TD6 STRUCTURES ALGÉBRIQUES POUR L'INFORMATIQUE

EXERCICE 1

1. Soit G un groupe fini d'ordre 60. Quels sont les ordres possibles pour les sous-groupes de G?

2. Soit G un groupe fini contenant un élément d'ordre 5 et un élément d'ordre 7. Pourquoi a–t–on $|G| \geq 35$?

EXERCICE 2 . Prouver ou prouver la négation de chacune des assertions suivantes:

1. Tout sous–groupe de $\mathbb{Z}$ est d'ordre fini.

2. Tout sous–groupe de $\mathbb{Z}$ est d'indice fini.

EXERCICE 3 . Décrire les éléments inversibles de $\mathbb{Z}/30\mathbb{Z}$.

EXERCICE 4 . On désigne par ϕ la fonction indicatrice d'Euler.

1. Soit $n = pq$ avec p et q deux nombres premiers distincts. Calculer alors $\phi(n)$.
   Indication: On rappelle que les seuls nombres qui ne sont pas premiers avec n sont des multiples de p ou des multiples de q.

2. Soit p un nombre premier. Calculer $\phi(p^e)$, où e est un entier positif.
   Indication: On rappelle que les seuls nombres qui ne sont pas premiers avec p^e sont des multiples de p.

EXERCICE 5
Soit G un groupe et $a \in G$. On rappelle que si il existe $k \in \mathbb{N}^*$ tel que $a^k = 1_G$, alors le plus petit entier $k \geq 1$ vérifiant $a^k = 1_G$ est appelé l'ordre de a. Il est noté $ord(a)$. Si aucun $k \geq 1$ ne vérifie $a^k = 1_G$, alors on dit que a est d'ordre infini. Montrer que $ord(a)$ est l'ordre (ou encore le cardinal) du sous-groupe engendré par $\{a\}$.

EXERCICE 6 . Soit G un groupe cyclique d'ordre n (i.e. $\exists a \in G$, tel que G est le groupe engendré par $\{a\}$ et $|G| = n$). Montrer que pour tout d diviseur de n, G possède un sous-groupe d'ordre d.
Indication. Si G est engendré par a et $n = dk$, considérer le groupe engendré par a^k.

EXERCICE 7 . Montrer que tout sous-groupe H d'un groupe cyclique G est lui-même cyclique.
Indication. Soit a un générateur de G. Considérer le plus petit entier positif k, tel que $a^k \in H$.

EXERCICE 8 . Soit $(G, .)$ un groupe et $a \in G$ un élément d'ordre n.

1. Montrer que $a^m = 1$ si et seulement si n divise m.

2. On suppose qu'il existe deux entiers p et t tels que $n = pt$. Montrer que $ord(a^t) = p$.
   Indication. Remarquer que $(a^t)^p = 1_G$. Puis, montrer qu'aucune puissance plus petite de a^t n'est égale à 1_G.

3. Soit p un diviseur premier de n. Supposons qu'il existe $x \in G$ tel que $x^p = a$. Montrer que $ord(x) = pn$.

EXERCICE 9 . Soit $(G, .)$ un groupe et $H \leq G$. Montrer que si $[G : H] = 2$, alors $gH = Hg$.

EXERCICE 10 . Soit $(G, .)$ un groupe fini avec $|G| = 2n$.

1. Combien existe-t-il d'éléments d'ordre 1 dans G ?
2. Soit $x \in G$. Montrer que $x = x^{-1} \iff ord(x) \leq 2$.
3. Déduire en regroupant les éléments de G par paires (élément, élément symétrique) que le nombre d'éléments d'ordre 2 dans G est impair.
4. En déduire que G contient un sous-groupe d'ordre 2.

EXERCICE 11 . Soit G un groupe et H un sous-groupe de G. On suppose que pour tout $h \in H$ et pour tout $g \in G$, $ghg^{-1} \in H$. Montrer alors que les classes à gauche selon H et les classes à droite selon H coïncident.

EXERCICE 12 . On admet que si a et b sont deux nombres entiers premiers entre eux, alors $\phi(ab) = \phi(a) * \phi(b)$.

1. Soit $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, la décomposition de $n \in \mathbb{N}^*$ en produit de facteurs premiers. Calculer $\phi(n)$.
2. Calculer $\phi(12)$ et $\phi(100)$.

EXERCICE 13 . Soit H et K deux sous-groupes d'un groupe fini G avec $ord(H)$ et $ord(K)$ premiers entre eux. Montrer que $H \cap K = \{1_G\}$.
Indication. Si $x \in H \cap K$ alors $x^{ord(H)} = 1_G = x^{ord(K)}$.