TD n°1 : Groupes

Exercice 1. Combien de relations d'équivalence peut-on définir sur $\{1, 2, 3, 4\}$?

Exercice 2. Soit E un ensemble muni d'une relation d'équivalence $\sim$. Notons $X = E/\sim$ l'ensemble quotient associé, i.e. l'ensemble des classes d'équivalence de cette relation, et $\pi : E \to X$ la projection canonique.

1. Soit $f : E \to F$ une application telle que : $(x \sim y) \implies (f(x) = f(y))$. Montrer qu'il existe une unique application $\overline{f} : X \to F$ telle que $f = \overline{f} \circ \pi$.
2. À quelle condition $\overline{f}$ est-elle injective ? Surjective ?

Exercice 3. Soit E un espace vectoriel sur k et F un sous-espace vectoriel de E.

1. Montrer que la relation définie par $x \sim y \Leftrightarrow y - x \in F$ est une relation d'équivalence et que l'ensemble quotient, noté E/F, a une structure d'espace vectoriel telle que la projection $\pi : E \to E/F$ est linéaire.
2. Montrer que si E est de dimension finie sur k, la dimension de E/F est égale à $\dim E - \dim F$.
3. Soit $f : E \to G$ une application linéaire de noyau F. Démontrer qu'il existe une application linéaire injective $\overline{f} : E/F \to G$ telle que $f = \overline{f} \circ \pi$.
4. *Application : théorème du rang.* Démontrer le théorème du rang en utilisant la notion d'espace quotient.

Exercice 4. Soit G un groupe. On note $\mathrm{Aut}(G)$ le groupe des automorphismes de G, la loi de groupe étant la composition.

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 ?

Exercice 5.
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. 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 7. *Groupes monogènes*

On rappelle qu'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 $\varphi(m) = \#\{d \in \mathbb{N}^* | \ d \leq m \text{ et } \operatorname{pgcd}(d,m) = 1\}$ la fonction indicatrice d'Euler. Démontrer la relation : $n = \displaystyle\sum_{d|n} \varphi(d)$.
5. Soient m et n deux entiers positifs. Déterminer l'ensemble des morphismes de groupes de $\mathbb{Z}$ dans $\mathbb{Z}$; de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$; de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}$; de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$.
6. Soient m et n deux entiers premiers entre eux. Montrer que $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/mn\mathbb{Z}$.
7. 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.
8. *Application :* Soit K un corps et G un sous-groupe fini du groupe multiplicatif K^*. Montrer que G est cyclique.

Exercice 8. *Le groupe multiplicatif de* $\mathbb{Z}/n\mathbb{Z}$

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 9. Soit p un nombre premier impair. Notons

$$G = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}, a, b, c \in \mathbb{Z}/p\mathbb{Z} \right\}.$$

1. Montrer que G est un sous-groupe non abélien de $\mathrm{GL}_3(\mathbb{Z}/p\mathbb{Z})$.
2. Montrer que tout élément de G est d'ordre p.

Exercice 10. *Le groupe diédral*

Soit $n \geq 3$ un entier. On note D_n l'ensemble des isométries du plan affine euclidien (c'est-à-dire les éléments de $O_2(\mathbb{R})$) qui laissent globalement invariant l'ensemble des sommets d'un polygone régulier à n côtés (que l'on pourra prendre comme étant les points d'affixe $e^{2ik\pi/n}$ avec $k = 0, \ldots, n-1$).

1. Montrer que D_n est un groupe d'ordre $2n$. Décrire géométriquement ses éléments.
   Indication : on pourra distinguer selon la parité de n.
2. Montrer que D_3 est engendré par deux éléments r et s tels que $r^3 = s^2 = \mathrm{id}$ et $sr = r^{-1}s$, puis que $D_3 \simeq \mathfrak{S}_3$.
3. Montrer que D_4 est engendré par deux éléments r et s tels que $r^4 = s^2 = \mathrm{id}$ et $sr = r^{-1}s$. En dresser la table de multiplication.
4. Notons $A_1 = (1,0)$, $A_2 = (0,1)$, $A_3 = (-1,0)$ et $A_4 = (0,-1)$ les sommets du carré standard. Montrer qu'on a un morphisme de groupes injectif $D_4 \to \mathfrak{S}_4$. Quelle est son image ? Celle-ci dépend-elle de la numérotation des sommets du carré choisie ?
5. Quels sont les sous-groupes propres de D_4 ? Pour chacun d'entre eux, déterminer un isomorphisme avec un groupe classique.
6. Montrer qu'en général, D_n est engendré par deux éléments r et s qui vérifient les relations $r^n = s^2 = \mathrm{id}$ et $sr = r^{-1}s$.