TD n°1 : Groupes

Exercice 1. [Groupes monogènes, groupes cycliques] Un groupe est dit monogène s'il est engendré par un seul élément. On dit qu'il est cyclique s'il est monogène et fini.

1. Montrer qu'un groupe monogène est isomorphe à $\mathbb{Z}$ ou $\mathbb{Z}/n\mathbb{Z}$ pour un entier $n \geq 1$.
2. Trouver tous les sous-groupes de $\mathbb{Z}$ et de $\mathbb{Z}/n\mathbb{Z}$. Montrer en particulier qu'ils sont monogènes, et que pour tout $d \geq 1$ divisant n, il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d.
3. Trouver les générateurs de $\mathbb{Z}$ et de $\mathbb{Z}/n\mathbb{Z}$. En déduire leur groupe d'automorphismes.
4. Soit φ l'indicatrice d'Euler définie par $\varphi(m) = \#\{d \in \mathbb{N}^* |\ d \leq m \text{ et } \mathrm{pgcd}(d,m) = 1\}$. Démontrer la relation : $n = \sum_{d|n} \varphi(d)$.
5. Soit G un groupe fini d'ordre n tel que, pour tout diviseur d de n, G contienne au plus un sous-groupe cyclique d'ordre d. Montrer que G est cyclique.
6. *Application :* Soit K un corps et G un sous-groupe fini du groupe multiplicatif K^*. Montrer que G est cyclique.

Exercice 2. [Sous-groupes de $\mathbf{Q}/\mathbf{Z}$] Montrer que $(\mathbf{Q}/\mathbf{Z}, +)$ possède un unique sous-groupe d'ordre n pour tout $n \geq 1$ et que ce groupe est cyclique.

Exercice 3. Le groupe $(\mathbf{Q}, +)$ peut-il être engendré par un nombre fini d'éléments ? Qu'en est-il de $(\mathbf{Q}^*, \times)$?

Exercice 4.
1. Soit $p \geq 3$ un nombre premier et $k \geq 1$ un entier. Montrer qu'il existe a_k premier avec p tel que $(1+p)^{p^k} = 1 + a_k p^{k+1}$. En déduire que $(\mathbb{Z}/p^k\mathbb{Z})^* \simeq \mathbb{Z}/p^{k-1}(p-1)\mathbb{Z}$.
2. Identifier le groupe $(\mathbb{Z}/2^k\mathbb{Z})^*$.
3. Pour quels entier $n \geq 1$, le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ est-il cyclique ?

Exercice 5. Soit G un groupe. On note $\mathrm{Aut}(G)$ le groupe des automorphismes de G, la loi de groupe étant la composition.

1. Montrer qu'un groupe dans lequel tous les carrés sont triviaux est commutatif. Un tel groupe est-il nécessairement fini ?
2. Montrer qu'un groupe fini d'ordre pair contient au moins un élément d'ordre 2, puis qu'il en contient en fait un nombre impair.
3. Soit $N \lhd G$ un sous-groupe distingué d'indice n. Montrer que pour tout $g \in G$, $g^n \in N$. Est-ce toujours vrai si l'on ne suppose plus que N est distingué ?
4. *(Plus difficile)* Soit G un groupe tel que $\mathrm{Aut}(G)$ soit cyclique. Montrer que G est abélien.

Exercice 6. [Automorphismes intérieurs]

1. Soit $a \in G$. Montrer que l'application $\varphi_a : g \mapsto aga^{-1}$ est un automorphisme de G. Un tel automorphisme est dit intérieur.
2. Soit $\mathrm{Inn}(G)$ l'ensemble des automorphismes intérieurs de G. Montrer que $\mathrm{Inn}(G)$ est un sous-groupe distingué de $\mathrm{Aut}(G)$.
3. Montrer que $\varphi : a \mapsto \varphi_a$ est un morphisme de groupes. Quel est son noyau ?

4. Que peut-on dire d'un groupe dont le groupe des automorphismes est trivial ?

Exercice 7. Caractériser l'ensemble des groupes dont l'ensemble des sous-groupes est fini.

Exercice 8. [Sous-groupes d'un groupe de type fini] On considère les matrices $X = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ et $Y = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, et on note G le sous-groupe de $GL_2(\mathbf{R})$ qu'elles engendrent.

1. Pour $n \in \mathbf{Z}$, calculer $X^{-n}YX^n$. On note H_n le sous-groupe de $GL_2(\mathbf{R})$ engendré par cet élément.
2. Montrer que pour tout $n \in \mathbf{Z}$, H_n est strictement inclus dans H_{n+1}.
3. Exhiber un sous-groupe de G qui est strictement inclus dans un de ses conjugués.
4. Exhiber un sous-groupe de G qui ne peut pas être engendré par un nombre fini d'éléments.

Exercice 9. [Ordre du produit de deux éléments] Soient G un groupe et x et y des éléments de G.

1. Montrer que xy et yx ont même ordre (éventuellement infini).
2. On suppose que x et y commutent et sont d'ordre fini. Montrer que G contient un élément dont l'ordre est le ppcm des ordres de x et y.
   Indication : on pourra commencer par le cas où ces ordres sont premiers entre eux.

Exercice 10. [Une condition suffisante pour être distingué] Soit G un groupe fini et soit H un sous-groupe de G. On considère l'action de G sur l'ensemble des classes de G modulo H. Notons $\theta : G \to S(G/H)$ le morphisme de groupes $g \mapsto \{xH \mapsto gxH\}$.

1. Montrer que $Ker(\theta)$ est le plus grand sous-groupe distingué de G contenu dans H.
2. Montrer que si $|G|$ ne divise pas $[G : H]!$, alors G contient un sous-groupe distingué non trivial.
3. Notons p le plus petit facteur premier de $|G|$. Déduire des questions précédentes que si $[G : H] = p$, alors H est distingué dans G.

Exercice 11. Soit G un groupe et soit H un sous-groupe distingué de G. Soit également K un sous-groupe quelconque de G.

1. Montrer que l'ensemble $KH = \{kh : k \in K, h \in H\}$ est un sous-groupe de G qui coïncide avec l'ensemble HK. Donner un contre-exemple dans le cas où H n'est pas distingué dans G.
2. Montrer l'existence d'un isomorphisme $KH/H \cong K/(K \cap H)$. On pourra montrer que le morphisme composé $K \hookrightarrow KH \twoheadrightarrow KH/H$ est surjectif.

Exercice 12. [Un premier exemple de suite exacte]

1. Soit G un groupe et $H \lhd G$. Montrer que la suite $1 \to H \to G \to G/H \to 1$ est exacte.
2. Réciproquement, montrer que si on a une suite exacte de la forme $1 \to H \to G \to K \to 1$, alors H s'identifie à un sous-groupe distingué de G et $K \cong G/H$.
3. Montrer que la suite $0 \to 2\mathbf{Z} \to \mathbf{Z} \to \mathbf{Z}/2\mathbf{Z} \to 0$ est exacte mais pas scindée.