MT10/P10 - Examen médian

Exercice 1 (groupe symétrique $\mathfrak{S}_n$) (10 points)
On rappelle que $\mathfrak{S}_n$ désigne le groupe des permutations de $[\![1,n]\!]$. Pour toute permutation $\sigma \in \mathfrak{S}_n$, on définit :

$$\begin{array}{rrcl} \text{son support :} & \mathrm{Supp}(\sigma) & \stackrel{\text{déf}}{=} & \{k \in [\![1,n]\!] : \ \sigma(k) \neq k\} \\ \text{sa longueur :} & \mathrm{long}(\sigma) & \stackrel{\text{déf}}{=} & \mathrm{card}(\mathrm{Supp}(\sigma)) \end{array}$$

On rappelle qu'un cycle de $\mathfrak{S}_n$ se note $c = \begin{pmatrix} i_1 & i_2 & \cdots & i_k \end{pmatrix}$, et qu'il faut le comprendre comme

$$c = \begin{pmatrix} i_1 & i_2 & \cdots & i_{k-1} & i_k \\ i_2 & i_3 & \cdots & i_k & i_1 \end{pmatrix},$$

les $n-k$ éléments non représentés restant fixes.

1. Soient σ et $\sigma' \in \mathfrak{S}_n$ tels que $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\sigma') = \emptyset$. Montrer que $\sigma \circ \sigma' = \sigma' \circ \sigma$.
2. Soit $r \in [\![2,n]\!]$ et soit un cycle $c = \begin{pmatrix} i_1 & i_2 & \cdots & i_r \end{pmatrix} \in \mathfrak{S}_n$.
   (a) Quels sont : son support ? sa longueur ? Expliciter $< c >$ le sous-groupe de $\mathfrak{S}_n$ engendré par c. Quel est son ordre ?
   (b) En déduire que pour tout $k \in [\![1,n]\!]$, le groupe $\mathfrak{S}_n$ admet des sous-groupes cycliques d'ordre k.
   (c) Décrire l'action naturelle de $< c >$ sur $[\![1,n]\!]$. Quelle est sa représentation $\rho : < c > \to \mathfrak{S}_n$? Cette action est-elle fidèle ?
   (d) Soit $x \in [\![1,n]\!]$. Décrire son orbite $\mathrm{Orb}(x)$ sous l'action de $< c >$. A quelle condition cette action est-elle transitive ?
   (e) Soit $x \in [\![1,n]\!]$. Que vaut $\mathrm{Stab}(x)$, son stabilisateur sous l'action de $< c >$?
3. Soit maintenant une permutation $\sigma \in \mathfrak{S}_n$ quelconque. On considère encore l'action naturelle de $< \sigma >$ sur $[\![1,n]\!]$.
   (a) Soit $x \in [\![1,n]\!]$. Décrire son orbite $\mathrm{Orb}(x)$ sous l'action de $< \sigma >$. Dans quel cas toutes les orbites n'ont-elles qu'un élément ?
   (b) Pour chaque orbite O non réduite à un élément, on définit une permutation par :

   $$\forall x \in [\![1,n]\!], \qquad \sigma_O(x) \stackrel{\text{déf}}{=} \left| \begin{array}{ccc} x & \text{si} & x \notin O \\ \sigma(x) & \text{si} & x \in O \end{array} \right.$$

   Montrer que σ_O est un cycle. Quel est son support ?
   (c) En déduire une écriture de σ comme composée de cycles à supports disjoints.
4. <u>Mise en pratique</u> : On considère la permutation

   $$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 5 & 2 & 4 & 8 & 9 & 1 & 3 & 6 & 7 \end{pmatrix} \quad \in \mathfrak{S}_{10}$$

   Décomposer σ en produit de cycles disjoints, donner leur ordre, en déduire celui de σ, puis calculer σ^{2010}.

Exercice 2 (anneaux et corps à 4 éléments) (5 points)

1. Dresser les tables d'addition et de multiplication des anneaux $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Montrer que ces anneaux ne sont pas isomorphes, et qu'aucun d'eux n'est un corps.
2. On considère un ensemble à 4 éléments notés $K = \{0, e, \alpha, \beta\}$. L'objectif est de trouver toutes les différentes lois $+$ et $*$ qui font de $(K, +, 0, *, e)$ un corps.
   (a) Expliquer brièvement pourquoi la table de $+$ doit être (au changement de nom près) l'une de celles de la question 1, mais que celle de $*$ est forcément distincte des tables de multiplication des anneaux de la question 1.
   (b) En utilisant le fait que $(K \setminus \{0\}, *, e)$ doit être un groupe, dresser l'unique table de Pythagore possible pour $*$.
   (c) Quelle doit être la caractéristique de K ? Quel est son sous-corps premier ?
   (d) En déduire la table de Pythagore pour $+$.
   (e) Expliciter les éléments de $\mathrm{Aut}(K)$, le groupe des automorphismes de K.
   (f) Développer, dans $K[X]$, le produit $(X - \alpha)(X - \beta)$.
3. Montrer que $X^2 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$. On désigne par $(X^2 + X + 1)$ l'idéal de $\mathbb{F}_2[X]$ qu'il engendre.
4. Expliciter les éléments de $\mathbb{F}_2[X]/(X^2 + X + 1)$ et dresser ses tables d'addition et de multiplication. Reconnaître les tables obtenues pour K.

Exercice 3 (arithmétique variée) (5 points)

1. Déterminer toutes les relations de Bézout $\lambda a + \mu b = \mathrm{pgcd}(a, b)$ pour $a = 236$ et $b = 125$. La droite d'équation $472x + 250y + 1 = 0$ passe-t-elle par des points à coordonnées (x, y) entières ?
2. Pour tout $n \in \mathbb{N}$, on veut calculer le reste de la division euclidienne de 65^n par 9. Expliquer pourquoi le problème est résolu si on calcule les restes des divisions euclidiennes par 9 des nombres de la forme

   $$65^{6k}, \quad 65^{6k+1}, \quad 65^{6k+2}, \quad 65^{6k+3}, \quad 65^{6k+4}, \quad 65^{6k+5}$$

   et calculer ces restes.
3. Résoudre dans $\mathbb{Z}$ le système congruent :

   $$\begin{cases} x = 0 & [2] \\ x = 1 & [3] \\ x = 2 & [5] \end{cases}$$