Anneaux et corps

Exercice 1. *Est-ce que les ensembles munis d'opérations suivants sont des anneaux, des corps ?*

1. $\mathbb{Z}, +, \cdot$
2. $\mathbb{R}[x], +, \cdot$
3. $\mathbb{Z}/n\mathbb{Z}, +, \cdot$

Exercice 2.

1. *Soient X un ensemble et G un groupe. Montrer que l'on peut munir l'ensemble $\mathcal{F}(X, G)$ des applications de X dans G d'une structure de groupe.*
2. *Soient X un ensemble et A un anneau. Montrer que l'on peut munir l'ensemble $\mathcal{F}(X, A)$ des applications de X dans A d'une structure d'anneau.*
3. *Soient X un ensemble et K un anneau. L'anneau $\mathcal{F}(X, K)$ est-il un corps ?*

Exercice 3. *Montrer que l'ensemble des éléments inversibles d'un anneau peut être muni d'une structure de groupe.*

Exercice 4. *Avec quel groupe d'ordre 4 les groupes suivants sont-ils isomorphes ?*

1. $(\mathbb{Z}/5\mathbb{Z})^*, \cdot$
2. $(\mathbb{Z}/8\mathbb{Z})^*, \cdot$
3. $(\mathbb{Z}/12\mathbb{Z})^*, \cdot$

Exercice 5. *Soit $\mathbb{Z}[i] = \{a + bi \mid a \in \mathbb{Z}, b \in \mathbb{Z}\}$. Cet ensemble est appelé l'anneau des entiers de Gauss. Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$.*

Exercice 6.

1. *Soit F_n le n-ième nombre de Fermat, $F_n = 2^{2^n} + 1, n \in \mathbb{N}$. Soit p un diviseur premier de F_n. Déterminer l'ordre de 2 dans F_p^*.*
2. *Montrer que p est de la forme $1 + k2^{n+1}$ avec $k \in \mathbb{N}^*$.*
3. *Montrer que F_5 n'est pas premier.*

Exercice 7. *Déterminer l'inverse de $\overline{526}$ dans $\mathbb{Z}/561\mathbb{Z}$.*

Exercice 8. *Montrer qu'il y a un isomorphisme d'anneaux*

$$\mathbb{Z}/72\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z} \cong \mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/168\mathbb{Z}.$$

Exercice 9.

1. *Soient G et H des anneaux. Montrer que $(G \times H)^* = G^* \times H^*$.*
2. *Soient $x \in G$ et $y \in H$ d'ordre fini. Montrer que l'ordre de $(x, y) \in G \times H$ est égal au $ppcm(o(x), o(y))$.*
3. *Calculer l'ordre de $\overline{526}$ dans $(\mathbb{Z}/561\mathbb{Z})^*$.*

Exercice 10.

1. *Montrer qu'un corps (commutatif) est un anneau intègre (si $ab = 0$ alors $a = 0$ ou $b = 0$).*
2. *Est-ce que la réciproque est vraie ?*

Exercice 11. (Théorème de Wilson)

1. *Supposons que n est premier. Résoudre l'équation $x^2 = 1$ dans $\mathbb{Z}/n\mathbb{Z}$.*
2. *Si n est premier, montrer que $(n-1)! \equiv -1$ mod n.*
3. *Montrer que réciproquement si $(n-1)! \equiv -1$ mod n, alors n est premier.*

Exercice 12. *(Division Euclidienne)*

1. *Soit A un anneau intègre et $P_1 \in A[x]$ un polynôme dont le coefficient dominant est inversible dans A. Montrer que pour tout polynôme $P_2 \in A[x]$, il existe un unique couple $(Q, R) \in A[x] \times A[x]$ tel que*

$$P_2 = P_1 Q + R, \qquad \text{avec } R = 0 \text{ ou } deg(R) < deg(P_1).$$

2. *Montrer que la condition sur le polynôme P_1 est nécessaire.*

Exercice 13. *Soient m et n deux entiers positifs tels que m divise n. Montrer que $x^m - 1$ divise $x^n - 1$.*

Exercice 14. *Soient A un anneau commutatif et a, b deux éléments de A. Montrer que l'idéal (a, b) est l'ensemble des éléments*

$$\{ax + by \mid x, y \in A\}.$$

Exercice 15.

1. *Montrer que tout idéal de $\mathbb{Z}$ est de la forme $a\mathbb{Z}$, où $a \in \mathbb{Z}$.*
2. *Trouver tous les idéaux d'un corps $\mathbb{K}$.*
3. *$\mathcal{J} = \{(\alpha, \alpha) : \alpha \in \mathbb{Z}\}$ est-il un idéal de l'anneau $\mathbb{Z}^2$?*

Exercice 16. *Soit I un idéal d'un anneau A. Montrer que :*

1. *$I = A$ si et seulement si I contient une unité (i.e. un élément inversible) ;*
2. *$(a) = A$ ssi a est inversible ;*

Exercice 17. *Soit A un anneau commutatif unitaire, soit I un idéal dans A. Montrer que le quotient A/I est un anneau commutatif.*

Exercice 18. *Soit A un anneau. Trouver les anneaux quotients*

1. $A[x]/(x)$,
2. $A[x,y]/(x)$,
3. $A[x,y]/(x,y)$,
   où $(x),(x,y)$ sont les idéaux engendrés réspectivement par x, x et y.

Exercice 19. *Soit $n \in \mathbb{Z}$. Trouver l'anneau quotient $\mathbb{Z}/(n)$.*

Exercice 20. *Vrai ou faux ? Clarifier votre réponse.*

1. *Soit $f : R \longrightarrow S$ un morphisme d'anneaux. Si T est un sous-anneau de R, alors $f(T)$ est un sous-anneau de S.*
2. *Soit $f : R \longrightarrow S$ un morphisme d'anneaux. Si T est un sous-anneau de S, alors $f^{-1}(T)$ est un sous-anneau de R.*
3. *Soit $f : R \longrightarrow S$ un morphisme d'anneaux. Si I est un idéal de R, alors $f(I)$ est un idéal de S.*
4. *Soit $f : R \longrightarrow S$ un morphisme d'anneaux. Si I est un idéal de S, alors $f^{-1}(I)$ est un idéal de R.*

Exercice 21. *Soit $f : A \longrightarrow B$ un morphisme d'anneaux.*

1. *Montrer que $Ker(f)$ est un idéal de A.*
2. *Montrer que $Im(f)$ est un sous-anneau de B.*
3. *Est-ce que $Im(f)$ est un idéal de B ?*

Exercice 22. *Déterminer les morphismes d'anneaux de $\mathbb{Q}$ vers soi-même.*

Exercice 23. *(Cryptographie à clef secret : exemple)*
On code un message en identifiant la lettre A au chiffre 1, la lettre B au 2 etc. On travaille dans $\mathbb{Z}/26\mathbb{Z}$ et on choisit une clef secrète $s \in \mathbb{Z}/26\mathbb{Z}$. Dans cet exemple de chiffrement, on effectue un décalage constant des lettres du message. Coder consiste à ajouter s à chacune des lettres du message alors que soustraire s à chaque lettre du message codé est l'opération de décodage. Quels inconvénients de ce cryptosystème est-ce que vous voyez ?

Exercice 24. *(Cryptographie : le système RSA, Rivest-Shamir-Adelman 1978). [Gourdon p.34]*
Soient p et q deux nombres premiers distincts ; on pose $n = pq$. Soient c et d deux entiers tels que $cd \equiv 1 \ mod \ \varphi(n)$.

1. *Soit $t \in \mathbb{Z}$. Montrer que $t^{cd} \equiv t \ mod \ n$.*

2. *Supposons que n et c soient connus (clef publique). Tout le monde peut coder un message $t \in \mathbb{Z}$ via l'application $g : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : \overline{t} \mapsto \overline{t}^c$. La fonction g s'appelle une fonction de chiffrement. Quelle est la fonction de déchiffrement ?*
3. *Expliquer en quoi ce système de cryptage est particulièrement difficile à attaquer.*