Structures Algébriques 1
Corrigé session 2

Exercice 1. Dans S_6, on considère les permutations

$$\alpha = (1\,3\,6)(2\,4), \text{ et } \beta = (1\,4\,5\,2).$$

1. Déterminer les décompositions en produits de cycles à supports disjoints de $\alpha\beta$ et $\beta\alpha$.
   $\alpha\beta = (1\,2\,3\,6)(4\,5)$; $\beta\alpha = (1\,3\,6\,4)(2\,5)$.
2. Déterminer l'ordre et la signature de α, β, $\alpha\beta$ et $\beta\alpha$.
   - α est d'ordre 6, β d'ordre 4, $\alpha\beta$ d'ordre 4 ainsi que $\beta\alpha$.
   - $\epsilon(\alpha) = \epsilon(\beta) = -1$; $\epsilon(\alpha\beta) = \epsilon(\beta\alpha) = +1$

Exercice 2. (*Résolution d'équations dans $\mathbb{Z}/n\mathbb{Z}$*)

1. Soient a et b deux entiers premiers entre eux.
   (a) Rappeler pourquoi il existe un entier a' tel que $aa' \equiv a'a \equiv 1 \mod b$.
   C'est Bézout.
   (b) Si c est un entier quelconque, décrire l'ensemble des entiers x tels que $ax \equiv c \mod b$, en fonction de b, c et a'.
   Application : déterminer l'ensemble des entiers a tels que $2a \equiv 9 \mod 11$.
   On a les équivalences

   $$ax \equiv c \mod b \Leftrightarrow a'ax \equiv a'c \mod b \Leftrightarrow x \equiv a'c \mod b.$$

   L'ensemble cherché est donc égal à $a'c + b\mathbb{Z}$.
   Application :

   $$13a \equiv 108 \mod 11 \Leftrightarrow 2a \equiv 9 \mod 11 \Leftrightarrow a \equiv 6 \times 9 \equiv 10 \mod 11$$

   puisque l'inverse de 2 modulo 11 est égal à 6.
2. Soit P un polynôme non nul à coefficients dans un anneau A.
   (a) *Question de cours :* que peut-on dire du nombre de racines de P dans A si A est intègre ? Le nombre de racines de P dans A est majoré par le degré de P.
   (b) Résoudre l'équation $x^2 = 1$ dans $\mathbb{Z}/8\mathbb{Z}$ et dans $\mathbb{Z}/73\mathbb{Z}$.
   Comme 73 est premier, l'anneau $\mathbb{Z}/73\mathbb{Z}$ est intègre (c'est même un corps). Par conséquent, le polynôme $X^2 - 1$ a au plus 2 racines dans $\mathbb{Z}/73\mathbb{Z}$, et il en a en fait exactement 2, à savoir 1 et -1. En revanche $\mathbb{Z}/8\mathbb{Z}$ n'est pas intègre, et la majoration précédente ne s'applique pas. Un examen de tous les éléments de $\mathbb{Z}/8\mathbb{Z}$ montre que l'équation $x^2 = 1$ a dans ce cas 4 racines, à savoir 1, -1, 3 et -3.

Exercice 3. Soient G et H deux groupes et f un morphisme de G dans H.
Dans les quatre premières questions, on notera multiplicativement les lois de groupe de G et H.

1. Soit K un sous-groupe de G.

(a) Montrer que $f(K)$ est un sous-groupe de H.

$f(K)$ est non vide car il contient $e_H = f(e_G)$. Si $y_1 = f(k_1)$ et $y_2 = f(k_2)$ sont deux éléments de $f(K)$, k_1 et k_2 appartenant à K, alors $k_1 k_2^{-1}$ appartient à K puisque celui-ci est un sous-groupe de G, et $y_1 y_2^{-1} = f(k_1)f(k_2)^{-1} = f(k_1 k_2^{-1})$ – on utilise ici le fait que f est un morphisme – est l'image par f d'un élément de K donc appartient à $f(K)$. Ceci permet de conclure que $f(K)$ est un sous-groupe de H, grâce au critère vu en cours.

(b) On suppose de plus que f est surjectif et que K est un sous-groupe distingué de G. Montrer qu'alors, $f(K)$ est un sous-groupe distingué de H.

Soient $y = f(k)$ un élément de $f(K)$, avec k élément de K, et x un élément quelconque de H. Comme f est surjectif, il existe $g \in G$ tel que $x = f(g)$, auquel cas $x^{-1}yx = f(g)^{-1}f(k)f(g) = f(g^{-1}kg)$ puisque f est u morphisme. Comme $K \lhd G$, le produit $g^{-1}kg$ appartient à K et $x^{-1}yx$ appartient donc bien à $f(K)$.

2. Soit $g \in G$ un élément d'ordre fini. Montrer que l'ordre de $f(g)$ est fini et divise celui de g.

   Si g est d'ordre n, alors $f(g)^n = f(g^n) = f(e_G) = e_H$, donc $f(g)$ est d'ordre fini et son ordre divise n.

3. On suppose dans cette question que G et H sont finis. Montrer que pour tout $g \in G$, l'ordre de $f(g)$ est un diviseur commun de l'ordre de G et de l'ordre de H.

   D'après la question précédente, l'ordre de $f(g)$ divise celui de g et divise donc l'ordre de G, grâce au théorème de Lagrange. Par ailleurs, toujours grâce au même théorème, l'ordre de $f(g)$ divise l'ordre H, puisque c'est un élément de H.

4. On considère dans cette question les groupes *additifs* $G = (\mathbb{Z}/6\mathbb{Z}, +)$ et $H = (\mathbb{Z}/8\mathbb{Z}, +)$. Décrire tous les morphismes de groupes de G dans H.

   On note $\overline{k}$ et $\widetilde{k}$ les classes d'un entier k modulo 6 et 8 respectivement. Si f est un morphisme de $(\mathbb{Z}/6\mathbb{Z}, +)$ dans $(\mathbb{Z}/8\mathbb{Z}, +)$, alors, en vertu des résultats précédents, l'ordre de l'élément $f(\overline{1})$ est un diviseur commun de 6 et de 8, c'est-à-dire un diviseur de 2. Il y a donc deux cas à envisager :

   - Si l'ordre de $f(\overline{1})$ vaut 1, alors $f(\overline{1}) = \widetilde{0}$. Il existe un unique morphisme satisfaisant cette condition à savoir le morphisme "trivial" $f(\overline{k}) = \widetilde{0}$ pour tout $\overline{k} \in \mathbb{Z}/6\mathbb{Z}$.
   - Si l'ordre de $f(\overline{1})$ vaut 2, alors $f(\overline{1}) = \widetilde{4}$, unique élément d'ordre 2 dans $\mathbb{Z}/8\mathbb{Z}$. On vérifie immédiatement que l'application

   $$\begin{aligned} f : \mathbb{Z}/6\mathbb{Z} &\longrightarrow \mathbb{Z}/8\mathbb{Z} \\ \overline{k} &\longmapsto f(\overline{k}) = \begin{cases} \widetilde{0} \text{ si } k \text{ est pair} \\ \widetilde{4} \text{ si } k \text{ est impair} \end{cases} \end{aligned}$$

   est bien un morphisme de $(\mathbb{Z}/6\mathbb{Z}, +)$ dans $(\mathbb{Z}/8\mathbb{Z}, +)$, et c'est le seul qui satisfasse la condition $f(\overline{1}) = \widetilde{4}$.

   Il y a donc deux morphismes distincts de $(\mathbb{Z}/6\mathbb{Z}, +)$ dans $(\mathbb{Z}/8\mathbb{Z}, +)$.

Exercice 4. Soit A un anneau *commutatif*, dont on note 0 l'élément neutre additif et 1 l'élément neutre multiplicatif. On suppose en outre que A n'est pas réduit à $\{0\}$.

On dit qu'un élément $a \in A$ est nilpotent s'il existe un entier naturel non nul n tel que $a^n = 0$.

Dans la suite, on note N l'ensemble des éléments nilpotents de A et $A^\times$ l'ensemble des éléments inversibles pour la multiplication.

1. Déterminer N et $A^\times$ dans les cas suivants :

   (a) $A = \mathbb{Z}/4\mathbb{Z}$.

   $N = \{\overline{0}, \overline{2}, \}$, $A^\times = \{\overline{1}, \overline{3}\}$.

(b) $A = \mathbb{Z}/6\mathbb{Z}$.
$N = \{\overline{0}\}$, $A^\times = \{\overline{1}, \overline{5}\}$.

(c) $A = \mathbb{Z}/12\mathbb{Z}$.
$N = \{\overline{0}, \overline{6}\}$, $A^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$.

2. Les groupes $(\mathbb{Z}/4\mathbb{Z})^\times$, $(\mathbb{Z}/6\mathbb{Z})^\times$ et $(\mathbb{Z}/12\mathbb{Z})^\times$ sont-ils cycliques ?

   $(\mathbb{Z}/4\mathbb{Z})^\times = \{\overline{1}, \overline{3}\} = \langle \overline{3} \rangle$ et $(\mathbb{Z}/6\mathbb{Z})^\times = \{\overline{1}, \overline{5}\} = \langle \overline{5} \rangle$ sont cycliques d'ordre 2. En revanche $(\mathbb{Z}/12\mathbb{Z})^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$ n'est pas cyclique car il ne contient pas d'élément d'ordre 4.

3. Soit $a \in A$ un élement nilpotent. Montrer que $1-a$ est inversible [*considérer le produit* $(1-a)(1+a+\cdots+a^k)$*, pour un entier naturel* k *bien choisi*].

   Soit n un entier naturel non nul tel que $a^n = 0$. Alors $(1-a)\sum_{k=0}^{n-1} a^k = 1 - a^n = 1$, moyennant quoi $1-a$ est inversible, d'inverse $\sum_{k=0}^{n-1} a^k$.

4. Montrer que si x et y sont nilpotents alors $x+y$ est nilpotent.

   Soient n et m deux entiers naturels non nuls tels que $x^n = y^m = 0$. L'anneau A étant commutatif, on peut appliquer la formule du binôme pour obtenir

$$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k} = \sum_{k=0}^{n} \binom{n+m}{k} x^k y^{n+m-k} + \sum_{k=n+1}^{n+m} \binom{n+m}{k} x^k y^{n+m-k}.$$

   Dans chacun des termes de la deuxième somme, l'exposant de x est plus grand que n, moyennant quoi tous ces termes sont nuls ; dans les termes de la première somme, c'est l'exposant $n+m-k$ de y est qui est supérieur ou égal à m, ce qui entraîne à nouveau la nullité de tous les termes. Au final, $(x+y)^{n+m} = 0$.

5. Montrer que N est un idéal de A.

   N est non vide car il contient 0. La question précédente, jointe au fait que l'opposé $-x$ d'un élément nilpotent x est évidemment nilpotent, montre que Nest un sous-groupe additif. Par ailleurs, si x est nilpotent, et si n est un entier naturel tel que $x^n = 0$, on a, pour tout $a \in A$

$$(ax)^n = a^n x^n = 0,$$

   moyennant quoi ax est nilpotent. Noter que, dans le calcul précédent, on a à nouveau utilisé la commutativité de A pour pouvoir écrire $(ax)^n = a^n x^n$.

Exercice 5.

On considère un groupe G d'ordre 143 opérant sur un ensemble X de cardinal 108. Le but de l'exercice est de montrer que cette action possède nécessairement des points fixes (on rappelle qu'un point x de X est fixe sous l'action de G si son orbite est réduite à un point, c'est-à-dire si $\forall g \in G,\ g \cdot x = x$)

1. Quelles sont les cardinaux possibles pour les orbites de l'action de G sur X ?

   L' orbite d'un élément x est en bijection avec le quotient G/G_x de G par le stabilisateur G_x de x. Par conséquent, son cardinal est un diviseur de l'ordre de $G = 143 = 11 \times 13$, qui doit en outre être inférieur ou égal à $108 = |X|$. Les valeurs possibles sont donc 1, 11 et 13.

2. Supposons, par l'absurde, que cette action ne possède pas de point fixe et notons a et b le nombre d'orbites de cardinal 13 et 11 respectivement.

(a) Appliquer la formule des classes pour obtenir une équation liant a et b.

S'il n'y a pas de points fixes, les orbites sont toutes de longueur 11 ou 13, et la formule des classes fournit l'équation

$$13a + 11b = 108. \tag{1}$$

(b) Conclure en montrant que cette équation n'a pas de solution dans $\mathbb{N}^2$.

Comme a et b sont des entiers positifs, on doit avoir $a \leq 8$ et $b \leq 9$ pour satisfaire les inégalités $13a \leq 108$ et $11b \leq 108$ découlant de (1). Par ailleurs, cette équation entraîne que $13a \equiv 108 \mod 11$, soit $a \equiv 10 \mod 11$, ce qui n'est pas compatible avec la contrainte $0 \leq a \leq 8$. L'équation (1) n'a donc pas de solution dans $\mathbb{N}^2$.