TD 7 - Algébre et arithmétique

Structures algébriques

Exercice 1 (Quelques groupes)**.** Parmi les exemples suivants, lesquels sont des groupes ?

a. $(\mathbb{N},+)$, $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$

b. $(\mathbb{N}^*,+)$, $(\mathbb{Z}^*,+)$, $(\mathbb{Q}^*,+)$, $(\mathbb{R}^*,+)$, $(\mathbb{C}^*,+)$

c. $(\mathbb{N},\times)$, $(\mathbb{Z},\times)$, $(\mathbb{Q},\times)$, $(\mathbb{R},\times)$, $(\mathbb{C},\times)$

d. $(\mathbb{N}^*,\times)$, $(\mathbb{Z}^*,\times)$, $(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,\times)$, $(\mathbb{C}^*,\times)$

e. Soit E un ensemble. L'ensemble des fonctions de E dans E muni de la composition est-il un groupe ? Qu'en est-il de l'ensemble des fonctions injectives ? surjectives ? bijectives ?

Exercice 2 (Structure additive de $\mathbb{Z}/n\mathbb{Z}$)**.** Montrer que $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe abélien.

Exercice 3 (Groupe et logique)**.** Soit $G = \{\text{Faux}, \text{Vrai}\}$. Pour chacune des lois $\star$ suivantes, dire si $(G,\star)$ forme un groupe ou non.

$$(G,\vee) \qquad (G,\wedge) \qquad (G,\Rightarrow) \qquad (G,\Leftrightarrow) \qquad (G,\oplus)$$

Exercice 4 (Groupes de fonctions)**.**

a. On considère l'ensemble $F = \{f\colon \mathbb{R}\to\mathbb{R}, x\mapsto ax+b \ : \ a,b\in\mathbb{R}, a\neq 0\}$.

i. Montrer que F est stable par composition : $\forall f,g\in F,\quad f\circ g\in F$.

ii. Montrer que F muni de la composition $\circ$ forme un groupe.

b. Soit E un ensemble et $(G,+)$ un groupe abélien. On considère l'ensemble $F=\{f\colon E\to G\}$. On munit F de la loi de composition $\boxplus\colon F\times F\to F$ définie par :

$$\forall f,g\in F, \forall x\in E \quad (f\boxplus g)(x) \coloneqq f(x)+g(x).$$

i. Montrer que la loi $\boxplus$ sur F est bien définie.

ii. Montrer que $(F,\boxplus)$ forme un groupe abélien.

Exercice 5 (Structure multiplicative de $\mathbb{Z}/n\mathbb{Z}$)**.** Soit $n\geq 2$.

a. Montrer que $(\mathbb{Z}/n\mathbb{Z},+,\times)$ est un anneau commutatif.

b. On considère le sous-ensemble $\mathbb{Z}/n\mathbb{Z}^\times\subset\mathbb{Z}/n\mathbb{Z}$ formé des éléments qui admettent un inverse multiplicatif.

i. Rappeler la définition de « x admet un inverse multiplicatif ».

ii. Construire la table de multiplication de $\mathbb{Z}/6\mathbb{Z}$. Décrire $\mathbb{Z}/6\mathbb{Z}^\times$. $(\mathbb{Z}/6\mathbb{Z},+,\times)$ est-il un corps ?

iii. Montrer que $(\mathbb{Z}/n\mathbb{Z},\times)$ n'est pas un groupe mais que $(\mathbb{Z}/n\mathbb{Z}^\times,\times)$ est un groupe.

Exercice 6 (Anneau de fonctions)**.** Soit E un ensemble. Soit $(A,+,\times)$ un anneau. En s'inspirant de l'Exercice 4, montrer que l'on peut munir l'ensemble $F=\{f\colon E\to A\}$ d'une structure d'anneau.

PGCD et algorithme d'Euclide étendu

Exercice 7 (Propriétés du PGCD et algorithme d'Euclide)**.**

a. Soit $a, b \in \mathbb{Z}$. Montrer que pour tout entier $k \in \mathbb{Z}$:

i. L'ensemble des diviseurs communs à a et b est égale à l'ensemble des diviseurs communs à $a + bk$ et b.

ii. $\text{pgcd}(a, b) = \text{pgcd}(a + bk, b)$.

b. En déduire les propositions suivantes :

i. Si q et r sont le quotient et le reste de la division euclidienne de a par b alors, $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

ii. L'algorithme d'Euclide est correct et termine.

iii. Les diviseurs communs à a et b sont exactement les diviseurs de $\text{pgcd}(a, b)$.

Exercice 8 (Algorithme d'Euclide (étendu))**.** **a.** Sans utiliser l'algorithme d'Euclide, calculer $\text{pgcd}(105, 12)$.

b. Retrouver le même résultat avec l'algorithme d'Euclide.

c. Que vaut $\text{pgcd}(a, b)$ pour $(a, b) = (167, 115)$? pour $(a, b) = (153, 40)$?

d. Pour chacune des paires (a, b) trouver $u, v \in \mathbb{Z}$ tels que $au + bv = \text{pgcd}(a, b)$.

Exercice 9 (Quelques équations diophantiennes)**.** **a.** Trouver une solution particulière, $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$, de l'équation $1075x + 63y = 1$.

b. Montrer que l'équation $1075x + 63y = 1$ admet une infinité de solutions entières et déterminer l'ensemble de solutions.

c. Prouver que l'équation $756x + 245y = 13$ n'admet aucune solution entière.

Exercice 10 (Inverses et équations modulaires)**.** **a.** 5 est-il inversible modulo 15 ? modulo 13 ? Si oui quel est son inverse ?

b. 110 est-il inversible modulo 63 ? modulo 32 ? Si oui quel est son inverse ?

c. Résoudre dans $\mathbb{Z}/13\mathbb{Z}$ l'équation $5x = 1$. En déduire les solutions dans $\mathbb{Z}$ de l'équation $5x \equiv 1 \bmod 13$.

Exercice 11 (Théorème des restes chinois)**.** **a.** On considère le système d'équations suivant :

$$\begin{cases} x \equiv 9 \bmod 17 \\ x \equiv 3 \bmod 10 \end{cases}$$

i. En observant que 10 et 17 sont premiers entre eux, trouver une solution particulière $x_0 \in \mathbb{Z}$ du système.

ii. Soit $x \in \mathbb{Z}$. Montrer que si x est une solution du système alors, $x \in x_0 + 170\mathbb{Z}$.

iii. Montrer que l'ensemble des solutions entières du système est exactement $x_0 + 170\mathbb{Z}$.

b. On considère le système d'équations suivant :

$$\begin{cases} x \equiv 3\ [17] \\ x \equiv 4\ [11] \\ x \equiv 5\ [6] \end{cases}$$

i. En observant que les modules sont 2 à 2 premiers entre eux, trouver une solution particulière $x_0 \in \mathbb{Z}$ du système.

ii. Soit $x \in \mathbb{Z}$. Montrer que si x est une solution du système alors, $x \in x_0 + 17 \cdot 11 \cdot 6\mathbb{Z}$.

iii. Montrer que l'ensemble des solutions entières du système est exactement $x_0 + 17 \cdot 11 \cdot 6\mathbb{Z}$.