

Algèbre 2 – TD n°3
Sous-groupes et morphismes. Le théorème de Lagrange. Groupes quotients.

Exercice 1 Donner la liste des tous les sous-groupes du groupe symétrique \mathfrak{S}_3 , en précisant pour chaque sous-groupe s'il est normal ou non.

Exercice 2 Soit $H \subset \mathbb{Z}$ un sous-groupe non-trivial (i.e. $H \neq \{0\}$).

1. Montrer que $H \cap \mathbb{N}^* \neq \emptyset$,
2. En utilisant le théorème de division euclidienne montrer que $H = d\mathbb{Z}$, où $d := \min(H \cap \mathbb{N}^*)$. En déduire que *tout sous-groupe de \mathbb{Z} est un sous-groupe cyclique*.

Exercice 3 1. Soit (G, \cdot) un groupe et $H, H' \subset G$ deux sous-groupes. Montrer que $H \cap H'$ est un sous-groupe de G .

2. Soit $(A, +)$ un groupe abélien, et $H, H' \subset A$ deux sous-groupes. Montrer que

$$H + H' := \{x + x' \mid x \in H, x' \in H'\}$$

est un sous-groupe de A . Montrer par un exemple que l'affirmation n'est pas vraie dans la cas non-abélien.

Exercice 4 Soient $m, n \in \mathbb{N}^*$. Rappeler la définition de $\text{pgcd}(m, n)$, $\text{ppcm}(m, n)$. Montrer que

1. $m\mathbb{Z} + n\mathbb{Z} = \text{pgcd}(m, n)\mathbb{Z}$,
2. $m\mathbb{Z} \cap n\mathbb{Z} = \text{ppcm}(m, n)\mathbb{Z}$,
3. $m\mathbb{Z} \subset n\mathbb{Z}$ si et seulement si m est un multiple de n , et si c'est le cas, alors a un isomorphisme $n\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}_d$, où $d := m/n$.

Exercice 5 Soit $n \in \mathbb{N}^*$.

1. Montrer que tout sous-groupe de \mathbb{Z}_n est cyclique. *Indication : Utiliser l'exercice 4 et la remarque suivante : Soient H un sous-groupe normal de G , $p : G \rightarrow G/H$ l'épimorphisme canonique, et S un sous-groupe de G/H . Alors $S = p^{-1}(S)/H$.*

2. Soit $x = [k] \in \mathbb{Z}_n$.

(a) Montrer que $\langle x \rangle = \langle [d]_n \rangle$ où $d := \text{pgcd}(k, n)$, et $\langle x \rangle \simeq \mathbb{Z}_l$, où $l := \frac{n}{d}$.

(b) Construire un isomorphisme $\mathbb{Z}_d \xrightarrow{\cong} \mathbb{Z}_n / \langle x \rangle$. *Indication : Appliquer le 1er théorème d'isomorphisme à un épimorphisme $\mathbb{Z} \rightarrow \mathbb{Z}_n / \langle x \rangle$.*

Exercice 6 Pour $n \in \mathbb{N}^*$ et $k \in \mathbb{Z}$ on va désigner par $[k]_n$ la classe de congruence de k modulo n . Soit $m, n \in \mathbb{N}^*$.

1. Montrer que la formule $g([k]_{mn}) = ([k]_m, [k]_n)$ définit un homomorphisme de groupes $g : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$.
2. Préciser $\ker(g)$, $\text{im}(g)$.
3. Étudier le cas où m, n sont premiers entre eux (i.e. où $\text{pgcd}(m, n) = 1$).
4. Généraliser ces résultats pour un système $(n_1, \dots, n_k) \in (\mathbb{N}^*)^k$ (où $k \geq 2$).

Exercice 7 Montrer que tout sous-groupe d'indice 2 est distingué.

Exercice 8 Pour tout nombre complexe $z = a + ib$ non nul (avec a et b réels), posons $M(z) := \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

1. Vérifier que $M(z)$ est inversible pour tout $z \in \mathbb{C}^*$,
2. Prouver que l'application $M : \mathbb{C}^* \rightarrow \text{GL}(2, \mathbb{R})$ donnée par $z \mapsto M(z)$ est un morphisme de groupes. Cet morphisme est-il injectif? Est-il surjectif?

Exercice 9 Rappelons qu'un isomorphisme $f : G \rightarrow G$ s'appelle automorphisme de G . Montrer que l'application $GL(n, \mathbb{R}) \rightarrow GL(n, \mathbb{R})$ donnée par $A \mapsto {}^t(A^{-1})$ est un automorphisme de $GL(n, \mathbb{R})$.

Exercice 10 Soit G un groupe. Rappelons qu'un isomorphisme $f : G \rightarrow G$ s'appelle automorphisme de G . A tout élément a de G on associe une application $\iota_a : G \rightarrow G$ par

$$\iota_a(x) = axa^{-1}.$$

1. Montrer que ι_a est un automorphisme de G (on dit que c'est un *automorphisme intérieur*).
2. Montrer que $\iota_a = \text{id}_G$ si et seulement si $a \in Z(G) = \{z \in G \mid \forall g \in G, gz = zg\}$ (le centre de G).
3. Montrer que l'ensemble $\text{Aut}(G)$ des automorphismes de G est un groupe (avec l'opération de composition d'applications).
4. Montrer que l'ensemble des automorphismes intérieurs $\text{Int}(G)$ est un sous-groupe du groupe $\text{Aut}(G)$. Ce sous-groupe est-il distingué dans $\text{Aut}(G)$?
5. Montrer que l'application $\phi : G \rightarrow \text{Int}(G)$, définie par $\phi(a) = \iota_a$, est un morphisme.
6. Déterminer le noyau de ϕ .
7. Soit $H \subset G$ un sous-groupe de G . Montrer que pour tout $a \in G$ l'image $\iota_a(H)$ de H par ι_a est un sous-groupe de G isomorphe à H , et que H est distingué si et seulement si $\forall a \in G, \iota_a(H) = H$.

Exercice 11 En utilisant le premier théorème d'isomorphisme construire des isomorphismes

1. $\mathbb{R}/\mathbb{Z} \xrightarrow{\cong} U$, où $U := \{z \in \mathbb{C} \mid |z| = 1\}$,
2. $\mathbb{C}^*/U \simeq \mathbb{R}_+^*$, $\mathbb{C}^*/\mathbb{R}_+^* \simeq U$,
3. $\mathbb{R}^*/\mathbb{R}_+^* \xrightarrow{\cong} \{\pm 1\}$,
4. $\mathbb{Z}_n \xrightarrow{\cong} U_n$, où $n \in \mathbb{N}^*$ et $U_n := \{z \in \mathbb{C} \mid z^n = 1\}$,
5. $GL(n, \mathbb{R})/SL(n, \mathbb{R}) \xrightarrow{\cong} \mathbb{R}^*$, $GL(n, \mathbb{C})/SL(n, \mathbb{C}) \xrightarrow{\cong} \mathbb{C}^*$.

Exercice 12 Un corps (commutatif) est un triplet $(K, +, \cdot)$, où $+$, \cdot sont deux lois de composition internes sur K telles que

- (1) $(K, +)$ est un groupe abélien, dont l'élément neutre sera noté 0_K .
- (2) $(K \setminus \{0_K\}, \cdot)$ est un groupe abélien, dont l'élément neutre sera noté 1_K .
- (3) la loi \cdot est distributive par rapport à la loi $+$, i.e. pour tout $(x, y, z) \in K \times K \times K$ on a $x \cdot (y + z) = x \cdot y + x \cdot z$.

1. Soit $n \in \mathbb{N}^*$. Montrer que sont équivalentes :

- (a) $(\mathbb{Z}_n, +, \cdot)$ est un corps.
- (b) n est un nombre premier.

Pour un nombre premier p , le corps $(\mathbb{Z}_p, +, \cdot)$ sera noté \mathbb{F}_p . Noter que ce corps est fini.

2. Combien de droites vectorielles il y a-t-il dans l'espace vectoriel \mathbb{F}_p^n ?

Exercice 13 Soit

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 5 & 2 & 1 \end{pmatrix} \in \mathfrak{S}_6.$$

1. Trouver une décomposition de σ en produit de cycles disjoints, et une décomposition de σ en produit de transpositions.
2. Déterminer la signature de σ en utilisant les deux décompositions et comparer les résultats.
3. Préciser l'ordre de σ et le sous-groupe cyclique engendré par σ .

Exercice 14 Soit $\{A_1, A_2, A_3, A_4\}$ l'ensemble des sommets d'un carré dans le plan \mathbb{R}^2 , et D_4 le groupe des isométries du plan qui laissent invariant cet ensemble.

1. Préciser l'image du morphisme naturel $r : D_4 \rightarrow \mathfrak{S}_4$ en décomposant chaque élément $\sigma \in \text{im}(r)$ en produit de cycles disjoints.
2. Classifier les sous-groupes et les sous-groupes distingués de D_4 . *Indication : Soit $D_4^0 \simeq U_4$ le sous-groupe formé par les rotations qui laissent invariant le carré. Classifier d'abord les sous-groupes de D_4^0 , puis les sous-groupes d'ordre 2 engendrés par une réflexion. Montrer que D_4 a aussi deux sous-groupes d'ordre 4 non-cycliques (donc isomorphes à $\mathbb{Z}_2 \times \mathbb{Z}_2$), chacun de ces sous-groupes contenant deux réflexions par rapport à deux axes perpendiculaires.*