Algèbre et Arithmétique 3

Feuille n°4 : groupes cycliques, groupes de permutations

Exercices à savoir faire chez soi

Exercice 1

1 Soit $\zeta = e^{\frac{18\,i\,\pi}{13}}$. Déterminer l'ordre de ζ et de ζ^3 dans $\mathbf{C}^\times$. Même question avec $\zeta = e^{\frac{4\,i\,\pi}{9}}$.

2 Sur le cercle unité, dessiner les éléments du groupes des racines 6-èmes de l'unité. Parmi ces éléments, marquer ceux qui sont d'ordre 6.

3 *Vrai ou faux ?* Une racine n-ème de l'unité est d'ordre n.

Exercice 2

Le groupe $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ est-il cyclique ? Et le groupe $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$? (regarder l'ordre de chacun des éléments et comparer à l'ordre du groupe ; pour le deuxième groupe, on peut aussi utiliser directement un résultat du cours...)

Exercice 3

Choisir un petit nombre premier p (disons inférieur à 20) et répondre aux questions suivantes : quels sont les ordres possibles des éléments du groupe $\mathbf{F}_p^\times$? Combien d'éléments de chaque ordre ce groupe possède-t-il ? Quels sont les éléments qui engendrent le groupe ? Recommencer avec un autre petit nombre premier...

Exercice 4

Écrire la table de multiplication de $\mathfrak{S}_3$ et vérifier que $\mathfrak{S}_3$ n'est pas commutatif.

Exercice 5

Soit σ la permutation $(1,2,3,4)(2,5)$. Déterminer σ^k pour tout $k \in \mathbf{Z}$. Quel est l'ordre de σ ?

Exercices à savoir faire

Exercice 6

Soit G un groupe, g_1 un élément d'ordre r_1 et g_2 un élément d'ordre r_2.

1 On suppose que g_1 et g_2 commutent. Montrer que $g_1\,g_2$ est d'ordre fini, et que son ordre divise $r_1\,r_2$.

2 On suppose dans cette question que g_1 et g_2 commutent et que r_1 et r_2 sont premiers entre eux. Soit n un entier vérifiant $(g_1\,g_2)^n = e$. Montrer qu'on a $g_1^{n\,r_2} = e$. Qu'en déduit-on sur n ? Montrer que $g_1\,g_2$ est d'ordre $r_1\,r_2$.

3 On suppose que g_1 et g_2 commutent. Montrer par un exemple que l'ordre de $g_1\,g_2$ n'est pas nécessairement $r_1\,r_2$, ni $\mathrm{ppcm}(r_1, r_2)$.

4 Un petit intermède « géométrique » : pour $z_0 \in \mathbf{C}$ et $\alpha \in \mathbf{U} = \{z \in \mathbf{C}, \quad |z| = 1\}$, on définit les applications

$$\rho_{z_0,\alpha} \;:\; z \mapsto \alpha(z - z_0) + z_0$$

et

$$\tau_{z_0} \; : \; z \mapsto z + z_0 .$$

Vérifier que $\rho_{z_0,\alpha}$ et τ_{z_0} sont des permutations de $\mathbf{C}$. Interprétation géométrique ? Montrer que

$$\{\rho_{z_0,\alpha}, \tau_{z_0}\}_{\substack{z_0 \in \mathbf{C},\\ \alpha \in \mathbf{U}}}$$

est un sous-groupe de $\mathfrak{S}_{\mathbf{C}}$. À quelle condition $\rho_{z_0,\alpha}$ (respectivement τ_{z_0}) est-il d'ordre fini ?

5 Montrer par un exemple que même si g_1 et g_2 sont d'ordre fini, $g_1\,g_2$ n'est pas nécessairement d'ordre fini (on pourra considérer par exemple des éléments du groupe de la question précédente).

Exercice 7

Soit $n \geqslant 3$ un entier. Montrer que $\mathfrak{S}_n$ n'est pas commutatif.

Exercice 8

1 Si $n \geqslant 4$, exhiber une permutation de $\mathfrak{S}_n$ qui est d'ordre 2 mais qui n'est pas une transposition.

2 Décrire les éléments d'ordre 2 de $\mathfrak{S}_n$ (on pourra considérer leur décomposition en cycles à supports disjoints).

Exercice 9

Soit $r \geqslant 2$ un entier et $d_1, \ldots, d_r$ des entiers deux à deux distincts. Vérifier soigneusement la relation

$$(d_1, d_2, \ldots, d_{r-1}, d_r) = (d_1, d_r)\,(d_1, d_{r-1}) \ldots (d_1, d_3)\,(d_1, d_2).$$

Exercice 10

1 Soit c un r-cycle et d un élément du support de c. Vérifier que le support de c est

$$\{c^k(d), \quad k \in \mathbf{Z}\} = \{c^k(d), \quad k \in \{0, \ldots, r-1\}\}.$$

2 Soit $\sigma \in \mathfrak{S}_n$ et r un entier strictement positif. Vérifier σ est d'ordre r si et seulement si on a

$$\forall d \in \{1, \ldots, n\}, \quad \sigma^r(d) = d$$

et

$$\forall k \in \{1, \ldots, r-1\}, \quad \exists d \in \{1, \ldots, n\}, \quad \sigma^k(d) \neq d.$$

En déduire que l'ordre d'un r-cycle est r.

3 Soit $c_1, \ldots, c_r$ des cycles dont les supports sont deux à deux disjoints et $\sigma = c_1\,c_2\,\ldots c_r$. Soit $i \in \{1, \ldots, r\}$. Vérifier que pour tout d dans le support de c_i, on a $c_i(d) = \sigma(d)$. En déduire que l'ordre de c_i divise l'ordre de σ, puis que l'ordre de σ est le ppcm des ordres des c_i.

4 La fin de cet exercice est consacré à la démonstration du fait que l'écriture d'une permutation comme produit de cycles à supports deux à deux disjoints est unique à l'ordre des facteurs près.

Soit $c'_1, \ldots, c'_s$ des cycles dont les supports sont deux à deux disjoints. On suppose qu'on a $c_1\,c_2\,\ldots c_r = c'_1\,c'_2 \ldots c'_s$. On veut montrer qu'on a $r = s$ et qu'à renumérotation éventuelle près, on a $c_i = c'_i$ pour tout i.

Soit d un élément du support de c_1. Vérifier que d est dans le support de l'un des c'_i. En renumérotant, on peut donc supposer que d est dans le support de c'_1.

5 Montrer que c_1 et c'_1 ont même support puis que $c'_1 = c_1$.

6 Conclure.

Exercice 11

Le but de cet exercice est de démontrer le résultat suivant, admis en cours : pour toute permutation σ et toute transposition τ, on a la relation $\varepsilon(\sigma\,\tau) = \varepsilon(\sigma)\,\varepsilon(\tau) = -\varepsilon(\sigma)$.

1 Soient r un entier supérieur à 2 et c un r-cycle. Soit τ une transposition telle que l'intersection du support de τ et du support de c est un singleton. Vérifier qu'on peut écrire $c = (d_1, d_2, \ldots, d_r)$ et $\tau = (d_1, d'_1)$, où $d_1, \ldots, d_r, d'_1$ sont $r+1$ entiers deux à deux distincts. Montrer que $c\tau$ est un $r+1$-cycle dont on déterminera le support.

2 Soient r un entier supérieur à 2 et c un r-cycle. Soit τ une transposition dont le support est inclus dans le support de c. Vérifier qu'on peut écrire $c = (d_1, d_2, \ldots, d_r)$ et $\tau = (d_1, d_i)$ où $d_1, \ldots, d_r$ sont r entiers deux à deux distincts et $i \in \{2, \ldots, r\}$. Montrer que $c\tau$ est un produit de deux cycles à supports disjoints, supports que l'on déterminera explicitement.

3 Soient r et s des entiers supérieurs à 2, c_1 un r-cycle et c_2 un s-cycle. On suppose les supports de c_1 et c_2 disjoints. Soit τ une transposition dont le support intersecte le support de c_1 *et* le support de c_2. Vérifier qu'on peut écrire $c_1 = (d_1, d_2, \ldots, d_r)$, $c_2 = (d'_1, \ldots, d'_s)$ et $\tau = (d_1, d'_1)$, où $d_1, \ldots, d_r, d'_1, \ldots, d'_s$ sont $r+s$ entiers deux à deux distincts. Montrer que $c_1\,c_2\,\tau$ est un $r+s$-cycle de support $\{d_1, \ldots, d_r, d'_1, \ldots, d'_s\}$.

4 Déduire des trois questions précédentes le résultat annoncé (on décomposera σ en produit de cycles à supports disjoints et on considèrera l'intersection du support de ces cycles avec le support de τ).

Exercice 12

Soit k un corps et P, Q des éléments de $k[X]$. Rappeler les formules vues en cours reliant le degré de $P + Q$ (respectivement de $P\,Q$) aux degrés de P et Q, puis les démontrer.

Exercices à chercher

Exercice 13

Soit E et F des ensembles et $f : E \to F$ une bijection. Montrer que l'application qui à $\sigma \in \mathfrak{S}_E$ associe $f \circ \sigma \circ f^{-1}$ induit un isomorphisme du groupe $\mathfrak{S}_E$ sur le groupe $\mathfrak{S}_F$.

Exercice 14

Soit $n \geqslant 2$ un entier. À tout élément σ de $\mathfrak{S}_{n-1}$ on associe l'application de $\mathbf{N}_n$ dans $\mathbf{N}_n$ qui à n associe n et à tout élément $i \in \{1, \ldots, n-1\}$ associe $\sigma(i)$. Cette application est notée $\varphi(\sigma)$. Montrer que $\varphi(\sigma)$ est un élément de $\mathfrak{S}_n$, puis que φ est un morphisme injectif du groupe $\mathfrak{S}_{n-1}$ vers le groupe $\mathfrak{S}_n$, dont l'image est le sous-groupe de $\mathfrak{S}_n$ constitué des permutations dont n est un point fixe.

Exercice 15

Soit $\sigma \in \mathfrak{S}_n$.

1 Soit

$$\iota(\sigma) = \#\{(i,j) \in \mathbf{N}_n, \quad 1 \leqslant i < j \leqslant n, \quad \sigma(i) > \sigma(j)\}.$$

$\iota(\sigma)$ est appelé le « nombre d'inversions » de σ. Montrer la formule

$$\varepsilon(\sigma) = (-1)^{\iota(\sigma)}.$$

2 Montrer la formule

$$\varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

3 En déduire une nouvelle démonstration du fait que ε est un morphisme de groupes.

Exercice 16

Soit $n \geqslant 1$ un entier et E un espace vectoriel de base $(e_1, \ldots, e_n)$. Soit σ un élément de $\mathfrak{S}_n$. Soit f_σ l'application linéaire $E \to E$ définie par $f_\sigma(e_i) = e_{\sigma(i)}$.

1 Montrer que f_σ est un élément de $\mathrm{GL}(E)$, puis que $\sigma \mapsto f_\sigma$ est un morphisme de $\mathfrak{S}_n$ vers $\mathrm{GL}(E)$.

2 Montrer qu'on a $\det(f_\sigma) = \varepsilon(\sigma)$.