdots,n_l)$ et $(m_1,m_2,\cdots,m_l)$ sont conjugues.

4. Montrons pas recurrence sur la longueur $l \geqslant 2$ que tout cycle $(n_1,n_2,\cdots,n_l)$, $n_1,n_2,\cdots,n_l \in \{1,2,\cdots,n\}$, peut s'ecrire comme la composee de transpositions. Prenons $l = 2$. Dans ce cas tout cycle s'ecrit (n_1,n_2) avec $n_1,n_2 \in \{1,2,\cdots,n\}$ et distincts, ce qui est une transposition par definition et donc une composee de transpositions. Maintenant, supposons, pour un $l \in \{2,\cdots,n-1\}$, que tout cycle de longueur l s'ecrit comme la composee de transpositions et montrons que c'est vrai pour $l+1$. Il est facile de voir que, pour tout $n_1,\cdots,n_{l+1} \in \{1,2,\cdots,n\}$ et distincts,

$$(n_1,n_2,\cdots,n_{l+1}) = (n_1,n_2,\cdots,n_l) \circ (n_l,n_{l+1}).$$

Ainsi, comme $(n_1,n_2,\cdots,n_l)$ s'ecrit comme la composee de transpositions (d'apres l'hypothese de recurrence), on en deduit que $(n_1,n_2,\cdots,n_l) \circ (n_l,n_{l+1})$ s'ecrit egalement comme la composee de transpositions et il en va donc de meme pour $(n_1,n_2,\cdots,n_{l+1})$.
Notons maintenant T_n le sous-groupe engendre par les $\frac{n(n-1)}{2}$ transpositions

$$(n_1,n_2), \ 1 \leqslant n_1 < n_2 \leqslant n.$$

Observons tout d'abord que ces transpositions sont bien des permutations et donc qu'elle appartiennent toutes a $\mathfrak{S}_n$. Ainsi, par definition d'un sous-groupe engendre, il est clair que $T_n \subset \mathfrak{S}_n$. Montrons maintenant que $\mathfrak{S}_n \subset T_n$. Soit $\sigma \in \mathfrak{S}_n$. D'apres l'enonce, on peut dire que σ peut s'ecrire comme la composee de permutations cycliques. Comme, d'apres la Question 4, toute permutation cyclique peut s'ecrire comme la composee de transpositions, on en deduit que σ peut s'ecrire comme la composee de transpositions. Maintenant, pour tout $n_1, n_2 \in \{1, 2, \cdots, n\}$ et distincts, il est clair que $(n_1, n_2) = (n_2, n_1)$. Ainsi, σ peut s'ecrire comme la composee de transpositions du type (n_1, n_2) avec $n_1, n_2 \in \{1, 2, \cdots, n\}$ et tels que $n_1 < n_2$. De plus, comme T_n est un sous-groupe, la composee d'elements de T_n appartient a T_n. On en deduit que $\sigma \in T_n$ et donc que $\mathfrak{S}_n \subset T_n$. Finalement, $\mathfrak{S}_n = T_n$, d'ou le resultat.

5. Les transpositions sont des cycles. La Question 3 nous dit donc que toutes les transpositions sont conjuguees entre elles. Comme ε est est un morphisme de groupes et que $\{\pm 1\}$ muni de la multiplication est commutatif (par commutativite de la multiplication), on obtient en appliquant le resultat de l'Exercice 1 que ε prend la meme valeur pour toutes les transpositions.

6. En appliquant la Question 4 de l'Exercice 2 de la Serie 4 ainsi que la deuxieme partie de la Question 4 de cet exercice, nous obtenons que tout morphisme $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ est completement determine par ses valeurs prises sur les transpositions du type (n_1, n_2) avec $n_1, n_2 \in \{1, 2, \cdots, n\}$ et tels que $n_1 < n_2$. Or la Question 4 nous donne qu'un tel morphisme prend la meme valeur pour toutes les transpositions. Ainsi, un tel morphisme peut prendre la valeur -1 sur toutes les transpositions (et s'il existe un morphisme satisfaisant ceci, il n'y en a qu'un seul) ou la valeur $+1$ sur toutes les transpositions (et s'il existe un morphisme satisfaisant ceci, il n'y en a qu'un seul). On obtient donc qu'il y a au plus deux morphismes de groupes $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$.