MT10/P10 - Corrigé de l'examen médian

Exercice 1 (groupe symétrique $\mathfrak{S}_n$) (12 points)

1. Soient σ et $\sigma' \in \mathfrak{S}_n$ tels que $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\sigma') = \emptyset$.
   Il s'agit de montrer que $\forall x \in [\![1,n]\!], \quad \sigma \circ \sigma'(x) = \sigma' \circ \sigma(x)$. Pour cela, on calcule :

$$\sigma \circ \sigma'(x) = \left| \begin{array}{ll} x & \text{si } x \notin \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\sigma') \\ \sigma(x) & \text{si } x \in \mathrm{Supp}(\sigma) \\ \sigma'(x) & \text{si } x \in \mathrm{Supp}(\sigma') \end{array} \right. = \sigma' \circ \sigma(x)$$

   En effet :
   - le premier cas n'utilise que la définition du support,
   - le second cas découle du fait que les supports sont disjoints,
   - le troisième cas utilise en plus le fait que $\mathrm{Supp}(\sigma)$ est stable par σ :

$$x \in \mathrm{Supp}(\sigma) \Longrightarrow \sigma(x) \in \mathrm{Supp}(\sigma)$$

   comme on le voit facilement par contraposée ($\sigma(\sigma(x)) = \sigma(x) \Longrightarrow \sigma(x) = x$ puisque σ est injective ...).

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) $\mathrm{Supp}(c) = \{i_1; i_2; \cdots; i_r\}$
   $\mathrm{long}(c) = r$
   Pour déterminer $< c >$, on calcule c^2, ..., c^k en s'arrêtant au plus petit entier $k > 1$ tel que $c^k = \mathrm{Id}$:

$$\begin{array}{c|cccc} x & i_1 & i_2 & \cdots & i_r \\ c(x) & i_2 & i_3 & \cdots & i_1 \\ c^2(x) & i_3 & i_4 & \cdots & i_2 \\ \vdots & \vdots & & & \\ c^{r-1}(x) & i_r & i_1 & \cdots & i_{r-1} \\ c^r(x) & i_1 & i_2 & \cdots & i_r \end{array}$$

   On a donc $< c >= \{\mathrm{Id}; c; \cdots; c^{r-1}\}$ et $\mathrm{ord}(c) = r$.

   (b) Pour $k = 1$, il suffit de prendre $< \mathrm{Id} >= \{\mathrm{Id}\}$ l'unique sous-groupe d'ordre 1 de $\mathfrak{S}_n$.
   Pour $k \in [\![2,n]\!]$, d'après la question précédente, il suffit de considérer $< c_k >$ où c_k est (par exemple) le cycle $c_k = \begin{pmatrix} 1 & 2 & \cdots & k \end{pmatrix} \in \mathfrak{S}_n$.

   (c) L'action naturelle de $< c >$ sur $[\![1,n]\!]$ est l'application

$$\begin{array}{rcl} \Phi :< c > \times [\![1,n]\!] & \longrightarrow & [\![1,n]\!] \\ (\sigma, x) & \longmapsto & \sigma(x) \end{array}$$

   Sa représentation est

$$\begin{array}{rcl} \rho :< c > & \longrightarrow & \mathfrak{S}_n \\ \sigma & \longmapsto & \sigma \end{array}$$

   ρ est évidemment injective : l'action est donc fidèle.

   (d) Soit $x \in [\![1,n]\!]$.

$$\mathrm{Orb}(x) = \left| \begin{array}{ll} \{x\} & \text{si } x \notin \mathrm{Supp}(c) \\ \mathrm{Supp}(c) & \text{si } x \in \mathrm{Supp}(c) \end{array} \right.$$

   L'action est transitive s'il n'y a qu'une seule orbite. C'est le cas si et seulement si $r = n$, autrement dit si c est un cycle de longueur maximale.

(e) Soit $x \in [\![1,n]\!]$.

$$\mathrm{Stab}(x) = \{\sigma \in < c > : \quad \sigma(x) = x\} = \left| \begin{array}{ll} < c > & \text{si } x \notin \mathrm{Supp}(c) \\ \mathrm{Id} & \text{si } x \in \mathrm{Supp}(c) \end{array} \right.$$

3. Soit maintenant une permutation $\sigma \in \mathfrak{S}_n$ quelconque. On considère encore l'action naturelle de $< \sigma >$ sur $[\![1,n]\!]$.

(a) Soit $x \in [\![1,n]\!]$. Si $x \notin \mathrm{Supp}(\sigma)$, on a $\mathrm{Orb}(x) = \{x\}$; dans tous les cas, on a

$$\mathrm{Orb}(x) = \left\{x; \sigma(x); \ldots; \sigma^{r-1}(x)\right\}$$

pour un certain $r \in [\![1,n]\!]$.
Les orbites ont toutes un seul élément si et seulement si $\sigma = \mathrm{Id}$.

(b) Pour chaque orbite O non réduite à un élément, on définit une permutation par :

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

On a vu à la question précédente que si $y \in O$, on a

$$O = \left\{y; \sigma(y); \ldots; \sigma^{r-1}(y)\right\}$$

Ainsi, σ_O est le cycle $\sigma_O = \begin{pmatrix} y & \sigma(y) & \cdots & \sigma^{r-1}(y) \end{pmatrix} \in \mathfrak{S}_n$, de support $\mathrm{Supp}(\sigma_O) = O$.

(c) Désignons par $O_1, \ldots, O_l$ les orbites non réduites à un élément de l'action de $< \sigma >$ sur $[\![1,n]\!]$, et posons $c_k = \sigma_{O_k}$ pour $k \in [\![1,l]\!]$. Comme orbites, les $O_1, \ldots, O_l$ sont deux à deux disjointes. On a donc

$$c_1 \circ \cdots \circ c_l(x) = \left| \begin{array}{ll} c_k(x) = \sigma(x) & \text{si } x \in O_k \\ x & \text{si } x \notin O_1 \cup \cdots \cup O_l \end{array} \right. \quad = \ \sigma(x)$$

4. Mise en pratique : On considère la permutation

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

Pour décomposer σ en produit de cycles disjoints, il suffit, d'après ce qui précède de calculer les orbites de l'action naturelle de $< \sigma >$.

x	1	2	3	4	5	6	7	8	9	10
$\sigma(x)$	10	5	2	4	8	9	1	3	6	7
$\sigma^2(x)$	7	8	5	4	3	6	10	2	9	1
$\sigma^3(x)$	1	3	8	4	2	9	7	5	6	10
$\sigma^4(x)$	10	2	3	4	5	6	1	8	9	7

On constate qu'il y a une seule orbite à un élément $\{4\}$, et trois autres orbites non réduites à un point. On a $\sigma = c_1 \circ c_2 \circ c_3$ où

$$\begin{aligned} c_1 &= \begin{pmatrix} 9 & 6 \end{pmatrix} \\ c_2 &= \begin{pmatrix} 1 & 10 & 7 \end{pmatrix} \\ c_3 &= \begin{pmatrix} 2 & 5 & 8 & 3 \end{pmatrix} \end{aligned}$$

sont des cycles d'ordres respectifs 2, 3 et 4. Comme

$$\begin{aligned} 2010 &= 0 \quad [2] \\ &= 0 \quad [3] \\ &= 2 \quad [4] \end{aligned}$$

il vient (puisque les c_k commutent)

$$\sigma^{2010} = c_1^{2010} \circ c_2^{2010} \circ c_3^{2010} = c_3^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 8 & 5 & 4 & 3 & 6 & 7 & 2 & 9 & 10 \end{pmatrix}$$

(remarquer que c_3^2 n'est pas un cycle)
Encore puisque les c_k commutent, l'ordre de $\sigma = c_1 \circ c_2 \circ c_3$ est le ppcm des ordres des c_k, soit $\mathrm{ord}(\sigma) = 12$, comme vous pouvez le vérifier par un calcul direct ...

Exercice 2 (anneaux et corps à 4 éléments) (9 points)

1. Tables d'addition et de multiplication de $(\mathbb{Z}/4\mathbb{Z}, +, 0, \cdot, 1)$:

x \ x'	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$x + x'$

x \ x'	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$x \cdot x'$

Tables d'addition et de multiplication de $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +, (0,0), \cdot, (1,1))$:

x \ x'	(0,0)	(1,1)	(1,0)	(0,1)
(0,0)	(0,0)	(1,1)	(1,0)	(0,1)
(1,1)	(1,1)	(0,0)	(0,1)	(1,0)
(1,0)	(1,0)	(0,1)	(0,0)	(1,1)
(0,1)	(0,1)	(1,0)	(1,1)	(0,0)

$x + x'$

x \ x'	(0,0)	(1,1)	(1,0)	(0,1)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(1,1)	(0,0)	(1,1)	(1,0)	(0,1)
(1,0)	(0,0)	(1,0)	(1,0)	(0,0)
(0,1)	(0,0)	(0,1)	(0,0)	(0,1)

$x \cdot x'$

Un isomorphisme d'anneau $f : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ devrait être un isomorphisme des groupes additifs sous-jacents. On devrait donc avoir $f(0) = (0,0)$; et par suite aucun des $f(1)$, $f(2)$,$f(3)$ ne peut être nul (*i.e.* égal à $(0,0)$). Mais, par ailleurs, on devrait aussi avoir :

$$f(2) = f(1+1) = f(1) + f(1) = (0,0)$$

C'est contradictoire. Les groupes $(\mathbb{Z}/4\mathbb{Z}, +, 0)$ et $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +, (0,0))$ ne sont pas isomorphes (ce qui avait été vu en cours et en TD ...), *a fortiori* les anneaux $(\mathbb{Z}/4\mathbb{Z}, +, 0, \cdot, 1)$ et $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +, (0,0), \cdot, (1,1))$ ne peuvent pas être isomorphes.
Aucun de ces anneaux n'est un corps : $2 \neq 0$ et n'a pas d'inverse dans $\mathbb{Z}/4\mathbb{Z}$; $(0,1) \neq (0,0)$ et n'a pas d'inverse dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

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) $(K, +, 0)$ doit être un groupe à 4 éléments. On a vu en cours (et aussi en TD ?) qu'un tel groupe est soit isomorphe à $(\mathbb{Z}/4\mathbb{Z}, +, 0)$, soit isomorphe à $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +, (0,0))$. Par contre, comme aucun des anneaux de la question 1 n'est un corps, la table de $*$ doit être distincte des tables de multiplication ces anneaux.

(b) $(K \setminus \{0\}, *, e)$ doit être un groupe à 3 éléments, dont on a vu en cours l'unicité. La table de Pythagore de la multiplication de $(K, +, 0, *, e)$ doit donc être :

x \ x'	0	e	α	β
0	0	0	0	0
e	0	e	α	β
α	0	α	β	e
β	0	β	e	α

$x * x'$

(c) $\mathrm{car}(K) = 2$ (unique nombre premier qui divise $\mathrm{card}(K) = 4$. Son sous-corps premier est $(\{0, e\}, +, 0, *, e)$, qui isomorphe à $\mathbb{F}_2$.

(d) Puisque $\mathrm{car}(K) = 2$, on doit avoir $e + e = 0$. Parmi les 2 tables possibles pour $+$, seule celle du type $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ convient. On a donc :

x \ x'	0	e	α	β
0	0	e	α	β
e	e	0	β	α
α	α	β	0	e
β	β	α	e	0

$x + x'$

(e) Tout automorphisme $f : K \to K$ doit vérifier $f(0) = 0$ et $f(e) = e$. Pour $f(\alpha)$, il ne reste que 2 choix :
(1) $f(\alpha) = \alpha$, et donc $f = \mathrm{Id}_K$;
(2) $f(\alpha) = \beta$, et donc $f(\beta) = \alpha$.
Vous pouvez vérifier que le second choix donne effectivement un automorphisme. Mais avec les résultats vus en cours, c'est inutile : on sait que K est une extension de degré 2 de $\mathbb{F}_2$, donc $\mathrm{Aut}(K)$ est cyclique d'ordre 2, engendré par l'automorphisme de Frobenius $x \mapsto x^2$ qui est bien l'automorphisme du choix (2) ci-dessus.

(f) Développons, dans $K[X]$, le produit $(X - \alpha)(X - \beta)$:

$$(X - \alpha)(X - \beta) = X^2 - \beta X - \alpha X + \alpha\beta = X^2 \underbrace{-e}_{=e} X + e$$

3. Le polynôme $P(X) = X^2 + X + 1 \in \mathbb{F}_2[X]$ ne s'annule pas sur $\mathbb{F}_2$: on a en effet $P(0) = 1$ et $P(1) = 1$. Donc P n'est divisible ni par X ni par $X - 1 = X + 1$ qui sont les seuls polynômes de degré 1 de $\mathbb{F}_2[X]$. Par conséquent, $X^2 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$.

4. Les éléments de $\mathbb{F}_2[X]/(X^2 + X + 1)$ sont les (classes des) restes possibles dans la division euclidienne des éléments de $\mathbb{F}_2[X]$ par $X^2 + X + 1$, *i.e.* les 4 polynômes de $\mathbb{F}_2[X]$ de degré au plus égal à 1 :

$$0, 1, X, X + 1$$

On calcule les tables d'addition et de multiplication (des polynômes de $\mathbb{F}_2[X]$ modulo $X^2 + X + 1$) :

P \ Q	0	1	X	$X+1$
0	0	1	X	$X+1$
1	1	0	$X+1$	X
X	X	$X+1$	0	1
$X+1$	$X+1$	X	1	0

$P + Q$

P \ Q	0	1	X	$X+1$
0	0	0	0	0
1	0	1	X	$X+1$
X	0	X	$X+1$	1
$X+1$	0	$X+1$	1	X

$P \cdot Q$

On reconnaît les tables de K : il suffit de noter α la classe de X (plutôt que X comme c'est l'usage ...) et β celle de $X+1$.
C'était prévisible puisque X^2+X+1 est justement le polynôme minimal de α sur le sous-corps premier de K.

Exercice 3 (arithmétique variée) (6 points)

1. Pour trouver une relation de Bézout $\lambda a + \mu b = \text{pgcd}(a,b)$ pour $a = 236$ et $b = 125$, on effectue l'algorithme d'Euclide étendu :

$$\begin{array}{rcl@{\qquad}rcl} 236 &=& 125\cdot 1 + 111 & 1\cdot a + (-1)\cdot b &=& 111 \\ 125 &=& 111\cdot 1 + 14 & -1\cdot a + 2\cdot b &=& 14 \\ 111 &=& 14\cdot 7 + 13 & 8\cdot a + (-15)\cdot b &=& 13 \\ 14 &=& 13\cdot 1 + 1 & -9\cdot a + 17\cdot b &=& 1 \end{array}$$

   On en déduit que $\text{pgcd}(a,b) = 1$, et les relations de Bézout :

$$(-9+125k)a + (17-236k)b = 1, \qquad k \in \mathbb{Z}$$

   S'il existait un couple d'entiers $(x,y) \in \mathbb{Z}\times\mathbb{Z}$ tel que $472x + 250y + 1 = 0$, on aurait $2|1$. Par conséquent, la droite d'équation $472x + 250y + 1 = 0$ ne passe par aucun point à coordonnées entières.

2. Pour tout $n \in \mathbb{N}$, on veut calculer le reste de la division euclidienne de 65^n par 9. Pour cela, on calcule modulo 9 les puissances successives de 65 :

$$\begin{array}{rcll} 65 &=& 2 & [9] \\ 65^2 &=& 4 & [9] \\ 65^3 &=& 8 & [9] \\ 65^4 &=& 7 & [9] \\ 65^5 &=& 5 & [9] \\ 65^6 &=& 1 & [9] \end{array}$$

   (Remarque 1 : on ne calcule surtout pas $65\cdot 65$, mais plutôt $2\cdot 2$ ...)
   (Remarque 2 : on voit ici la particularité de l'exposant 6, qui fait tout son intérêt pour le calcul demandé ...)
   On retrouve ensuite "cycliquement" les mêmes résultats :

$$\begin{array}{rcll} 65^{6k} &=& (65^6)^k = 1 & [9] \\ 65^{6k+1} &=& 65^{6k}65 = 2 & [9] \\ 65^{6k+2} &=& 65^{6k}65^2 = 4 & [9] \\ 65^{6k+3} &=& 65^{6k}65^3 = 8 & [9] \\ 65^{6k+4} &=& 65^{6k}65^4 = 7 & [9] \\ 65^{6k+5} &=& 65^{6k}65^5 = 5 & [9] \end{array}$$

3. Soit à résoudre dans $\mathbb{Z}$ le système congruent :

$$\left\{\begin{array}{rcll} x &=& 0 & [2] \\ x &=& 1 & [3] \\ x &=& 2 & [5] \end{array}\right.$$

   Voir TD correspondant. Réponse : $\{22 + 30k \ : \ k \in \mathbb{Z}\}$.