Feuille d'exercices 2

Sous-groupes

Exercice 1. Montrer que

(a) $(\mathbf{R}^{>0}, \cdot)$ est un sous-groupe de $(\mathbf{R}^{\times}, \cdot)$.

(b) $(\mathbf{Z}, +)$ est un sous-groupe de $(\mathbf{R}, +)$.

(c) $(n\mathbf{Z}, +)$ est un sous-groupe de $(\mathbf{Z}, +)$ et de $(\mathbf{R}, +)$.

Pourquoi $(\mathbf{R}^{>0}, \cdot)$ n'est pas un sous-groupe de $(\mathbf{R}, +)$?

Exercice 2. (a) Démontrer qu'une partie $K \subseteq \mathbf{Z}$ est un sous-groupe de $(\mathbf{Z}, +)$ si et seulement s'il existe $d \in \mathbf{N}$ tel que $K = d\mathbf{Z}$. De surcroît, d est unique.

(b) Soit $a, b \in \mathbf{N}$. Vérifier que la partie

$$a\mathbf{Z} + b\mathbf{Z} = \{ka + \ell b : k, \ell \in \mathbf{Z}\}$$

est un sous-groupe de $(\mathbf{Z}, +)$. Soit $c, d \in \mathbf{N}$ tels que

$$a\mathbf{Z} + b\mathbf{Z} = c\mathbf{Z}, \qquad a\mathbf{Z} \cap b\mathbf{Z} = d\mathbf{Z}.$$

Que peut-on dire de c et de d ?

Exercice 3. (a) D'après le théorème de Lagrange, quels sont les ordres possibles des sous-groupes de S_3 ?

(b) Dresser la liste de tous les sous-groupes de S_3.

(c) Montrer que ceci est une sous-groupe de S_4 :

$$H = \big\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\big\}.$$

Exercice 4. (a) Soit $c = (i_1\ i_2\ \dots\ i_k) \in S_n$ un k-cycle. Montrer que $c = (i_1\ i_2)(i_2\ i_3)\cdots(i_{k-1}\ i_k)$.

(b) Montrer que toute permutation $\sigma \in S_n$ est un produit de transpositions de la forme $(i\ j)$, avec $i < j$ dans $\{1, \dots, n\}$.

(c) Montrer que pour tout $i, j \in \{1, \dots, n\}$ vérifiant $i < j - 1$, on a $(i\ j) = (j-1\ \ j)(i\ \ j-1)(j-1\ \ j)$. En déduire que le groupe S_n est engendré par les transpositions $(i\ \ i+1)$ avec $1 \leqslant i \leqslant n-1$.

(d) Montrer que S_n est engendré par deux éléments : le cycle $(1\ 2\ \dots n)$ et la transposition $(1\ 2)$.

Exercice 5. On rappelle qu'on a défini le groupe diédral D_{2n} comme le sous-groupe de S_n qui préserve la relation R_n donnée par

$$i\ R_n\ j \iff |i - j| = 1 \text{ ou } (i = n \text{ et } j = 1) \text{ ou } (i = 1 \text{ et } j = n).$$

Le groupe D_{2n} est engendré par la rotation $r = (1\ 2 \cdots n)$ et la symétrie axiale $s = (2\ n)(3\ n-1)\cdots$; r est d'ordre n et s est d'ordre 2. Enfin

$$D_{2n} = \{s^i r^j : i = 0, 1; j = 0, \dots, n-1\}$$

et tous les éléments dans cette liste sont distincts ($|D_{2n}| = 2n$).

(a) Montrer la relation $rs = sr^{-1}$.

(b) Montrer que tout élément qui n'est pas une rotation (puissance de r) est d'ordre 2. En conclure que D_{2n} est engendré par deux éléments : s et sr, tous les deux d'ordre 2.

Exercice 6. Soit G le groupe de symétries d'un cube. Montrer que $|G| = 48$ et que G n'est pas abélien.

Exercice 7. On a vu en cours que les groupes $(\mathbf{R}, +)$ et $(\mathbf{R}^{>0}, \times)$ sont isomorphes. Montrer que :

(a) $(\mathbf{R}, +) \ncong (\mathbf{R}^*, \times)$.

(b) $(\mathbf{C}, +) \ncong (\mathbf{C}^*, \times)$.

(c) $(\mathbf{Q}, +) \ncong (\mathbf{Q}^{>0}, \times)$.

(d) $(\mathbf{R}^*, \times) \cong (\mathbf{R}^{>0}, \times) \times \mathbf{U}_2$.

Exercice 8. La relation $H \leq G$ est un ordre partiel sur les groupes. Autrement dit, cette relation est :

- *Réflexive :* $G \leq G$
- *Antisymétrique :* $H \leq G$ et $G \leq H$ implique $G = H$ (*en tant que groupes !*)
- *Transitive :* Si $K \leq H$ et $H \leq G$ alors $K \leq G$

Exercice 9. Soit G un groupe et $H, K \leq G$ deux sous-groupes.

(a) Rappeler pourquoi $H \cap K \leq G$.

(b) Montrer que $HK \leq G$ si et seulement si $HK = KH$.

(c) Trouver une condition nécessaire et suffisante pour que $H \cup K \leq G$.
Indication : si $x \in H \setminus K$ et $y \in K \setminus H$, que peut-on dire de xy ?

Exercice 10. Soit G un groupe et $x \in G$. Le *centralisateur de x dans G*, noté $C_G(x)$, est l'ensemble des éléments de G qui commutent avec x :

$$C_G(x) = \{y \in G : xy = yx\}.$$

Le *centre* de G, noté $Z(G)$, est défini par

$$Z(G) = \bigcap_{x \in G} C_G(x).$$

Montrer que $C_G(x)$ et $Z(G)$ sont des sous-groupes de G et que $Z(G)$ est abélien.

Exercice 11. Soit G un groupe et $x \in G$.

(a) Montrer que $x \in Z(G)$ si et seulement si $C_G(x) = G$.

(b) Montrer que G est abélien si et seulement si $Z(G) = G$.

Exercice 12. Soit G un groupe, $H \leq G$ et $K = C_G(H)$. Montrer que $H \leq C_G(K)$.

Exercice 13. Soit G un groupe non trivial et $x \in G$. Montrer que $C_G(x)$ n'est jamais trivial.

Exercice 14. Soit $G = S_3$. Calculer $C_G(\sigma)$ pour chaque $\sigma \in G$, ainsi que $Z(G)$.
Pouvez-vous calculer $Z(S_n)$ pour tout $n \in \mathbf{N}$?

Exercice 15. Soit G un groupe et $A \subseteq G$ une partie de G. Le *normalisateur de A dans G*, noté $N_G(A)$, est défini par

$$N_G(A) = \{x \in G : xAx^{-1} = A\}.$$

(a) Montrer que le normalisateur $N_G(A)$ est un sous-groupe de G.

(b) Montrer que si $H \leq G$, alors $H \leq N_G(H)$.

Exercice 16. (a) Quelles sont les classes à gauche de $(\mathbf{R}\setminus\{0\},\cdot)$ modulo $(\mathbf{R}^{>0},\cdot)$? À droite ?

(b) Quelles sont les classes de $(\mathbf{Z},+)$ modulo $(n\mathbf{Z},+)$?

Exercice 17. Soit $H=\{e,(1\,2)\}\subseteq S_3$.

(a) Montrer que $H\leq S_3$.

(b) Montrer que $S_3/H\neq H\setminus S_3$.

(c) Montrer que $|S_3/H|=|H\setminus S_3|$ en les calculant explicitement.

Exercice 18. On note par $(\mathbf{Z}/n\mathbf{Z})^\times$ l'ensemble des éléments de $\mathbf{Z}/n\mathbf{Z}$ inversibles pour la multiplication. Montrer que :

(a) Pour $\bar{k}\in\mathbf{Z}/n\mathbf{Z}$, $\bar{k}\in(\mathbf{Z}/n\mathbf{Z})^\times$ ssi $\operatorname{pgcd}(k,n)=1$. En particulier, $|(\mathbf{Z}/n\mathbf{Z})^\times|=\phi(n)$, où ϕ est l'indicatrice d'Euler.

(b) $((\mathbf{Z}/n\mathbf{Z})^\times,\cdot)$ est un groupe avec identité $\bar{1}$.

(c) Appliquer le théorème de Lagrange pour déduire le théorème d'Euler : pour tout $n\geq 2$ et $a\in\mathbf{N}$, si $\operatorname{pgcd}(a,n)=1$, alors $a^{\phi(n)-1}\equiv 1 \mod n$.

(d) En déduire le petit théorème de Fermat : si p est premier et $a\in\mathbf{N}$, alors $a^p\equiv a \mod p$.

Exercice 19. Soit G un groupe fini, d'ordre n. Supposons que pour chaque d, G possède au plus d membres dont l'ordre divise d. Montrer que G est cyclique.

Pour cela, vous pouvez suivre les étapes suivantes :

(a) Soit $x\in G$, disons $\operatorname{ord}(x)=d$. Montrer que

$$\langle x\rangle=\{y\in G:\operatorname{ord}(y)\mid d\}.$$

(b) Pour chaque d, soit

$$\alpha(d)=|\{x\in G:\operatorname{ord}(x)=d\}|.$$

Montrer que si $\alpha(d)>0$ alors $d\mid n$ et $\alpha(d)=\varphi(d)$, où φ est lindicatrice d'Euler que nous avons étudiée dans la fiche précédente.

(c) Conclure, en comparant les deux sommes $\sum_{d|n}\alpha(d)$ et $\sum_{d|n}\varphi(d)$.

Exercice 20. À l'aide de l'exercice précédent, montrer que si K est un corps et si $G\leq K^\times$ est un sous-groupe fini, alors G est cyclique.

Exercice 21. Montrer que pour p premier, $((\mathbf{Z}/p\mathbf{Z})^\times,\cdot)\cong\big(\mathbf{Z}/(p-1)\mathbf{Z},+\big)$.