TD n°3 : Algèbre I

Informatique Appliquée - S1 - 2023/2024 - Pr. El Mahjour

Groupes, anneaux et corps finis

Exercice 1

Soit G un ensemble non-vide muni d'une loi de composition interne $*$ associative qui vérifie de plus les assertions suivantes :

- $\exists e \in G, \forall x \in G, \quad x * e = x.$
- $\forall x \in G, \exists y_x \in G$ tel que $x * y_x = e.$

Montrer que $(G, *)$ est un groupe. [01]

Exercice 2

On considère le groupe des permutations $\mathfrak{S}_5$. Soit $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$ et $\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$ et $\sigma_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 3 & 5 \end{pmatrix}$

1. Calculer σ_1^2 et en déduire σ_1^{-1}.
2. Quel est l'ordre de σ_4 ?
3. Sans faire de calculs dire si : $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$? $\sigma_3 \circ \sigma_1 = \sigma_1 \circ \sigma_3$?
4. Comment appelle-t-on σ_1 et σ_2 ? Représentez-les autrement.
5. Quelle est la relation entre σ_1, σ_2 et σ_3.

[02]

Exercice 3

Pour tout couple (a,b) de $\mathbb{R}^2$, on pose la matrice $M_{a,b} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. Soit $\mathscr{S} = \left\{ M_{a,b} : (a,b) \in \mathbb{R}^2 \right\}$. Soit l'application

$$\begin{array}{rccc} f: & \mathscr{S} & \longrightarrow & \mathbb{C} \\ & M_{a,b} & \longmapsto & a + ib. \end{array}$$

1. Montrer que $(\mathscr{S}, +)$ est un sous-groupe pour la loi usuelle d'addition des matrices carrées $\mathscr{M}_2(\mathbb{R})$.
2. Montrer que f est un isomorphisme du groupe $(\mathscr{S}, +)$ dans le groupe $(\mathbb{C}, +)$.

[03]

Exercice 4

1. Montrer que $(\mathbb{Z}/3\mathbb{Z}, +, \times)$ est un corps fini.
2. Cherchez des structures de corps à 4 éléments.

[04]

1 Artihmétique dans $\mathbb{Z}$

Exercice 5

1. Calculer $37+35$ modulo 63 et 37×55 modulo 63.
2. Trouver le $pgcd(433014481, 18000)$ en décomposant 18000 en produit de facteurs premiers.
3. Pour les questions qui suivent, on peut utiliser une petite calculatrice :
   (a) Calculer le $pgcd$ de $a = 42098$ et de $b = 36146$ avec l'algorithme d'Euclide.
   (b) Retrouver ce résultat en décomposant a et b en produit de facteurs premiers.
   (c) Déterminer des entiers u et v tels que $pgcd(a,b) = au + bv$.
   (d) Quel est l'inverse de 583 dans $\mathbb{Z}/679\mathbb{Z}$.

[05]

Exercice 6 Petit théorème de Fermat [1]

1. Soient p un nombre premier et k un entier tel que $1 \leqslant k < p$. Montrer que C_p^k est divisible par p.
2. Montrer que $a^p \equiv a\ [p]$ pour tout entier a par récurrence sur a

[06]

1. Petit exercice supplémentaire : démontrez que l'équation $x^n + y^n = z^n$ n'a pas de solutions en entiers strictement positifs, pour tout entier $n > 2$. *La légende dit que Pierre Fermat n'avait pas assez de place sur la marge de son cahier pour compléter la preuve de ce théorème.*