Feuille 2 : Quotients

Exercice 21 (♡ Groupes d'ordre premier)**.**
Soit p un nombre premier et G un groupe d'ordre p.

(1) Montrer que G n'a pas de sous-groupe autre que $\{e\}$ et G.
(2) En déduire que G est cyclique.

Exercice 22 (♡ Ordre d'un élément)**.**
Soient G un groupe et $x, y \in G$ deux éléments d'ordre fini de G.

(1) Montrer que l'ordre de yxy^{-1} est égal à l'ordre de x.
(2) De même, montrer que les ordres de xy et de yx sont égaux.
(3) Soit H un autre groupe et $f \in \mathrm{Hom}(G, H)$. Montrer que l'ordre de $f(x)$ divise l'ordre de x.
(4) Soit $k \in \mathbb{N}$. Montrer que l'ordre de x^k divise l'ordre de x.
(5) (★) On suppose que les ordres de x et y sont premiers entre eux et que $xy = yx$. Montrer que l'ordre de xy est le produit des ordres de x et y.
(6) (★) Trouver un exemple où l'ordre de xy n'est pas le produit des ordres de x et de y.

Exercice 23 (★ Quelques propriétés de parité)**.**

(1) Soit G un groupe fini d'ordre pair. Montrer qu'il existe un élément d'ordre 2. (Considérer les éléments tels que $x \neq x^{-1}$)
(2) Soit H un groupe fini d'ordre impair. Montrer que tous les éléments de H sont d'ordre impair.
(3) En déduire que tout élément de H possède une unique "racine carrée". (Une racine carrée de $y \in H$ est un élément $x \in H$ tel que $x^2 = y$).

Exercice 24 (♠ Existence d'élément d'ordre p)**.**

(1) Soit G un groupe, et x un élément d'ordre p dans G, avec p premier. Montrer que les éléments $\left\{x^k \,|\, 1 \leq k \leq p-1\right\}$ sont tous distincts et d'ordre p.
(2) Utiliser la question précedente pour montrer que dans un groupe d'ordre 35, il existe au moins un élément d'ordre 5 et un élément d'ordre 7.

Exercice 25 (Groupe diédral)**.**
Soit Hex l'ensemble des six sommets formant un hexagone régulier dans $\mathbb{R}^2$ centré en $(0,0)$ et tel que $A = (1,0) \in \mathrm{Hex}$. On note $\mathcal{D}$ l'ensemble des isométries qui préservent Hex, c'est à dire :

$$\mathcal{D} = \{\phi \in \mathrm{O}(\mathbb{R}^2), \forall P \in \mathrm{Hex}, \phi(\mathrm{P}) \in \mathrm{Hex}\}$$

(1) Montrer que $\mathcal{D}$ est un groupe pour la composition $\circ$.
(2) Montrer que $\mathcal{D}_A = \{\phi \in \mathcal{D}, \phi(A) = A\}$ est un sous-groupe d'ordre 2 de $\mathcal{D}$.
(3) Soient $\phi, \phi' \in \mathcal{D}$. Montrer que $\overline{\phi} = \overline{\phi}'$ dans $\mathcal{D}/\mathcal{D}_A$ si et seulement si $\phi(A) = \phi'(A)$.
(4) En déduire que $[\mathcal{D} : \mathcal{D}_A] = 6$ et que $\mathcal{D}$ est d'ordre 12.
(5) Déterminer les sous-groupes de $\mathcal{D}$, et justifier que $\mathcal{D}$ n'est pas cyclique.

Exercice 26 (★ Groupes sans sous-groupes)**.**
Soit G un groupe qui n'a pas de sous-groupes propre (c'est à dire distinct de $\{e\}$ et G).

(1) Montrer que G est monogène.
(2) Soit x un générateur de G. Montrer que si $x^2 \neq e$ alors x^2 est aussi un générateur de G.
(3) En déduire que G est cyclique d'ordre p avec p premier.

Exercice 27 (♠ Isomorphismes)**.**
Dans chacun des exemples, on appliquera le théorème d'isomorphisme à un morphisme bien choisi.

(1) Montrer que le quotient $\mathbb{C}/\mathbb{R}$ est isomorphe à $\mathbb{R}$.
(2) Montrer que le quotient $\mathbb{R}/\mathbb{Z}$ est isomorphe à $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$.
(3) Soit $G = (\mathbb{R}^*, \times)$ et $H = \mathbb{R}^*_+$. Montrer que G/H est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.
(4) Soit $G = \mathrm{GL}_2(\mathbb{R})$ et $H = \{k \cdot \mathrm{I}_2 \mid k \in \mathbb{R}^{+*}\}$. Montrer que H est bien le noyau d'un morphisme, et montrer que G/H est isomorphe à $\mathrm{SL}_2(\mathbb{R})$.

Exercice 28 (Racines de l'unité)**.**
Soit l'ensemble de toutes les racines de l'unité :

$$\mathbb{U}_\infty = \{z \in \mathbb{C} \,|\, \exists n \geq 1, z^n = 1\}$$

(1) Montrer que $\mathbb{U}_\infty$ est un sous-groupe de $\mathbb{C}^*$.
(2) Montrer que $\mathbb{U}_\infty$ est isomorphe à $\mathbb{Q}/\mathbb{Z}$.
(3) Montrer que $\mathbb{U}_\infty$ n'est pas de type fini.

Exercice 29 (♠ Sous-Groupes distingués)**.**
Soit H et K deux sous-groupes distingués du groupe G.

(1) Montrer que $H \cap K$ est un sous-groupe distingué de G.
(2) Montrer que $HK = \{hk | h \in H, k \in K\}$ est un sous-groupe de G, puis montrer qu'il est distingué dans G.

Exercice 30 (★ Groupe Affine)**.**
Pour $a, b \in \mathbb{C}$ on pose la fonction $f_{a,b} : z \mapsto az + b$ de $\mathbb{C}$ dans $\mathbb{C}$.
Soit $G = \left\{ f_{a,b} \middle| \, a \in \mathbb{C}^*, b \in \mathbb{C} \right\}$

(1) Montrer que G est un groupe pour la composition usuelle.
(2) Soit $T = \left\{ z \mapsto z + b \;\middle|\; b \in \mathbb{C} \right\}$. Montrer que $T < G$ et que T est isomorphe à $\mathbb{C}$.
(3) Soit $H = \left\{ z \mapsto az \;\middle|\; a \in \mathbb{C}^* \right\}$. Montrer que $H < G$ et que H est isomorphe à $\mathbb{C}^*$.
(4) Montrer que T est un sous-groupe distingué de G, et que H n'est pas un sous-groupe distingué de G.
(5) Montrer que le quotient G/T est isomorphe à $\mathbb{C}^*$.

Exercice 31 (Relation définie par une partie)**.**
Soit G un groupe et E une partie de G. On définit la relation $\sim_E$ par

$$\forall x, y, \in G, \quad x \sim_E y \Leftrightarrow x^{-1}y \in E$$

Montrer que si $\sim_E$ est une relation d'équivalence, alors E est un sous-groupe de G.

Exercice 32 (★ Indice 2)**.**
Soit G un groupe et H un sous-groupe d'indice 2. Montrer que H est distingué.

Exercice 33 (♡ Générateurs des groupes cycliques)**.**
Soient $n \geq 2$ et $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$. Montrer que $\overline{k}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$ si et seulement si k est premier avec n.

Exercice 34 (♠ Sous-groupes d'un groupe cyclique)**.**
Soit $n \in \mathbb{N}^*$ et $G = \mathbb{Z}/n\mathbb{Z}$. Soit $k \in \mathbb{Z}$ et $d = \text{pgcd}(k, n)$.

(1) Déterminer l'ordre de $\overline{k}$ dans G.
(2) Montrer que $\overline{k}$ et $\overline{d}$ engendrent le même sous-groupe de G.
(3) En déduire que si m divise n, il existe un unique sous-groupe C_m d'ordre m.
(4) Donner la liste des sous-groupes de $\mathbb{Z}/12\mathbb{Z}$.

Exercice 35 (♡ Théorème d'Euler et de Fermat)**.**
Soit $a, n \in \mathbb{N}$.

(1) On suppose que $a \wedge n = 1$. Montrer que $a^{\varphi(n)} \equiv 1 \mod (n)$. (Théorème d'Euler)
(2) On suppose maintenant que n est un nombre premier. Montrer que si $a \notin n\mathbb{Z}$ alors $\overline{a} \in \mathbb{Z}/n\mathbb{Z}^*$. En déduire l'ordre de $(\mathbb{Z}/n\mathbb{Z})^*$.
(3) Montrer que si $\overline{a} \neq \overline{0}$ alors $\overline{a}^{n-1} = \overline{1}$.
(4) En déduire que pour tout $a \in \mathbb{Z}$, on a n divise $a^n - a$. (petit théorème de Fermat)
(5) Calculer le reste de la division euclidienne de 17^{2017} par 11.

Exercice 36 (♠ Groupe d'automorphisme)**.** Soit $G = \mathbb{Z}/n\mathbb{Z}$.

(1) Soit $a \in (\mathbb{Z}/n\mathbb{Z})$. Montrer que l'application suivante est un endomorphisme de G.

$$\begin{aligned} \phi_a : (\mathbb{Z}/n\mathbb{Z}, +) &\longrightarrow (\mathbb{Z}/n\mathbb{Z}, +) \\ x &\longmapsto a \times x \end{aligned}$$

(2) A quelle condition sur n et a, l'application ϕ_a est-elle un automorphisme ?
(3) Montrer que l'application suivante est un isomorphisme :

$$\begin{aligned} \Phi : ((\mathbb{Z}/n\mathbb{Z})^*, \times) &\longrightarrow (\text{Aut}(G), \circ) \\ a &\longmapsto \phi_a \end{aligned}$$

Exercice 37 (★ Morphismes entre groupes cycliques)**.**
Soit $m, n \in \mathbb{Z}$, et on note $G = \mathbb{Z}/m\mathbb{Z}$ et $H = \mathbb{Z}/n\mathbb{Z}$.

(1) Soit $f \in \text{Hom}(G, H)$. Montrer que l'ordre de $f(\overline{1})$ dans $\mathbb{Z}/n\mathbb{Z}$ divise le pgcd $d = m \wedge n$.
(2) En déduire que si m et n sont premiers entre eux, alors le seul morphisme de G dans H est le morphisme nul.
(3) Montrer que $\text{Hom}(G, H)$ est un sous-groupe de $(\mathcal{F}(G, H), +)$ le groupe des applications à valeur dans le groupe $(H, +)$.
(4) Montrer que si n divise m, alors pour tout morphisme $\psi : G \to H$ il existe $k \in \mathbb{Z}$ tel que $\psi = \overline{\phi_k}$. C'est à dire que $\psi(\overline{x}) = \overline{kx}$ pour tout $x \in G$.
(5) Montrer que $\text{Hom}(G, H)$ est isomorphe à $\mathbb{Z}/d\mathbb{Z}$.