Université Claude Bernard - Lyon 1 Semestre d'automne 2019-2020

L3 - Algèbre et Mathématiques Discrètes

Feuille d'exercices n° 3

Groupes

---

1 Généralités

1.1 Exemples et non-exemples

Soit X un ensemble, on note $\mathcal{F}_X$ l'ensemble des fonctions de X dans X et $\mathcal{S}_X$ l'ensemble des bijections de X sur X.

1. On fixe une partie A de X. Quels sont les groupes dans la liste suivante (l'opération est la composition) ?

$$\text{(i)} \quad \mathcal{F}_X; \qquad \text{(ii)} \quad \mathcal{S}_X; \qquad \text{(iii)} \quad \{\sigma \in \mathcal{S}_X,\ \sigma(A) \subset A\}; \qquad \text{(iv)} \quad \{\sigma \in \mathcal{S}_X,\ \sigma(A) = A\}.$$

2. Ici, on prend $X = \mathbb{R}^n$ pour n entier naturel. Même question avec :

$$\text{(v)} \quad \{\sigma \in \mathcal{S}_{\mathbb{R}^n},\ \sigma \text{ isométrie}\}; \qquad \text{(vi)} \quad \{\sigma \in \mathcal{F}_{\mathbb{R}^n},\ \sigma \text{ linéaire et } \det(\sigma) \geq 0\}.$$

3. Soit n un entier, $n \geq 2$. Est-ce que $(\mathbb{Z}/n\mathbb{Z} \setminus \{0\}, \cdot)$ est un groupe ?

4. Les ensembles suivants, munis du produit matriciels, sont-ils des groupes ?

$$\text{(viii)} \quad \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} :\ a, b, c, d \in \mathbb{R}^{+*} \right\}; \qquad \text{(ix)} \quad \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} :\ a, b, c, d \in \mathbb{R} \text{ et } ad - bc > 0 \right\}.$$

1.2 Racines de l'unité

Pour $n \in \mathbb{N}^*$, on note $\mu_n = \{z \in \mathbb{C}^*,\ z^n = 1\}$. Montrer que μ_n est un groupe d'ordre n.

1.3 $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}^*$.

1. Vérifier que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien de cardinal n.
2. Vérifier que $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ est un monoïde commutatif. Est-ce un groupe ? (Justifier).
3. Soit $m \in \mathbb{N}$. Montrer que les propriétés suivantes sont équivalentes :
   a) $(m, n) = 1$;
   b) $\overline{m}$ engendre le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$;
   c) $\overline{m}$ est inversible dans $(\mathbb{Z}/n\mathbb{Z}, \cdot)$.
4. En déduire que $((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$ est un groupe abélien de cardinal $\varphi(n)$ (la fonction d'Euler, dont la valeur est le nombre d'entiers relativement premiers à n, entre 1 et $n - 1$.

1.4

Soit I et J les deux matrices suivantes de $\mathrm{GL}_2(\mathbb{C})$:

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

1. Dresser la table de multiplication du sous groupe $Q = \langle I, J \rangle$ de $\mathrm{GL}_2(\mathbb{C})$.
2. Calculer l'ordre de tout élément de Q.
3. Calculer les sous-groupes de Q.
4. Calculer le centre de Q.
5. Existe-t-il un élément $a \in Q$ tel que $Q = \langle a \rangle$?

1.5 Groupe symétrique

On considère les transpositions adjacentes du groupe symétriques S_4 suivantes :

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = 2134, \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = 1324 \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = 1243.$$

On considère les sous-groupes

$$H = \langle \tau_1, \tau_2 \rangle; \quad K = \langle \tau_2, \tau_3 \rangle; \quad L = \langle \tau_1, \tau_3 \rangle.$$

1. Quels sont les ordres de H, K et L ?
2. Écrire la table de multiplication de ces sous-groupes. Sont-ils abéliens ?
3. Que remarquez-vous ?

2 Sous-groupes, morphismes

2.1 Intersection et réunion de sous-groupes

1. L'intersection d'une famille non vide quelconque de sous-groupes de G est un sous-groupe.
2. Soient H et K deux sous-groupes d'un groupe G. Démontrer que $H \cup K$ est un sous-groupe si et seulement si $H \subset K$ ou $K \subset H$.

2.2 Morphismes

Soient $\theta : G \to G'$ et $\psi : G' \to G''$ deux morphismes de groupes. Montrez que :

1. $\theta(e) = e'$;
2. $\theta(x^{-1}) = \theta(x)^{-1}$;
3. $H \leq G$ implique $\theta(H) \leq G'$;
4. $H' \leq G'$ implique $\theta^{-1}(H') \leq G$, où $\theta^{-1}(H') = \{x \in G \mid \theta(x) \in H'\}$;
5. $\phi \circ \theta : G \to G''$ est un morphisme de groupes ;
6. $\theta(\langle S \rangle) = \langle \theta(S) \rangle$, pour tout $S \subseteq G$;
7. $\mathrm{ord}(\theta(x))$ divise à la fois $\mathrm{ord}(x)$ et $|Im(\theta)|$, pour tout $x \in G$.

2.3 Isomorphisme de groupes

1. Est-ce que $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ et $(\mathbb{Z}_4, +)$ sont deux groupes isomorphes ?
2. Montrer que les groupes additifs suivants sont deux à deux non isomorphes :

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_8.$$

2.4

Montrer que les groupes $(\mathbb{R}, +)$, $(\mathbb{R}^*, \times)$, $(\mathbb{Z}^{\mathbb{N}}, +)$, $\big((\mathbb{Z}/n\mathbb{Z})^{\mathbb{N}}, +\big)$ (où $n \geq 2$) sont deux à deux non isomorphes. Montrer que $(\mathbb{R}, +)$ et $(\mathbb{R}^{+*}, \times)$ sont isomorphes.

2.5

Soit G un groupe noté multiplicativement. À quelle condition l'application $\phi : G \to G$, $x \to x^{-1}$ est-elle un morphisme ?

2.6

Soient G et G' deux groupes finis tels que $\mathrm{PGCD}(|G|, |G'|) = 2$. Montrez que s'il existe un morphisme $\theta : G \to G'$ tel que $\mathrm{Ker}(\theta) \neq G$, alors G admet un sous-groupe d'indice 2.

2.7 Sous-groupe engendré

Soit G un groupe (noté multiplicativement) et soit X une partie de G. L'intersection de tous les sous-groupes de G qui contiennent est un sous-groupe (pourquoi est-elle non vide ?). On note $\langle X \rangle$ ce sous-groupe.

1. Vérifie que si H est un sous-groupe de G qui contient X, alors $\langle X \rangle \subset H$.
2. Supposons que $X = \{g\}$. Vérifier que $\langle X \rangle = \{g^k,\ k \in \mathbb{Z}\}$. Pour $n \in \mathbb{N}$, quels sont les éléments g de μ_n qui engendrent μ_n ? Même question avec $\mathbb{Z}/n\mathbb{Z}$.
3. Comment décrire le groupe engendré par un élément dans un groupe noté additivement ? Décrire $\langle X \rangle$ lorsque G est le groupe additif $\mathbb{R}$ et $X = \{1, \sqrt{2}\} \subset \mathbb{R}$.
4. À nouveau, $G = \mathbb{R}$. Soient a et b deux rationnels. Montrer que $\langle \{a, b\} \rangle = \{k/m,\ k \in \mathbb{Z}\}$, où m est le ppcm des dénominateurs de a et b (écrits sous forme irréductible) et k le pgcd.

2.8 Ordre d'un élément

Soit G groupe (noté multiplicativement) de neutre e. L'ordre d'un élément g est, s'il existe, le plus petit entier naturel non nul n tel que $g^n = e$; si $g^k \neq e$ pour tout $k \in \mathbb{N}^*$, on dit que g est d'ordre infini.

1. Vérifier que le seul élément d'ordre 1 est e.
2. Soit g un élément de G. Montrer que $\langle g \rangle$ est isomorphe à μ_n ou à $\mathbb{Z}$, selon que l'ordre n de g est fini ou infini.
3. Soit g un élément d'ordre n et soit $k \in \mathbb{Z}$. Montrer que $g^k = e$ si et seulement si n divise k.
4. Exprimer l'ordre de g^k en fonction de k et de l'ordre de g.

2.9 Groupes cycliques

1. Montrer qu'un groupe d'ordre premier est cyclique.
2. Étant donnés deux groupes G_1 et G_2, montrer que $G_1 \times G_2$ est cyclique si et seulement si G_1 et G_2 le sont et $\mathrm{PGCD}(|G_1|, |G_2|) = 1$.
3. Pour G cyclique d'ordre n et $d|n$, montrer que G admet un unique sous-groupe d'ordre d et que ce sous-groupe est cyclique. Combien G a-t-il d'éléments d'ordre d ?

2.10 Théorème de Lagrange

1. Soit G un groupe tel que tout élément $x \neq e$ a ordre 2. Montrez que G est abélien.
2. Soit G un groupe d'ordre 10. Montrez qu'il possède un élément d'ordre 5.
3. Soit G un groupe qui a un sous-groupe d'ordre 4 et un d'ordre 10. Sachant que l'ordre de G est plus petit que 50, en déduire les ordres possibles de G.

2.11 Groupe quotient

Soit $G = \{\frac{m}{n} \in \mathbb{Q} \mid \mathrm{PGCD}(m, n) = 1 \text{ et } n \text{ divise } 12\}$

1. Montrez que G est un sous groupe de $(Q, +)$.
2. Calculez l'ordre du groupe quotient $G/\mathbb{Z}$ et prouvez que $G/\mathbb{Z}$ est un groupe cyclique.
3. Calculer l'ordre du groupe quotient $G/\mathbb{Z}_3$.

2.12 Automorphismes intérieurs

Soit G un groupe. Pour tout $h \in G$, on note $\mathrm{Ad}_h : G \to G$, $g \mapsto hgh^{-1}$. C'est l'application de *conjugaison par* h.

1. Vérifier que l'application $\mathrm{Ad}_h : G \to G$, $g \mapsto hgh^{-1}$ est un automorphisme de G. Vérifier aussi que $\mathrm{Ad}_h = \mathrm{Id}_G$ si et seulement si pour tout g de G, h et g commutent.
2. Montrer que $\mathrm{Ad} : G \to aut(G)$, $h \mapsto \mathrm{Ad}_h$ est un morphisme. Quel est son noyau ?
3. Soit h un élément de G et soit θ un automorphisme de G. Calculer $\theta \circ \mathrm{Ad}_h \circ \theta^{-1}$.

2.13 Matrices inversibles à coefficients dans $\mathbb{Z}/n\mathbb{Z}$

Soit $G = (GL_3(3), \cdot)$ le groupe des matrices inversibles de taille 3 à coefficients dans $\mathbb{Z}/3\mathbb{Z}$.

1. Quel est l'ordre de G ?
2. Soit $T_3(3) = \{A \in G \mid a_{ij} = 0, \forall i, j,\ i > j\}$. Montrez qu'il est un sous-groupe de G. Quel est son ordre ? Quel est l'ordre de ses éléments ?
3. Soit $D_3(3) = \{A \in G \mid a_{ij} = 0, \forall i, j,\ i \neq j\}$. Montrez qu'il est un sous-groupe de $T_3(3)$. Quel est son cardinal ? Quel est l'ordre de ses éléments ?
4. Soit $UT_3(3) = \{A \in T_3(3) \mid a_{ii} = 1, \forall i\}$. Montrez qu'il est un sous-groupe de $T_3(3)$. Quel est son ordre ? Quel est l'ordre de ses éléments ?
5. Montrez que tout élément de $T_3(3)$ s'écrit comme un produit d'un élément de $D_3(3)$ pour un élément de $T_3(3)$.

3 Quelques propriétés du groupe symétrique

3.1

Soient $\gamma_1, \ldots, \gamma_r$ des cycles de longueurs respectives $\ell_1, \ldots, \ell_r$ dont les supports sont tous disjoints et soit $\sigma = \gamma_1 \cdots \gamma_r$. Montrer qu'une permutation σ' est conjuguée à σ si et seulement si σ' s'écrit comme produit de cycles à supports disjoints $\gamma'_1, \ldots, \gamma'_r$ de longueurs respectives $\ell_1, \ldots, \ell_r$.

3.2

Soit n un entier naturel non nul. Montrer que le groupe symétrique $\mathcal{S}_n$ est engendré par chacune des parties suivantes :

(a) $A = \big\{(1,i),\ 2 \leq i \leq n\big\}$; (b) $B = \big\{(i,i+1),\ 1 \leq i \leq n-1\big\}$; (c) $C = \big\{(1,2),\ (1,2,\ldots,n)\big\}$.

3.3

Montrer que toutes les transpositions sont conjuguées. Déduire de la question précédente qu'il existe au plus deux morphismes $\mathcal{S}_n \to \mathbb{C}^*$ (ce sont le morphisme trivial et la signature).

3.4

Soit $\sigma = (3,6)(7,9)(2,5)(4,7)(6,8)(1,4)$ dans $\mathcal{S}_9$.

1. Est-ce que σ peut être engendré par moins de 6 transpositions ?
2. Quel est l'ordre de σ ?
3. Quel est l'ordre maximal d'un élément de $\mathcal{S}_9$?

3.5

Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 1 & 5 & 3 \end{pmatrix} \in S_9$.

1. Écrivez σ comme produit de cycles disjoints et calculer $|\langle\sigma\rangle|$.
2. Soit $\tau \in S_6$ telle que $\tau\sigma = \sigma\tau$. Prouvez que $\tau(5) = 5$ et que $\tau(\{1,4\}) = \{1,4\}$.
3. Prouvez que $\tau = \sigma^i$ pour $i \in \mathbb{N}$.

3.6 Orbites

1. Soit n un entier non nul, soit $X = \{1, 2, \ldots, n\}$ et soit G un sous-groupe de $\mathcal{S}_n$. On note $\sim$ la relation définie sur X par : $i \sim j$ s'il existe $\sigma \in G$ tel que $\sigma(i) = j$. Montrer que $\sim$ est une relation d'équivalence. Les classes d'équivalences sont appelées les *orbites* de G.
2. Soit G un sous-groupe de $\mathcal{S}_4$ d'indice 4 (c'est-à-dire que $|\mathcal{S}_4|/|G| = 4$). En étudiant les orbites de G, montrer qu'il existe $i \in \{1,2,3,4\}$ tel que $G = \{\sigma \in \mathcal{S}_4,\ \sigma(i) = i\}$.

3.7 Sous-groupes distingués

Le but de cette section est d'étudier le fait que $K \lhd H$ et $H \lhd G \not\Rightarrow K \lhd G$.
On considère le groupe $G = AG_4$.

1. Montrer que $H = \langle id, (12)(34), (13)(24), (14)(23)\rangle$ est un sous-groupe distingué dans G.
2. Montrer que $K = \langle id, (12)(34)\rangle$ est un sous-groupe distingué dans H.
3. Montrer que K est un sous-groupe de G qui n'est pas distingué dans G.
4. Calculer tous les sous-groupes de AG_4.