Séance 3 : Structures algébriques (groupes)

Exercice 3.1. Pour chacune des structures algébriques suivantes, déterminer s'il s'agit d'un monoïde, en précisant quel est l'élément neutre et quels sont les éléments inversibles le cas échéant, puis s'il s'agit d'un groupe :

1. $\mathbb{N}$ muni de l'addition usuelle ;
2. $\mathbb{N}$ muni de la multiplication usuelle ;
3. $\mathbb{Z}$ muni de l'addition usuelle ;
4. $\mathbb{Z}$ muni de la multiplication usuelle ;
5. $\mathbb{Q}$ muni de l'addition usuelle ;
6. $\mathbb{Q}$ muni de la multiplication usuelle ;
7. $\mathbb{Q}^{m\times n}$, avec $m, n \in \mathbb{N}\setminus\{0\}$, muni de la fonction $(A, B) \mapsto ARB$ où $R \in \mathbb{Q}^{n\times m}$ avec $\operatorname{rang} R = \min\{m, n\}$;
8. A^A, avec A un ensemble non vide, muni de la composition ;
9. $\mathscr{P}(A)$, avec A un ensemble non vide, muni de l'intersection ;
10. $\mathscr{P}(A)$, avec A un ensemble non vide, muni de l'union.

Exercice 3.2. Soit un triangle équilatéral de sommets A, B et C.

1. Définir l'ensemble des symétries du triangle ABC. Par symétrie, on entend une transformation du triangle qui le ramène à lui-même, éventuellement avec permutation des sommets.
2. Montrer que ces symétries, prises avec la composition comme opération, forment un groupe.
   On se rend compte que les éléments du groupe sont des fonctions et, plus particulièrement, des permutations sur l'ensemble $\{A, B, C\}$.
3. Montrer que ce groupe n'est pas commutatif.
4. Écrire la table de Cayley (table d'opération) de ce groupe.

> Soient A et B deux ensembles **finis**. Si $|A| = |B|$, alors pour toute fonction de A dans B, l'injectivité, la surjectivité et la bijectivité sont des propriétés équivalentes.

Exercice 3.3. Dans un monoïde A, un *inverse à gauche* de $a \in A$ est un élément $b \in A$ tel que $ba = 1$ alors qu'un *inverse à droite* de a est un élément $b \in A$ tel que $ab = 1$.

1. Démontrer que, dans un monoïde fini, tout inverse à gauche est aussi un inverse à droite. Autrement dit, si un élément possède un inverse à gauche, alors cet élément est inversible.
   Indication. Commencer par montrer que, si un élément a admet un inverse à gauche, alors a admet un inverse à droite. Démontrer pour cela que l'application $f : x \mapsto ax$ est injective. Montrer ensuite que cet inverse à droite est inverse à gauche.
2. Le résultat énoncé au point précédent reste-t-il vrai pour des monoïdes infinis ? Considérer dans $\mathbb{N}^{\mathbb{N}}$ les fonctions $a : t \mapsto \lfloor t/2 \rfloor$ et $b : t \mapsto 2t$.
   Notation. Pour tout réel x, $\lfloor x \rfloor$ désigne la *partie entière par défaut* de x, c'est-à-dire le plus grand entier inférieur ou égal à x.
3. (Août 2020.) Démontrer que, si tous les éléments d'un monoïde possèdent un inverse à gauche, alors le monoïde est un groupe.
   Indication. Considérer un inverse à gauche d'un inverse à gauche d'un élément a.

Exercice 3.4. Soit G un groupe et $H \subset G$. Montrer que H est un sous-groupe de G si :

- H contient au moins un élément et
- $\forall x, y \in H$, le produit xy^{-1} est un élément de H

Exercice 3.5. Dans le groupe additif $\mathbb{Z}_9$, que valent $\langle 1 \rangle$, $\langle 2 \rangle$ et $\langle 3 \rangle$? Quel est l'inverse de 5 ?

Exercice 3.6. Pour tout entier $n > 1$, soit $\mathbb{Z}_n^*$ l'ensemble des éléments inversibles dans le monoïde $\mathbb{Z}_n := \{0, \ldots, n-1\}$ muni de la multiplication modulo n. Calculer $|\mathbb{Z}_n^*|$ si n est le produit de deux nombres premiers distincts.
Indication. Utiliser le résultat du cours suivant :

$$\mathbb{Z}_n^* = \{x \in \{1, \ldots, n-1\} \mid \gcd(x, n) = 1\}.$$

Exercice 3.7. On se place dans le groupe multiplicatif $\mathbb{Z}_{13}^*$.

1. Quelles valeurs peut prendre l'ordre d'un élément quelconque ?
2. Quels sont les ordres respectifs de 2, 3, 4 et 5 ?
3. Combien y a-t-il de classes latérales modulo $\langle 5 \rangle$? Quelles sont-elles ? Écrire la table de Cayley du groupe quotient $\mathbb{Z}_{13}^* / \langle 5 \rangle$.
4. Résoudre l'équation $x^{2019} = 5$.
5. Trouver $n \in \{0, \ldots, 11\}$ tel que $11^n = 2$.

Exercice 3.8 (août 2020 : casser le protocole de Diffie-Hellman)**.** Supposons que Alice et Bob exécutent le protocole de Diffie-Hellman, et que Ève écoute leurs communications. Ève apprend ainsi que Alice et Bob ont choisi d'employer le groupe multiplicatif $\mathbb{Z}_p^*$ avec $p := 7$ et le générateur $g := 3$, et observe que Alice et Bob échangent $g^x = 2$ et $g^y = 5$. Que vaut g^{xy} ?

Exercice 3.9. Soit S_n le groupe des permutations sur $\{0, \ldots, n-1\}$.

1. Vérifier que S_n est un groupe.
2. Quel est l'ordre de S_n ?
3. Donner des générateurs des sous-groupes d'ordres 2 et 3 de S_3.
4. On a vu au cours que tout monoïde A peut être décrit comme un sous-monoïde de A^A. On se propose ici de démontrer le *théorème de Cayley* : tout groupe fini d'ordre n est isomorphe à un sous-groupe de S_n. Vérifier pour cela que, si $G := \{x_0, \ldots, x_{n-1}\}$ est un groupe fini d'ordre n, la fonction f suivante définit bien un isomorphisme vers un sous-groupe de S_n :

   $$f : G \to S_n : x_i \mapsto \pi_i \text{ où } \pi_i(j) := k \text{ avec } x_i x_j = x_k.$$

   Autrement dit, pour chaque $i \in \{0, \ldots, n-1\}$, π_i est l'élément de S_n qui à chaque $j \in \{0, \ldots, n-1\}$ associe l'unique $k \in \{0, \ldots, n-1\}$ tel que $x_i x_j = x_k$.
5. On peut construire un graphe orienté d'ordre n à partir d'un élément π de S_n en plaçant une arête de i à $\pi(i)$ pour chaque $i \in \{0, \ldots, n-1\}$. Dessiner le graphe généré par chacun des éléments de S_3. Dessiner le graphe généré par la permutation $x^3 + 2 \bmod 11$ interprétée comme un élément de S_{11}. Expliquer pourquoi tout graphe de ce type sera formé de cycles disjoints.