Feuille d'exercices 11: Anneaux, $\mathbb{Z}/n\mathbb{Z}$.

Exercice 11.1 : (niveau 1)
Résoudre dans $\mathbb{Z}/13\mathbb{Z}$ l'équation en l'inconnue x suivante : $x^2 + 2x + \overline{10} = 0$.

Exercice 11.2 : (niveau 1)

1°) Soient $(G, .)$ et $(G', .)$ deux groupes et $f : G \longrightarrow G'$ un morphisme de groupes. Soit $x \in G$. On suppose que x est d'ordre fini n. Montrer que $f(x)$ est aussi d'ordre fini et que cet ordre divise n.

2°) Déterminer tous les morphismes de groupes de $\mathbb{Z}/7\mathbb{Z}$ dans $\mathbb{Z}/13\mathbb{Z}$, et de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$.

Exercice 11.3 : (niveau 1)
Soit K un corps.

1°) Quels sont les idéaux de K ?

2°) Peut-on énoncer une propriété réciproque ?

3°) Soient A un anneau différent de $\{0\}$ et $f : K \longrightarrow A$ un morphisme d'anneaux. Montrer que f est injectif.

Exercice 11.4 : (niveau 1)
Soit f un endomorphisme de corps sur $\mathbb{R}$.
1°) Montrer que, pour tout $x \in \mathbb{R}_+$, $f(x) = f(\sqrt{x})^2$.
En déduire que f est croissante.
2°) a) Montrer que, pour tout $(n, x) \in \mathbb{N} \times \mathbb{R}$, $f(nx) = nf(x)$.
b) Montrer que pour tout rationnel x, $f(x) = x$.
3°) Montrer que f est l'application identité de $\mathbb{R}$ dans $\mathbb{R}$.

Exercice 11.5 : (niveau 2)
Montrer que $(p-1)! \equiv -1\ [p]$ si et seulement si p est premier (c'est le théorème de Wilson).
*I*ndication : Lorsque p est premier, on pourra commencer par calculer dans $\mathbb{Z}/p\mathbb{Z}$ la quantité $\prod_{k=2}^{p-2} \overline{k}$ en regroupant $\overline{k}$ et $\overline{k}^{-1}$.

Exercice 11.6 : (niveau 2)
L'ensemble des entiers de Gauss est $\mathbb{Z}[i] = \{a + ib \ / \ a, b \in \mathbb{Z}\}$.

1°) Montrer que $\mathbb{Z}[i]$ est un anneau.

2°) Déterminer les éléments inversibles de $\mathbb{Z}[i]$.

3°) Démontrer que, pour tout $u, v \in \mathbb{Z}[i]$ avec $v \neq 0$, il existe $q, r \in \mathbb{Z}[i]$ tels que $u = vq + r$ avec $|r| < |v|$.

4°) Montrer que $\mathbb{Z}[i]$ est un anneau principal.

Exercice 11.7 : (niveau 2)
Déterminer les morphismes d'anneaux de $\mathbb{Z}^n$ dans $\mathbb{Z}$ (où $n \in \mathbb{N}^*$).

Exercice 11.8 : (niveau 2)
Soit $\mathbb{K}$ un corps. Montrer que $(\mathbb{K}, +)$ et $(\mathbb{K}^*, \times)$ ne sont pas des groupes isomorphes.

Exercice 11.9 : (niveau 2)
Soit p un nombre premier et $k \in \mathbb{N}^*$ tel que $k \wedge (p-1) = 1$. Montrer que l'application $\begin{array}{ccc} \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ x & \longmapsto & x^k \end{array}$ est une bijection.

Exercice 11.10 : (niveau 2)
Soit p un nombre premier. Montrer que pour tout $k \in \mathbb{N}$, $\displaystyle\sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^k \in \{0, -1\}$.

Exercice 11.11 : (niveau 2)
p et q sont deux entiers premiers et impairs. On suppose que q divise $2^p - 1$.
Montrer que $q \equiv 1 \ [2p]$.

Exercice 11.12 : (niveau 2)

1°) Soit A un anneau. On dira qu'un élément de A est nilpotent si et seulement s'il existe $k \in \mathbb{N}^*$ tel que $a^k = 0_A$.
Soient x et y deux éléments nilpotents de A tels que $xy = yx$.
Montrer que xy et $x + y$ sont nilpotents.

2°) Soit n un entier naturel supérieur ou égal à 2 que l'on décompose en produit de facteurs premiers : $n = \displaystyle\prod_{i=1}^{k} p_i^{\alpha_i}$, où, pour tout $i \in \{1, \ldots, k\}$, $p_i \in \mathbb{P}$ et $\alpha_i \in \mathbb{N}^*$.
a) Quels sont les éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$?
b) Donner une condition nécessaire et suffisante pour que tout diviseur de 0 de $\mathbb{Z}/n\mathbb{Z}$ soit nilpotent.

Exercice 11.13 : (niveau 2)
Lorsque $n \in \mathbb{N}^*$, on note $\varphi(n)$ l'indicatrice d'Euler.
Déterminer les entiers $n \in \mathbb{N}^*$ tels que $\varphi(n)$ divise n.

Exercice 11.14 : (niveau 3)
Soient $r, s \in \mathbb{N}^*$, $A_1, \ldots, A_r$, $B_1, \ldots, B_s$ des anneaux intègres tels que $A = A_1 \times \cdots \times A_r$ et $B = B_1 \times \cdots \times B_s$ sont isomorphes. Montrer que $r = s$.

Exercice 11.15 : (niveau 3)
Soit E un ensemble fini. On admet que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau (où $A\Delta B = (A \setminus B) \cup (B \setminus A)$). Montrer que tous ses idéaux sont principaux.
Est-ce encore vrai lorsque E est infini ?

Exercice 11.16 : (niveau 3)
On s'intéresse à l'équation $5x^3 + 11y^3 + 13z^3 = 0$ où les inconnues sont dans $\mathbb{Z}$.

1°) Si $(x, y, z) \in \mathbb{Z}^3$ est solution, montrer que 13 divise x, y, z.

2°) Quelles sont les solutions de l'équation ?

Exercice 11.17 : (niveau 3)
Soit f une bijection d'un ensemble E dans lui-même.
Montrer qu'il existe deux involutions g et h sur E telles que $f = g \circ h$.

Exercices supplémentaires

Exercice 11.18 : (niveau 1)
Si B est un anneau, on note $Inv(B)$ l'ensemble des éléments inversibles de B.
Soient E un ensemble et A un anneau. Montrer que $Inv(\mathcal{F}(E,A)) = \mathcal{F}(E, Inv(A))$

Exercice 11.19 : (niveau 1)
Dans un anneau commutatif $(A, +, .)$, montrer que pour tout $n \in \mathbb{N}$ et $a_1, \ldots, a_n \in A$,
$2\sum_{k=1}^{n} a_k(a_1 + \cdots + a_k) = \Big(\sum_{k=1}^{n} a_k\Big)^2 + \sum_{k=1}^{n} a_k^2$.

Exercice 11.20 : (niveau 1)
Soient A et B deux anneaux commutatifs, $f : A \longrightarrow B$ un morphisme d'anneaux, et I un idéal de A. Montrer que $f(I)$ est un idéal de $Im(f)$.

Exercice 11.21 : (niveau 1)

1°) Soit p un nombre premier. Résoudre l'équation $x^2 = x$ dans $\mathbb{Z}/p\mathbb{Z}$.

2°) Résoudre l'équation $x^2 = x$ dans $\mathbb{Z}/34\mathbb{Z}$.

3°) Résoudre l'équation $x^2 = x$ dans $\mathbb{Z}/30\mathbb{Z}$.

Exercice 11.22 : (niveau 1)
Soit $n \in \mathbb{N}^*$ et $x_1, \ldots, x_n \in \mathbb{Z}$.
Montrer qu'il existe $J \subset \{1, \ldots, n\}$ tel que $J \neq \emptyset$ et n divise $\sum_{j \in J} x_j$.

Exercice 11.23 : (niveau 2)
Soit $n, m \in \mathbb{N}^*$ deux entiers premiers entre eux. Montrer que $n^{\varphi(m)} + m^{\varphi(n)} \equiv 1[nm]$.

Exercice 11.24 : (niveau 2)

1°) Résoudre l'équation $10x \equiv 14\ [15]$ en l'inconnue $x \in \mathbb{Z}$.

2°) Résoudre l'équation $10x \equiv 14\ [18]$ en l'inconnue $x \in \mathbb{Z}$.

3°) Plus généralement, si $(a, b) \in \mathbb{Z}^2$ et $m \in \mathbb{N}^*$, comment résoudre l'équation $ax \equiv b\ [m]$?

Exercice 11.25 : (niveau 2)
Soient A un anneau commutatif et I un idéal de A. On appelle radical de I et on note $R(I)$ l'ensemble des $x \in A$ pour lesquels il existe $n \in \mathbb{N}^*$ tel que $x^n \in I$.

1°) Montrer que $R(I)$ est un idéal de A contenant I.

2°) Montrer que $R(R(I)) = R(I)$.

3°) Soit J un second idéal de A. Montrer que $R(I \cap J) = R(I) \cap R(J)$.

4°) Soit $k \in \mathbb{Z}$. Avec $A = \mathbb{Z}$, déterminer $R(k\mathbb{Z})$.

Exercice 11.26 : (niveau 2)
Montrer que tout anneau intègre fini est un corps.

Exercice 11.27 : (niveau 2)
Soit A un anneau commutatif non réduit à $\{0\}$.

1°) On suppose que les seuls idéaux de A sont les idéaux triviaux ($\{0\}$ et A). Démontrer que A est un corps.

2°) Un idéal I de A est dit premier lorsque $\forall x, y \in A,\ (xy \in I) \Longrightarrow (x \in I \vee y \in I)$. On suppose que tous les idéaux de A sont premiers. Démontrer que A est intègre, puis que $x \in x^2A$ pour tout $x \in A$ et enfin que A est un corps.

Exercice 11.28 : (niveau 2)
Montrer que l'ensemble des nombres décimaux est un anneau principal.

Exercice 11.29 : (niveau 2)
Soit A un anneau commutatif. On note N l'ensemble des éléments nilpotents de A et $B = \{1 + x \ / \ x \in N\}$. Montrer que $(B, \times)$ est un groupe.

Exercice 11.30 : (niveau 2)
Soit $n, k \in \mathbb{N}^*$. Donner une condition nécessaire et suffisante pour que l'application identiquement nulle soit l'unique morphisme de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/k\mathbb{Z}$.

Exercice 11.31 : (niveau 3)
Soit p un nombre premier.
On note $\mathbb{Z}_{(p)} = \{\frac{\alpha}{\beta}/(\alpha, \beta) \in \mathbb{Z}^2, \alpha \wedge \beta = 1 \text{ et } \beta \notin p\mathbb{Z}\}$.

1°) Montrer que $\mathbb{Z}_{(p)}$ est un anneau commutatif intègre.

2°) Montrer que $I = \{\frac{\alpha}{\beta}/(\alpha, \beta) \in \mathbb{Z}^2, \alpha \wedge \beta = 1, \alpha \in p\mathbb{Z} \text{ et } \beta \notin p\mathbb{Z}\}$ est un idéal de $\mathbb{Z}_{(p)}$, différent de $\mathbb{Z}_{(p)}$.

3°) Montrer que tout idéal de $\mathbb{Z}_{(p)}$ différent de $\mathbb{Z}_{(p)}$ est inclus dans I.

4°) Décrire les idéaux de $\mathbb{Z}_{(p)}$.

Exercice 11.32 : (niveau 3)
On note $\mathbb{Z}[j] = \{x + jy/x \in \mathbb{Z}, y \in \mathbb{Z}\}$ où $j = e^{\frac{2i\pi}{3}}$.

1°) Vérifier que $\mathbb{Z}[j]$ est un sous-anneau de $\mathbb{C}$.

2°) Soit $u \in \mathbb{Z}[j]$. Montrer que u est inversible (dans $\mathbb{Z}[j]$) si et seulement si $\mid u \mid= 1$.

3°) Montrer que l'ensemble U des éléments inversibles de $\mathbb{Z}[j]$ est un groupe multiplicatif, dont on déterminera les éléments.

Exercice 11.33 : (niveau 3)
La suite croissante des nombres premiers satisfait-elle une relation de récurrence linéaire à coefficients rationnels ?

Exercice 11.34 : (niveau 3)
Soit $(p, q) \in \mathbb{N}^{*2}$, avec $p < q$. On suppose que p et q sont premiers entre eux et que q est premier avec 10.
Montrer que le développement décimal de $\frac{p}{q}$ est périodique et qu'une période est $\varphi(q)$, où φ désigne l'indicatrice d'Euler.

Exercice 11.35 : (niveau 3)
Soit x un réel irrationnel. On suppose que x n'est pas transcendant, c'est-à-dire qu'il existe un polynôme non nul P à coefficients rationnels tel que $P(x) = 0$.

1°) Montrer que $I = \{R \in \mathbb{Q}[X] \ / \ R(x)\}$ est un idéal de $\mathbb{Q}[X]$.
En déduire qu'il existe un unique $\pi_x \in \mathbb{Q}[X]$ tel que π_x est unitaire et $I = \pi_x \mathbb{Q}[X]$.

2°) On note $d = \deg(\pi_x)$.
Montrer qu'il existe $M \in \mathbb{R}_+^*$ tel que, pour tout $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ vérifiant $|x - \frac{p}{q}| \leq 1$, $|\pi_x(\frac{p}{q})| \leq M|x - \frac{p}{q}|$.
En déduire qu'il existe $C \in \mathbb{R}_+^*$ tel que, pour tout $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$, $|x - \dfrac{p}{q}| \geq \dfrac{C}{q^d}$.

3°) Soit a un entier supérieur ou égal à 2. Montrer que $\displaystyle\sum_{k=0}^{+\infty} a^{-k!}$ est transcendant.