Année universitaire 2019/2020
Licence 2, S4, mathématiques
Structures algébriques 1 – **Feuille 4-correction**

On note $\mathcal{S}_n$ le groupe des permutations de l'ensemble $\{1,\dots,n\}$, et $\mathcal{A}_n$ le sous-groupe des permutations paires.

Exercice 1

(1) (cours) $\sigma c\sigma^{-1} = (\sigma(c_1),\dots,\sigma(c_l))$.

(2) $\sigma c = c\sigma$ si et seulement si $\sigma c\sigma^{-1} = c$, c'est-à-dire d'après la question précédente, $(\sigma(c_1),\dots,\sigma(c_l)) = (c_1,\dots,c_l)$. Il existe donc $i \in \{1,\dots,l\}$ tel que $\sigma(c_1) = c_i$, et les suivants s'en déduisent : $\sigma(c_2) = c_{(i+1)\%l}$, …, $\sigma(c_l) = c_{(i+n-1)\%l}$, où on note ici $k\%l$ le représentant de la classe de k modulo l entre 1 et l. On reconnaît alors que $\sigma = c^{i-1}$.

(*Remarque : attention cela ne signifie pas que σ est lui-même un cycle, considérer $(1,2,3,4)^2$ par exemple*).

(3) On a successivement $(1,2)(1,2,3,4) = (2,3,4)$ et $(2,3,4)(1,2,3,4) = (1,3,2,4)$ d'où $(1,2) = (1,3,2,4)(1,2,3,4)^2$ et $(1,2)$ est un produit de cycles de longueur 4.

(4) Quitte à conjuguer, on obtient que toute transposition s'écrit comme un produit de 4-cycles. Plus précisément on a, si i,j,k,l sont deux à deux disjoints,

$$(i,j) = (i,k,j,l)(i,j,k,l)^2.$$

Comme les transpositions engendrent $\mathcal{S}_n$, les 4-cycles engendrent $\mathcal{S}_n$ (pour $n \geq 4$).

(5) Les 3-cycles sont de signature 1, tout produit de 3-cycles est donc de signature 1 (donc pair), car la signature est un morphisme de groupes. On ne peut donc pas engendrer $\mathcal{S}_n$ tout entier : l'élément $(1,2)$ en particulier ne peut pas s'écrire comme produit de 3-cycles.

Exercice 2

(1) On pose l'application $\phi : \mathcal{S}_n \to \mathcal{S}_m, \sigma \mapsto \tilde{\sigma}$, où $\tilde{\sigma}$ est défini par

$$\tilde{\sigma}(i) = \begin{cases} \sigma(i) \text{ si } i \leq n \\ i \text{ sinon} \end{cases}.$$

(*La permutation $\tilde{\sigma}$ n'est rien d'autre que la permutation σ "vue" dans $\mathcal{S}_m$ au lieu de $\mathcal{S}_n$*).

On vérifie que c'est bien un morphisme de groupe : $\forall \sigma,\rho \in \mathcal{S}_n, \forall i \in \{1,\dots,m\}$,

$$\tilde{\sigma} \circ \tilde{\rho}(i) = \begin{cases} \sigma(\rho(i)) \text{ si } i \leq n \\ i \text{ sinon} \end{cases} = \widetilde{\sigma\rho}(i).$$

De plus ce morphisme est injectif, car

$$\mathrm{Ker}(\phi) = \{\sigma,\ \tilde{\sigma} = id\} = \{\sigma,\ \sigma = id\} = \{id\}.$$

Pour chaque $\gamma \in \mathcal{S}_m$, on peut construire un morphisme injectif de $\mathcal{S}_n$ dans $\mathcal{S}_m$ de façon similaire en posant $\phi_\gamma(\sigma) = \gamma\tilde{\sigma}\gamma^{-1}$. Cette permutation permute les éléments de du sous-ensemble $\{\gamma(1),\dots,\gamma(n)\}$ à n éléments de $\mathcal{S}_m$.

(2) On pose $\psi : \mathcal{S}_n \to \mathcal{A}_{n+2}$ défini par

$$\psi(\sigma) = \begin{cases} \sigma \text{ si } \sigma \in \mathcal{A}_n \\ \sigma \circ (n+1, n+2) \text{ sinon.} \end{cases}$$

Cette application est bien définie car si σ est de signature -1 alors $\sigma \circ (n+1, n+2)$ est de signature 1. C'est bien un morphisme de groupe : pour tout $\sigma, \rho \in \mathcal{S}_n$, on utilise que σ et ρ commutent avec $(n+1, n+2)$ par disjonction des supports, pour obtenir que

$$\begin{aligned} \psi(\sigma)\psi(\rho) &= \begin{cases} \sigma\rho \text{ si } \sigma \in \mathcal{A}_n, \rho \in \mathcal{A}_n \\ \sigma\rho(n+1, n+2) \text{ si } \sigma \in \mathcal{A}_n, \rho \notin \mathcal{A}_n \\ \sigma(n+1, n+2)\rho \text{ si } \sigma \notin \mathcal{A}_n, \rho \in \mathcal{A}_n \\ \sigma(n+1, n+2)\rho(n+1, n+2) \text{ si } \sigma \notin \mathcal{A}_n, \rho \notin \mathcal{A}_n \end{cases} \\ &= \begin{cases} \sigma\rho \text{ si } \sigma, \rho \text{ de même parité} \\ \sigma\rho(n+1, n+2) \text{ sinon} \end{cases} \\ &= \psi(\sigma\rho). \end{aligned}$$

On a $\mathrm{Ker}(\psi) = \{\sigma,\ \sigma = id \text{ si } \sigma \in \mathcal{A}_n, \sigma(n+1, n+2) = id \text{ sinon}\} = \{id\}$, donc ψ est injectif.

(3) Par l'absurde, on suppose l'existence d'un morphisme injectif ϕ de $\mathcal{S}_4$ dans $\mathcal{A}_5$. On note que $\mathcal{S}_4$ est de cardinal 24 et $\mathcal{A}_5$ de cardinal 60. Comme ϕ est un morphisme, $\mathrm{Im}(\phi)$ est un sous-groupe de $\mathcal{A}_5$ donc son ordre divise $|\mathcal{A}_5| = 60$ par le théorème de Lagrange. D'autre part, par injectivité de ϕ on aurait $|\mathrm{Im}(\phi)| = |\mathcal{S}_4| = 24$, mais 24 ne divise pas 60 d'où la contradiction.

(4) On montre déjà qu'un morphisme injectif envoie un élément d'ordre 6 sur un élément d'ordre 6 (propriété générale). En effet, les contraintes $\sigma^6 = id$ et $\sigma^k \neq id$ pour $k \in \{1, \dots 5\}$ se traduisent après application de ϕ par $\phi(\sigma^6) = \phi(\sigma)^6 = \phi(id) = id$ et de même $\phi(\sigma^k) = \phi(\sigma)^k \neq id$ (c'est ici qu'on utilise l'injectivité de ϕ), et $\phi(\sigma)$ est d'ordre 6.

Par l'absurde, on suppose l'existence d'un morphisme injectif de $\mathcal{S}_5$ dans $\mathcal{A}_6$. D'après la remarque précédente, un tel morphisme enverrait un élément d'ordre 6 sur un élément d'ordre 6. Dans $\mathcal{S}_5$, il y a des éléments d'ordre 6, comme $(1, 2)(3, 4, 5)$ (il y en a même 20), mais il n'y a pas d'éléments d'ordre 6 dans $\mathcal{A}_6$. En effet les possibilités pour décomposer un élément d'ordre 6 en produit de cycles à supports disjoints sont un cycle de longueur 6 ou un cycle de longueur 3 fois un cycle de longueur 2 : ces deux possibilités sont toutes de signature -1. On obtient donc une contradiction.

Exercice 3 et Exercice 4. cf correction du DS de 2019.

Exercice 5

(1) On note que E contient 8 éléments : $E = \{(\overline{0}, \overline{0}, \overline{0}), (\overline{0}, \overline{0}, \overline{1}), (\overline{0}, \overline{1}, \overline{0}), (\overline{0}, \overline{1}, \overline{1}), (\overline{1}, \overline{0}, \overline{0}), (\overline{1}, \overline{0}, \overline{1}), (\overline{1}, \overline{1}, \overline{0}), (\overline{1}, \overline{1}, \overline{1})\}$. On vérifie que l'application définit bien une action de $\mathcal{S}_3$ sur E :

— $\forall (x_1, x_2, x_3) \in E, id * (x_1, x_2, x_3) = (x_1, x_2, x_3)$
— $\forall (x_1, x_2, x_3) \in E, \forall \sigma, \rho \in \mathcal{S}_3, \sigma * (\rho * (x_1, x_2, x_3)) = \sigma * (x_{\rho^{-1}(1)}, x_{\rho^{-1}(2)}, x_{\rho^{-1}(3)})$. On pose alors $y_i = x_{\rho^{-1}(i)}$, on a

$$\begin{aligned} \sigma * (\rho * (x_1, x_2, x_3)) &= \sigma * (y_1, y_2, y_3) \\ &= (y_{\sigma^{-1}(1)}, y_{\sigma^{-1}(2)}, y_{\sigma^{-1}(3)}) \\ &= (x_{\rho^{-1}(\sigma^{-1}(1))}, x_{\rho^{-1}(\sigma^{-1}(2))}, x_{\rho^{-1}(\sigma^{-1}(3))}) \\ &= (x_{(\sigma\rho)^{-1}(1)}, x_{(\sigma\rho)^{-1}(2)}, x_{(\sigma\rho)^{-1}(3)}) \\ &= (\sigma\rho) * (x_1, x_2, x_3) \end{aligned}$$

.

(2) $\mathrm{Orb}((\overline{0}, \overline{0}, \overline{0})) = \{(\overline{0}, \overline{0}, \overline{0})\}$.
$\mathrm{Orb}((\overline{0}, \overline{0}, \overline{1})) = \{(\overline{0}, \overline{0}, \overline{1}), (\overline{0}, \overline{1}, \overline{0}), (\overline{1}, \overline{0}, \overline{0})\} = \mathrm{Orb}((\overline{0}, \overline{1}, \overline{0})) = \mathrm{Orb}((\overline{1}, \overline{0}, \overline{0}))$.
$\mathrm{Orb}((\overline{0}, \overline{1}, \overline{1})) = \{(\overline{0}, \overline{1}, \overline{1}), (\overline{1}, \overline{1}, \overline{0}), (\overline{1}, \overline{0}, \overline{1})\} = \mathrm{Orb}((\overline{1}, \overline{1}, \overline{0})) = \mathrm{Orb}((\overline{1}, \overline{0}, \overline{1}))$.
$\mathrm{Orb}((\overline{1}, \overline{1}, \overline{1})) = \{(\overline{1}, \overline{1}, \overline{1})\}$.
$\mathrm{Stab}((\overline{0}, \overline{0}, \overline{0})) = \mathcal{S}_3 = \mathrm{Stab}(\overline{1}, \overline{1}, \overline{1}))$.
$\mathrm{Stab}((\overline{0}, \overline{0}, \overline{1})) = \{id, (1,2)\} = \langle (1,2) \rangle = \mathrm{Stab}((\overline{1}, \overline{1}, \overline{0}))$.
$\mathrm{Stab}((\overline{0}, \overline{1}, \overline{0})) = \{id, (1,3)\} = \langle (1,3) \rangle = \mathrm{Stab}((\overline{1}, \overline{0}, \overline{1}))$.
$\mathrm{Stab}((\overline{1}, \overline{0}, \overline{0})) = \{id, (2,3)\} = \langle (2,3) \rangle = \mathrm{Stab}((\overline{0}, \overline{1}, \overline{1}))$.

(3) Pour les éléments $(\overline{0}, \overline{0}, \overline{0})$ et $(\overline{1}, \overline{1}, \overline{1})$, la formule des classes $|\mathrm{Orb}(x)||\mathrm{Stab}(x)| = |G|$ est bien vérifiée : $1 \times 6 = 6$. Pour les autres éléments, la formule des classes est vérifiée, on a bien $3 \times 2 = 6$.

Exercice 6

(1) L'équation des classes implique que $|\mathrm{Orb}(x)|$ divise $|G| = 15$. Les cardinaux possibles des orbites sont donc 1, 3, 5, 15.

(2) En utilisant que l'ensemble E est la réunion disjointe des orbites, et qu'il y a n_i orbites à i éléments, on obtient successivement :

$$[E| = n = \sum_{\mathcal{O} orbite} |\mathcal{O}| = \sum_{i=1}^{15} i n_i.$$

(3) D'après les questions précédentes,

$$7 = \sum_{i=1,3,5,15} i n_i = \sum_{i=1,3,5} i n_i.$$

Les différentes partitions de 7 obtenues avec 1,3,5 sont 5+1+1, 3+3+1, 3+1+1+1+1. On note que dans tous les cas il y a toujours au moins une orbite à un élément, ce qui correspond par définition à un point fixe de l'action.

(4) On regarde de même les partitions de 14 à l'aide de 3 et 5 : la seule possibilité est $5 \times 1 + 3 \times 3$. Il y a donc une orbite à 5 éléments et trois orbites à 3 éléments.

(5) Se donner une action de groupe G sur X est équivalent à se donner un morphisme de groupes $G \to \mathrm{Sym}(X)$ (cours). Ici si on cherche un exemple avec $|X| = 14$, on a donc $\mathrm{Sym}(X) \simeq \mathcal{S}_{14}$; on peut choisir comme morphisme par exemple celui défini par

$$\overline{1} \mapsto (1,2,3)(4,5,6),(7,8,9)(10,11,12,13,14),$$

qui correspond à la configuration de la question (4). On pourrait construire également facilement une action de G avec points fixes, comme celle définie par

$$\overline{1} \mapsto (1,2,3)(4,5,6,7,8),$$

qui a 6 points fixes. On peut montrer par des arguments semblables qu'il n'existe pas d'action de $\mathbb{Z}/15\,\mathbb{Z}$ sur un ensemble à 7 éléments.

Exercice 7

(1) On note déjà que l'action est bien définie, au sens où elle ne dépend pas du choix du représentant k de la classe $\overline{k}$: si k' est un autre représentant de cette classe, alors il existe $n \in \mathbb{Z}$ tel que $k' = k + np$, et donc $\sigma^{k'} = \sigma^{k+np} = \sigma^k$ car σ est d'ordre p.

Montrons que c'est bien une action de groupe.

— $\forall (x_1,\dots,x_p), \quad \overline{0} * (x_1,\dots,x_p) = (x_{\sigma^0(1)},\dots,x_{\sigma^0(p)}) = (x_1,\dots,x_p)$.

— $\forall (x_1,\dots,x_p), \forall \overline{k},\overline{l} \in \mathbb{Z}/p\,\mathbb{Z}, \quad \overline{k} * (\overline{l} * (x_1,\dots,x_p)) = \overline{k} * (x_{\sigma^l(1)},\dots,x_{\sigma^l(p)})$. On pose ensuite $y_i = x_{\sigma^l(i)}$ et on a $\overline{k} * (y_1,\dots,y_p) = (y_{\sigma^k(1)},\dots,y_{\sigma^k(p)}) = (x_{\sigma^l(\sigma^k(1))},\dots,x_{\sigma^l(\sigma^k(p))}) = (x_{\sigma^{k+l}(1)},\dots,x_{\sigma^{k+l}(p)}) = (\overline{k}+\overline{l}) * (x_1,\dots,x_p)$.

(2) D'après l'équation des classes le cardinal de chaque orbite divise le cardinal du groupe, p, et comme p est premier les seules possibilités sont 1 ou p. On note l le nombre d'orbites de cardinal 1 (et donc de points fixes), on a alors $k - l$ orbites de cardinal p par hypothèse. L'ensemble est la réunion disjointe des orbites donc on a l'égalité

$$|E^p| = n^p = l \times 1 + (k-l) \times p.$$

On va montrer que $l = n$. Considérons un point fixe $(x_1,\dots,x_p)$. Cela signifie que $\forall k, \forall i, \quad s_{\sigma^k(i)} = x_i$. D'après la formule explicite pour σ on a que $\sigma^k(i) \equiv i + k[p]$. On obtient alors l'égalité $x_i = x_j$ pour tous i et j. Ainsi la seule possibilité pour le point fixe est $(x,\dots,x)$. Il y en a n, d'où $l = n$ et on obtient la formule voulue.

(3) La formule précédente modulo p donne donc $n^p \equiv n[p]$.

Exercice 8

(1)

$$\begin{aligned} z \in Z(G) &\Leftrightarrow \forall g \in G,\ zg = gz \\ &\Leftrightarrow \forall g \in G,\ z = gzg^{-1} \\ &\Leftrightarrow \mathrm{Orb}(z) = \{z\}. \end{aligned}$$

(2) On note $|G| = p^s$. Les cardinaux possibles pour les orbites sont les p^k avec $k \leq s$ par l'équation des classes. Notons n_i le nombre d'orbites à i éléments. Comme l'ensemble G est la réunion disjointe des orbites, on a $|G| = p^s = \sum_{k=0}^{s} p^k n_{p^k}$. D'après la question

précédente $n_1 = |Z(G)|$. Le reste de la somme est divisible par p d'où il existe $M \in \mathbb{N}$ tel que $p^s = |Z(G)| + pM$, et en passant modulo p, $|Z(G)| \equiv 0[p]$. En particulier $Z(G)$ n'est pas réduit à l'élément neutre.

Exercice 9 (Formule de Burnside)

On note donc $X = \{(g, x) \in G \times E \mid g \cdot x = x\}$. Pour chaque g fixé dans G il y a exactement $|\mathrm{Fix}(g)|$ éléments $x \in E$ tels que $(g, x) \in X$. On a donc $|X| = \sum_{g \in G} |\mathrm{Fix(g)}|$.

D'autre part, à x fixé dans E, il y a $|\operatorname{Stab}(x)|$ éléments $g \in G$ tels que $(g, x) \in X$. On a donc $|X| = \sum_{x \in E} |\operatorname{Stab}(x)|$. D'après l'équation des classes, $|Stab(x)| = |G|/|\operatorname{Orb}(x)|$. On utilise ensuite que E est la réunion disjointe des orbites pour obtenir

$$|X| = \sum_{x \in E} \frac{|G|}{|\operatorname{Orb}(x)|} = \sum_{\mathcal{O} orbite} \sum_{x \in \mathcal{O}} \frac{|G|}{|\mathcal{O}|} = \sum_{\mathcal{O} orbite} |\mathcal{O}| \frac{|G|}{|\mathcal{O}|} = \sum_{\mathcal{O} orbite} |G| = r|G|.$$

La formule de Burnside s'en déduit directement.