Feuille d'exercices 1

Notion de groupe. Le groupe symétrique.

Exercice 1. Déterminer lesquelles des opérations suivantes sont associatives et/ou commutatives :

- l'opération $*$ sur $\mathbf{Z}$ définie par $a * b = a + b + ab$;
- l'opération $*$ sur $\mathbf{Q}$ définie par $a * b = (a + b)/5$;
- l'opération $*$ sur $\mathbf{Z} \times \mathbf{Z}$ définie par $(a, b) * (c, d) = (ad + bc, bd)$;
- l'opération $*$ sur $\mathbf{R}$ définie par $a * b = \max(a, b)$.

Exercice 2. Est-ce un groupe ? Si oui, est-il abélien ?

- $(\mathbf{R}, +)$, $(\mathbf{R}, \cdot)$.
  Quid de $(\mathbf{K}, +)$ et $(\mathbf{K}, \cdot)$ où $\mathbf{K}$ est un corps quelconque ($\mathbf{R}$, $\mathbf{C}$, $\mathbf{Q}$) ?
- $(\mathbf{R}^\star, \cdot)$, $(\mathbf{R}^\star, +)$, où $\mathbf{R}^\star = \mathbf{R} \setminus \{0\}$.
  Quid de $(\mathbf{K}^\star, \cdot)$, $(\mathbf{K}^\star, +)$ pour un corps $\mathbf{K}$ quelconque ?
- $(\mathbf{R}^{>0}, \cdot)$, $(\mathbf{R}^{>0}, +)$.
- $(\mathbf{U}, +)$, $(\mathbf{U}, \cdot)$, où $\mathbf{U} = \{z \in \mathbf{C} : |z| = 1\}$.
- $(\mathbf{U}_n, \cdot)$, où $\mathbf{U}_n = \{z \in \mathbf{C} : z^n = 1\}$, c'est l'ensemble des *racines n-ièmes* de l'unité.
- $(\mathbf{Z}, +)$, $(\mathbf{Z}, \cdot)$, $(\mathbf{Z}^\star, \cdot)$?
- $(\mathbf{Z}/n\mathbf{Z}, +)$, $(\mathbf{Z}/n\mathbf{Z}, \cdot)$.
- $(\mathbf{R}, *)$ avec l'opération $a * b = \max(a, b)$.
- Notons par $M(n, \mathbf{R})$, l'ensemble des matrices $n \times n$ à coordonnées réelles. Muni de l'addition de matrices, est-ce un groupe ? Et muni de la multiplication ?
- Notons par $\mathrm{GL}(n, \mathbf{R})$ l'ensemble des matrices $n \times n$ *inversibles* à coordonnées réelles. Muni de l'addition de matrices, est-ce un groupe ? Et muni de la multiplication ?

Dans la suite, sauf mention contraire explicite, nous utiliserons toujours la notation multiplicative.

Exercice 3. Soient G_1 et G_2 deux groupes.

(a) Montrer que l'ensemble $G_1 \times G_2$ muni de la loi de composition

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 g_1', g_2 g_2')$$

est un groupe. On l'appelle le *produit direct* des groupes G_1 et G_2.

(b) Montrer que le produit direct $G_1 \times G_2$ est abélien si et seulement si les groupes G_1 et G_2 le sont.

Exercice 4. (a) Montrer qu'il existe un seul groupe à un élément. Il s'appelle le *groupe trivial*.

(b) Dresser la liste des tables de multiplication possibles pour un groupe à deux éléments $\{e, x\}$ (où e sera le neutre, et $x \neq e$).

(c) Pareil, pour un groupe à trois élément $\{e, x, y\}$.

(d) Et pour quatre éléments ?

Exercice 5 (Loi associative généralisée)**.** Soit G un groupe et soient $x_1, \ldots, x_k \in G$. Montrer que dans l'expression

$$x_1 \cdot x_2 \cdots x_k$$

l'ordre dans lequel on fait les multiplications n'est pas important et le résultat est toujours le même. (*Indication* : induction sur k.)

Exercice 6. Soit G un groupe. Montrer que pour tout $x, y \in G$:

$$e^{-1} = e \qquad (xy)^{-1} = y^{-1}x^{-1}, \qquad (x^{-1})^{-1} = x.$$

Énoncer les identités analogues en notation additive. A-t-on besoin de les démontrer elles aussi ?

Exercice 7. Soit G un groupe et $x, y, z \in G$. Alors :

$$x = y \iff zx = zy \iff xz = yz \iff x^{-1} = y^{-1}.$$

En déduire que les applications suivantes sont des bijections de G avec lui-même :

- La *translation à gauche* par z : $x \mapsto zx$.
- La *translation à droite* par z : $x \mapsto xz$.
- L'inverse : $x \mapsto x^{-1}$.

Exercice 8. Soit G un groupe.

On rappelle que pour $x \in G$ et $n \in \mathbf{N}$, on définit x^n par récurrence : $x^0 = e$ et $x^{n+1} = x^n x$. Puisque x^{-1} est déjà défini (c'est l'inverse !), nous définissons pour $n \geq 2$: $x^{-n} = (x^n)^{-1}$. Ceci définit x^n pour tout $n \in \mathbf{Z}$.

Montrer que pour tout $x \in G$ et $n, m \in \mathbf{Z}$:

$$x^{-n} = (x^n)^{-1}, \qquad x^{m+n} = x^m x^n, \qquad x^{mn} = (x^m)^n.$$

Attention : pour certaines identités il y a plusieurs cas à considérer, selon si m, n (et $m+n$) sont positifs, négatifs, ou nuls.

Traduire ces identités à la notation additive.

Exercice 9. Montrer qu'un groupe G dont tous les éléments x vérifient $x^2 = e$ est abélien.

Exercice 10. Soit G un groupe fini. Montrer qu'il existe un entier $N \geq 1$ tel que, pour tout $x \in G$, $x^N = e$.

Exercice 11. Soit G le groupe $(\mathbf{Z}/12\mathbf{Z}, +)$. Calculer les ordres de tous les éléments de G.

Exercice 12. Soit G un groupe, $x \in G$, et $n \in \mathbf{N}^\star$.

(a) Soit $m = \mathrm{ord}(x)$ et supposons que $m < \infty$. Montrer que $x^n = e \iff m \mid n$.

(b) Montrer que $\mathrm{ord}(x) = \mathrm{ord}(x^{-1})$.

(c) Si $\mathrm{ord}(x) = \infty$, alors $\mathrm{ord}(x^n) = \infty$.

(d) Si $\mathrm{ord}(x) = m < \infty$, alors $\mathrm{ord}(x^n) = m/\operatorname{pgcd}(m, n) = \operatorname{ppcm}(m, n)/n$.

Exercice 13. Pour $n \in \mathbf{N}^\star$, soit $\varphi(n)$ le nombre des entiers $0 \leq m < n$ qui sont premiers avec n. Ceci définit une fonction $\varphi : \mathbf{N}^\star \to \mathbf{N}^\star$ appelée l'*indicatrice d'Euler*.

On fixe $n \in \mathbf{N}^\star$, et on se rappelle que $G = (\mathbf{Z}/n\mathbf{Z}, +)$ est un groupe additif.

(a) À l'aide de lexercice précédent, montrer que l'ordre de tout membre de G est un diviseur de n (c'est un cas particulier d'un théorème bien plus général).

(b) Montrer que G possède exactement $\varphi(n)$ membres d'ordre n – lesquels ?

(c) Plus généralement, si $d \mid n$, montrer que G possède exactement $\varphi(d)$ membres d'ordre d – lesquels ?

(d) En déduire l'identité suivante :

$$n = \sum_{d|n} \varphi(d).$$

Exercice 14. Montrer que si X est fini alors $|S_X| = |X|!$ (factorielle de $|X|$). En particulier, $|S_n| = n!$

Ceci est valable aussi lorsque X est vide, ou lorsque $n = 0$, avec la convention que $0! = 1$ (c'est l'unique valeur possible, pour que l'identité $(n+1)! = n! \cdot (n+1)$ soit valable aussi pour $n = 0$).

Exercice 15. Soit X un ensemble.

(a) Montrer que la composition de deux permutations de X est encore une permutation de X.

(b) Montrer que la composition de permutations est associative (pour tout dire, c'est vrai pour n'importe quel composition d'applications, dès lors qu'elle est bien définie !)

(c) Montrer que l'application identité id_X est neutre (à gauche, ou des deux côtés, comme il vous plaît) pour la composition de permutations.

(d) Montrer que pour toute permutation $\sigma \in S_X$ il existe une permutation $\sigma' \in S_X$ qui est sont inverse pour la loi de composition (à gauche ou des deux côtés, encore).

(e) Montrer que S_X, muni de la loi de composition, est un groupe.

Exercice 16. Un cycle $\sigma = (x_1\ x_2\ \ldots\ x_m)$ est toujours une permutation, et on a $\sigma^k(x_i) = x_j$ si et seulement si $j \equiv i + k \mod m$.

Exercice 17. Soit $\sigma \in S_X$. Alors

(a) $\mathrm{supp}(\sigma^n) \subseteq \mathrm{supp}(\sigma)$ pour tout $n \in \mathbf{Z}$.

(b) $\mathrm{supp}(\sigma) = \mathrm{supp}(\sigma^{-1})$.

(c) $\sigma = e$ si et seulement si $\mathrm{supp}(\sigma)$ est vide.

(d) Si $x \in \mathrm{supp}(\sigma)$ alors $\sigma(x) \in \mathrm{supp}(\sigma)$, d'où $\sigma^n(x) \in \mathrm{supp}(\sigma)$ pour tout $n \in \mathbf{N}$ (voire $n \in \mathbf{Z}$).

(e) Le cardinal de $\mathrm{supp}(\sigma)$ n'est jamais égal à un.

Exercice 18. (a) Calculer la décomposition en cycles et les ordres de tous les éléments de S_3.

(b) Soient σ et τ les permutations suivantes dans S_8 :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 7 & 6 & 5 & 1 & 8 & 3 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 8 & 6 & 7 & 4 & 3 & 5 \end{pmatrix}.$$

Trouver les décompositions en cycles disjoints des permutations suivantes : $\sigma, \sigma^{-1}, \tau, \sigma^2, \sigma\tau$.

(c) Soit $\sigma = (1\ 2\ 3)(4\ 5)(6\ 7\ 8\ 9\ 10) \in S_{10}$. Calculer σ^{100}.

Exercice 19. (a) Démonter qu'un élément de S_n est d'ordre 2 si et seulement s'il est le produit de transpositions disjointes.

(b) Soit p un nombre premier. Montrer qu'un élément de S_n est d'ordre p si et seulement s'il est le produit de cycles disjoints d'ordre p. Montrer en donnant un exemple que ce n'est pas forcément le cas si p n'est pas premier.

Exercice 20. L'ordre d'un m-cycle est m. Plus généralement, si σ est le produit de k cycles disjoints de longueurs $m_1, \ldots, m_k$, alors $\mathrm{ord}(\sigma) = \mathrm{ppcm}(m_1, \ldots, m_k)$.

Donner un exemple où c'est faux lorsque les cycles ne sont pas disjoints (il en existe un dans S_3).