Anneaux

1 Introduction aux anneaux

Exercice 1. Les anneaux $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/5\mathbb{Z}$.
Dressez les tables de Cayley des lois + et × de $\mathbb{Z}/4\mathbb{Z}$ puis que $\mathbb{Z}/5\mathbb{Z}$. Quels sont les éléments inversibles de chacun des anneaux ?

Exercice 2. Éléments neutres.

1) Que valent les éléments 0_A et 1_A pour l'anneau $A = (\mathbb{Z}/2\mathbb{Z})^2$?
2) Même question pour $A = \mathcal{P}(\{1,2\})$.

Exercice 3. Calculs dans un anneau.
Pour chacun des éléments a suivants vus dans leur anneaux respectifs, donnez $-a$, $3a$, a^2 et (s'il existe) a^{-1}.

1) $4 \in \mathbb{Z}$
2) $4 \in \mathbb{Z}/5\mathbb{Z}$
3) $X+1 \in \mathbb{R}[X]$
4) $X+1 \in (\mathbb{Z}/2\mathbb{Z})[X]$
5) $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \mathcal{M}_2(\mathbb{R})$
6) $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \mathcal{M}_2(\mathbb{Z}/2\mathbb{Z})$

Exercice 4. Le groupe $\mathbb{Z}/4\mathbb{Z}^\times$.
En vous aidant de l'exercice 1, donnez les éléments des groupes $\mathbb{Z}/4\mathbb{Z}^\times$ et $\mathbb{Z}/5\mathbb{Z}^\times$.

Exercice 5. Calcul d'inverses dans $\mathbb{Z}/n\mathbb{Z}$.

1) Calculez les inverses (s'ils existent) de 11 et 15 dans $\mathbb{Z}/20\mathbb{Z}$.
2) Calculez les inverses (s'ils existent) de 1, 3 et 11 dans $\mathbb{Z}/111\mathbb{Z}$.
3) Trouvez de tête les inverses de 1, 2, 3 et 4 dans $\mathbb{Z}/5\mathbb{Z}$.

Exercice 6. Indicatrice d'Euler.

1) Calculez $\phi(n)$ pour tout entier $2 \leq n \leq 10$.
2) Que vaut $\phi(p)$ si p est un nombre premier ?

Exercice 7. Preuve du théorème d'Euler-Fermat.
Vous savez que le groupe $\mathbb{Z}/n\mathbb{Z}^\times$ est d'ordre $\phi(n)$. Le théorème précédent est alors un corollaire immédiat d'un résultat du chapitre précédent sur les ordres. Rédigez une preuve de ce théorème.

2 Chiffrement de Hill

Exercice 8. Matrice inversible, ou pas.
Considérons la matrice $M \in \mathcal{M}_3(A)$ définie par

$$M = \begin{pmatrix} 1 & 2 & 1 \\ 4 & 0 & 2 \\ 1 & 3 & 1 \end{pmatrix}.$$

Cette matrice est-elle inversible si $A = \mathbb{R}$? $A = \mathbb{Z}$? $A = \mathbb{Z}/6\mathbb{Z}$? $A = \mathbb{Z}/7\mathbb{Z}$?

Exercice 9. Chiffrement de Hill 1.
Posons $m = 2$ et $n = 3$. Avec ces paramètres, le chiffrement de Hill traite des éléments de $(\mathbb{Z}/2\mathbb{Z})^3$, donc permet de chiffrer des blocs de 3 bits. Considérons la matrice E dans $\mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$ donnée ci-dessous avec son inverse $D = E^{-1}$:

$$E = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad D = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

1) Vérifiez que $E \times D = \mathrm{Id}_3$ dans $\mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$.
2) Chiffrez tous les messages de $(\mathbb{Z}/2\mathbb{Z})^3$ avec la clé E.
3) Trouvez deux messages p et p' ayant seulement 1 bit différent tels que :
   3.1) c et c' ont 2 bits différents ;
   3.2) c et c' ont 3 bits différents.

Exercice 10. Chiffrement de Hill 2.
Considérons le chiffrement de Hill avec $m = 5$ et $n = 3$. Il permet donc de chiffrer un message dans $(\mathbb{Z}/5\mathbb{Z})^3$ avec une clé dans $\mathrm{GL}_3(\mathbb{Z}/5\mathbb{Z})$.

1) Expliquez pourquoi la matrice suivante appartient à $\mathrm{GL}_3(\mathbb{Z}/5\mathbb{Z})$ sans calculer son inverse.
$$E = \begin{pmatrix} 1 & 2 & 1 \\ 4 & 0 & 2 \\ 1 & 3 & 1 \end{pmatrix}.$$
2) Calculez son inverse $D = E^{-1}$ puis vérifiez que $E \times D = \mathrm{Id}_3$.
3) Chiffrez puis déchiffrez le message $p = (1, 2, 3)$.

Exercice 11. Cryptanalyse de Hill.
Votre mission, que vous acceptez, est la suivante. Nous venons d'intercepter le message chiffré c et grâce à des techniques de ... persuasion, nous avons obtenu le message clair p associé :

$$p = (1,3,0, \quad 2,0,1, \quad 1,3,2, \quad 3,0,0),$$
$$c = (2,1,3, \quad 0,1,0, \quad 2,3,3, \quad 3,0,2).$$

Le chiffrement utilise les paramètres $m = 4$, $n = 3$. À vous de retrouver la clé de chiffrement. Cette mission conditionne le succès d'un projet *top secret*. Malheureusement nous ne pouvons vous le révéler. Non, ce n'est pas un manque d'inspiration.