Théorie des groupes

Correction contrôle continu 2

Exercice 1 Répondre par « vrai » ou « faux »à la question suivante. *Répondre « vrai » implique que vous donniez une preuve complète et valide de l'assertion ; répondre « faux » implique que vous donniez une preuve complète et valide de la négation de l'assertion proposée.*

Soit G un groupe abélien non trivial. Soit H_1, H_2, H_3 trois sous-groupes (distincts) non triviaux de G tels que $G = \sum_{i=1}^{3} H_i$. Alors $G = \oplus_{i=1}^{3} H_i$ si et seulement si $H_1 \cap H_2 \cap H_3 = (e_G)$.

Correction : Pour G n'importe quel groupe abélien non-trivial, $G \times G$ fournit un contre-exemple simple :
$H_1 =< (1,0) >\cong G$
$H_2 =< (0,1) >\cong G$
$H_3 =< (1,1) >\cong G$
Il est clair que $H_1 \cap H_2 \cap H_3 = \{e_G\}$, mais $G \times G \ncong G \times G \times G$.

C'est l'exemple bien connu : Trois droites de $\mathbb{R}^2$ qui se croisent en l'origine sont d'intersection triviale, mais ne sont pas en somme directe.

Exercice 2 Soit G un groupe d'ordre 77 agissant sur un ensemble X de cardinal 41. Montrer que l'action de G sur X admet forcément un point fixe.

Correction : Le cardinal de chaque orbite divise l'ordre du groupe. Elles peuvent donc être de taille 1,7,11 ou 77. Il est bien sur impossible d'avoir une orbite de taille 77 dans un ensemble de cardinal 41.

Supposons que l'action n'a pas de point fixe. C'est équivalent à dire qu'elle n'a pas d'orbite de taille 1. Notons x le nombre d'orbites de taille 7 et y le nombre d'orbites de taille 11.

Les orbites formant une partition de X, on a (formule des classes) : $7x + 11y = 41$.

En regardant cette égalité modulo 7, on obtient :

$$4y \equiv 6[7]$$

4 étant inversible dans $\mathbb{Z}/7\mathbb{Z}$ (car 7 est premier avec 4), d'inverse 2, cette congruence est équivalente à

$$y \equiv 5[7]$$

Et donc $y = 5 + 7k$ avec $k \in \mathbb{N}$. Donc $11y \geq 55$. Or on doit avoir $11y \leq 41$, donc ceci est absurde. Notre hypothèse de départ est donc fausse, et l'action admet au moins un point fixe.

Exercice 3 Soient $p < q$ deux nombres premiers tels que p ne divise pas $q-1$. Soit G d'ordre pq.

1. Montrer que G a un unique q-Sylow.
2. En déduire que $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes_\alpha \mathbb{Z}/p\mathbb{Z}$ où α est un morphisme de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$.
3. Montrer que G est abélien.

Correction :

1. Par théorème de Sylow, $n_q \equiv 1[q]$ et $n_q \mid p < q$, donc $n_q = 1$.
2. Soit P un p-Sylow. P est d'ordre p premier donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
   Q est d'ordre q premier donc isomorphe à $\mathbb{Z}/q\mathbb{Z}$.
   Par ordre des éléments, $P \cap Q = \{e\}$.
   Montrons que $QP = G$:
   -QP est un groupe : Soient $q, q' \in Q$ et $p, p' \in P$. $pq'^{-1}p^{-1} = q_0 \in Q$ car $Q \lhd G$.

Donc $qpq'^{-1}p'^{-1} = qpq'^{-1}p^{-1}pp'^{-1} = qq_0pp'^{-1} \in QP$. QP est donc un groupe.

-QP est un groupe contenant Q et P, donc de cardinal $> p$ et q. Comme $|PQ|$ divise $|G| = pq$, on doit avoir $|PQ| = |G|$ et donc $QP = G$.

Par théorème de produit semi-direct, $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes_\alpha \mathbb{Z}/p\mathbb{Z}$.

3. $\alpha : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$. Donc $ord(\alpha(1)) \mid p$ et $ord(\alpha(1)) = 1$ ou p.
   De plus, $\alpha(1) \mid |\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})|$.
   Comme q est premier, $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/q\mathbb{Z})^\star$, donc $|\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})| = q - 1$. p ne divise pas $q-1$ par hypothèse, donc $\alpha(1)$ est d'ordre 1, donc est trivial. Comme 1 génère $\mathbb{Z}/p\mathbb{Z}$, α est le morphisme trivial et le produit est direct.
   Donc G est abélien isomorphe à $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Exercice 4 Soit ϕ un automorphisme de $\mathfrak{S}_n$ qui transforme une transposition en une transposition.

1. Montrer qu'il existe 3 entiers de $[\![1, n]\!]$ distincts a_1, a_2, a_3 tels que $\phi((12)) = (a_1a_2)$ et $\phi((13)) = (a_1a_3)$.
2. Que vaut $\phi^{-1}((a_2a_3))$?
3. Montrer que pour $i \in [\![4, n]\!]$, il existe a_i tel que $\phi((1i)) = (a_1a_i)$.
4. Montrer que $s : i \mapsto a_i$ est bijective. Donc $s \in \mathfrak{S}_n$.
5. En déduire que ϕ est l'automorphisme intérieur conjuguant par s.

Culture : Tout automorphisme de $\mathfrak{S}_n$ transforme une transposition en transposition si et seulement si $n \neq 6$ (exercice de combinatoire). Pour $n \neq 6$, tous les automorphismes de $\mathfrak{S}_n$ sont donc intérieurs. Le cas $\mathfrak{S}_6$ est plus compliqué. En effet, $\mathrm{Int}(\mathfrak{S}_6)$ *est d'indice 2 dans* $\mathrm{Aut}(\mathfrak{S}_6)$.

Correction :

1. Par hypothèse, $\phi((12))$ et $\phi((13))$ sont des transpositions.
   Si $\phi((12))$ et $\phi((13))$ sont à supports disjoints elles commutent. Or (12) et (13) ne commutent pas. $(12)(13) = (132) \neq (123) = (13)(12)$. Donc $\phi((12))$ et $\phi((13))$ ne sont pas à supports disjoints. Comme ϕ est bijective $\phi((12))$ et $\phi((13))$ sont différentes. Donc leur support a exactement un élément en commun, noté a_1.
2. $\phi^{-1}((a_2a_3)) = \phi^{-1}((a_1a_2).(a_1a_3).(a_1a_2)) = (12)(13)(12) = (23)$.
3. Soit $i \in [\![4, n]\!]$.
   $\phi((12))$ et $\phi((1i))$ ne commutent pas (car images d'éléments ne commutant pas), donc ne sont pas à support disjoints. De même, $\phi((1i))$ et $\phi((13))$ ne sont pas à support disjoints.
   Si a_1 n'est pas dans le support de $\phi((1i))$, alors a_2 et a_3 y sont, et comme ϕ envoie une transposition sur une transposition, $\phi((1i)) = (a_2a_3)$ et par la question précédente, $(1i) = \phi^{-1}(\phi((1i))) = (23)$, ce qui est absurde. Donc a_1 est dans le support de $\phi((1i))$ et il existe donc a_4 tel que $\phi((1i)) = (a_1a_4)$.
4. Si $s(i) = s(j)$, alors $\phi((1i)) = \phi((1j))$. Comme ϕ est un automorphisme, $(1i) = (1j)$, et donc $i = j$.
   s est donc injective sur un ensemble fini, donc est bijective.
5. Soit $i \in [\![1, n]\!]$. On pose $\gamma = s \circ (1i) \circ s^{-1}$.
   $\gamma(a_1) = (s \circ (1i))(1) = s(i) = a_i$.
   De même, $\gamma(a_i) = a_1$.
   Si $j \neq 1, i$, alors $\gamma(j) = (s \circ (1i))(j) = s(j) = a_j$.
   Donc $\gamma = (a_1a_i)$. On a montré que ϕ et la conjugaison par s coïncident sur $\{(1i),\ \ i \in [\![1, n]\!]\}$, qui est un ensemble générant $\mathfrak{S}_n$, donc ϕ est la conjugaison par s.