Université de Caen **Structures mathématiques pour l'informatique** **Année 2017-2018**
UFR de Sciences **Contrôle terminal, deuxième session.** **juin 2018**

Toutes les réponses doivent être soigneusement justifiées.
La qualité de la rédaction interviendra de manière importante dans la notation.
Durée : 2h

Exercice 1 Soit n un entier supérieur ou égal à 2. On considère l'anneau $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. On note $\mathbb{Z}_n^\times$ le groupe multiplicatif des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. On rappelle que l'ordre d'un groupe fini désigne son cardinal, i.e. son nombre d'éléments. On rappelle que la fonction indicatrice d'Euler , notée ϕ, associe à un entier $n \geq 2$, le nombre d'entiers k dans $[1, n]$ premiers avec n. Par exemple, $\phi(2) = 1$, $\phi(6) = 2$.

1. Donner la liste des éléments de $\mathbb{Z}_5^\times$.
2. Soit p un nombre premier. Quel est l'ordre de $\mathbb{Z}_p^\times$?
3. Donner la liste des éléments de $\mathbb{Z}_{15}^\times$.
4. Soit $n = pq$ avec p et q deux nombres premiers distincts. Montrer que l'ordre de $\mathbb{Z}_n^\times$ est $(p-1)(q-1)$. *Indication :* On rappelle que les seuls nombres qui ne sont pas premiers avec n sont des multiples de p ou des multiples de q.
5. Soit $n = pqr$ avec p, q et r trois nombres premiers deux à deux distincts. Montrer que l'ordre de $\mathbb{Z}_n^\times$ est $(p-1)(q-1)(r-1)$.
6. Calculer $\phi(15)$ et $\phi(30)$.
7. Montrer que lorsque $x \in \{1, \ldots, n-1\}$ est premier avec n, alors $x^{\phi(n)} = 1 \mod n$. *Indication :* Pensez au théorème d'Euler, généralisation du petit théorème de Fermat.
8. Calculer $3^{124356} \mod 7$ et $2^{12435634127} \mod 15$.

Exercice 2
On considère le sous-ensemble $V \subset S_4$ défini par

$$V = \{id, (12)(34), (13)(24), (14)(23)\}.$$

1. Montrer que V est un sous-groupe de S_4.
2. Quel est l'indice $[S_4 : V]$ de V dans S_4 ?
3. Soit W le sous-groupe de S_4 engendré par $(12)(34)$. W est-il un groupe cyclique ?
4. Quel est l'indice $[S_4 : W]$ de W dans S_4 ?
5. Montrer que W est un sous-groupe distingué de V ($W \lhd V$).
6. On rappelle que A_4 désigne le sous-groupe de S_4, formé par les permutations de signature 1. Montrer que W est un sous-groupe de A_4.
7. Quel est l'indice $[A_4 : W]$ de W dans A_4 ?

Exercice 3

1. Soit G un groupe d'ordre 15. Quels sont les ordres possibles pour les sous-groupes de G ?
2. Soit G un groupe fini contenant un élément d'ordre 7 et un élément d'ordre 9. Pourquoi a–t–on $|G| \geq 63$?

Exercice 4
On considère les deux permutations suivantes σ et φ de S_9 définies par :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 5 & 6 & 4 & 2 & 1 & 9 & 7 & 3 \end{pmatrix},$$

$$\varphi = (3,4,1)\,(2,7)\,(3,7)\,(3,5,7,8,)\,(2,6,7)\,(2,9)\,.$$

1. Trouver pour chacune d'elles :
   (a) la décomposition en produit de cycles à supports disjoints,
   (b) la signature,
   (c) l'ordre,
   (d) une décomposition en produit de transpositions
2. Calculer σ^{2018} et φ^{2018}.
3. Calculer $\sigma\varphi\sigma^{-1}$.
4. On rappelle que deux permutations α et β sont conjuguées, si il existe une permutation γ telle que $\alpha = \gamma\beta\gamma^{-1}$. Les permutations σ et φ sont-elles conjuguées ? Justifier.

Exercice 5

Soit $(G, .)$ un groupe. On appelle conjugaison par $a \in G$, l'application f_a de G dans G définie par $f_a(x) = a.x.a^{-1}$. On rappelle qu'un automorphisme de G est un isomorphisme de G dans G et que l'ensemble des automorphismes d'un groupe, muni de $\circ$ (la composition des applications) est un groupe. Il sera noté $Aut(G)$.

1. Montrer que f_a est un automorphisme de G.
2. Soit $\Gamma = \{f_a : a \in G\}$. Montrer que $(\Gamma, \circ)$ est un groupe.
   (Indication : il suffit de montrer que c'est un sous-groupe de $Aut(G)$).
3. Soit $\Phi : G \to \Gamma, a \mapsto f_a$. Vérifier que Φ est un morphisme. Est-il injectif ?
   (Indication : Calculer le noyau $\ker \Phi$, lorsque G est un groupe commutatif).