Feuille 2 : Groupes Finis

Exercice 19 (♡ Arithmétique élémentaire)**.**
Soient $a, b, c \in \mathbb{Z}$.

(1) Supposons $\langle a, b\rangle = \mathbb{Z}$. Montrer que $\langle a, bc\rangle = \langle a, c\rangle$.
(2) En déduire que si $bc \in a\mathbb{Z}$ et $\langle a, b\rangle = \mathbb{Z}$ alors $c \in a\mathbb{Z}$. Traduisez cette question en terme de pgcd et de divisibilité. Reconnaissez-vous le résultat ?
(3) Montrer que si $m\mathbb{Z}$ est un sous-groupe de $d\mathbb{Z}$, il existe $a, b \in \mathbb{Z}$ tels que $\langle a, b\rangle = d\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

Exercice 20 (♠ PGCD × PPCM)**.** Soient $a, b \in \mathbb{N}$. Et soient $m = a \vee b$ et $d = a \wedge b$.

(1) Soit $x \in m\mathbb{Z}$. Justifier que $\langle ax, bx\rangle \subset ab\mathbb{Z}$.
(2) Soient a', b' tels que $a = da'$ et $b = db'$. Justifier que $da'b' \in m\mathbb{Z}$.
(3) Montrer que $md = ab$.

Exercice 21 (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 22 (♡ 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 23 (★ Groupes sans sous-groupes)**.**
On veut montrer la réciproque de la question 1 de l'exercice précédent. Soit G un groupe qui n'a pas de sous-groupes (autre que $\{e\}$ et G).

(1) Montrer que G est monogène.
(2) Soit x un générateur de G. Montrer que soit $x^2 = e$, soit x^2 est un générateur de G.
(3) En déduire que G est cyclique d'ordre p avec p premier.

Exercice 24 (♡ Ordre d'un élément)**.**
Soient G, H deux groupes.

(1) Soient $x, y \in G$. 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 $f \in \mathrm{Hom}(G, H)$ et $x \in G$. Montrer que l'ordre de $f(x)$ divise l'ordre de x.
(4) Soit $x \in G$ et $k \in \mathbb{N}$. 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 y.

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 (★ Quelques propriétés)**.**
(1) Soit G un groupe fini d'ordre pair. Montrer qu'il existe un élément d'ordre 2. (Considérer les éléments tels que $x = x^{-1}$)
(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", c'est à dire

$$\forall x \in H, \exists! y \in H, x = y^2$$

Exercice 27 (♠ 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 d'ordre 7.

Exercice 28 (♡ 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 29 (♠ 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 $\bar{k}$ dans G.
(2) Montrer que $\bar{k}$ et $\bar{d}$ 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 30 (♠ Equations diophantiennes)**.**
Résoudre dans $\mathbb{Z}$ les équations suivantes, pour les différentes valeurs de k :
(1) $13x + 8y = k$ avec $k = 0, 1, 4$.
(2) $95x + 71y = 46$
(3) $35x + 14y = k$ avec $k = 0, 10, 14$.
(4) $12x + 15y + 20z = 7$

Exercice 31. ♠ Résoudre les systèmes suivants :

$$\begin{cases} x \equiv 11 & \pmod{18} \\ x \equiv 25 & \pmod{77} \end{cases} \qquad \begin{cases} x \equiv 2 & \pmod{140} \\ x \equiv -3 & \pmod{99} \end{cases}$$

Exercice 32 (★ Le Cuisinier Chinois)**.**
Une bande de 17 pirates dispose d'un butin composé de N pièces d'or d'égale valeur. Ils décident de se le partager également et de donner le reste au cuisinier (non pirate). Celui ci reçoit 3 pièces. Mais une rixe éclate et 6 pirates sont tués. Tout le butin est reconstitué et partagé entre les survivants comme précédemment; le cuisinier reçoit alors 4 pièces. Dans un naufrage ultérieur, seuls le butin, 6 pirates et le cuisinier sont sauvés. Le butin est à nouveau partagé de la même manière et le cuisinier reçoit 5 pièces.
Quelle est alors la fortune minimale que peut espérer le cuisinier lorsqu'il décide d'empoisonner le reste des pirates ?

Exercice 33. ♠ Montrer les énoncés suivants
(1) Tout nombre carré est congru à 0 ou 1 modulo 4.
(2) Tout nombre carré est congru à 0 ou 1 ou 4 modulo 8.
(3) Un nombre de la forme $4k + 3$ ne peut pas s'écrire comme une somme de deux carrés.