COMPLÉMENTS SUR LES ANNEAUX

EXERCICE 1 (Sous-anneau de $(\mathbb{Z}^2,+,\times)$).

Pour $d\in\mathbb{N}$, on note $A_d=\left\{(x,y)\in\mathbb{Z}^2 \text{ tel que } d \text{ divise } (y-x)\right\}$

1. Montrer que A_d est un sous anneau $(\mathbb{Z}^2,+,\times)$.
2. Inversement, soit A un sous anneau de $(\mathbb{Z}^2,+,\times)$.
   Montrer que $H=\{x\in\mathbb{Z}/(x,0)\in A\}$ est un sous groupe de $(\mathbb{Z},+)$.
3. En déduire qu'il existe $d\in\mathbb{N}$ tel que $H=d\mathbb{Z}$ et $A=A_d$.

EXERCICE 2 (Sous-corps de $(\mathbb{Q},+,.)$).

Démontrer que $\mathbb{Q}$ n'admet pas d'autre sous-corps que lui-même.

EXERCICE 3 (Les autmorphismes de $(\mathbb{R},+,\times)$).

Soit σ un automorphisme de $(\mathbb{R},+,\times)$

1. Montrer que si $x\geqslant 0$ alors $\sigma(x)\geqslant 0$.
2. Montrer que σ est croissant.
3. Montrer que $\forall r\in\mathbb{Q}$: $\sigma(r)=r$. Puis déterminer σ.

EXERCICE 4 (Mines).

Les groupes multiplicatifs $\mathbb{U}\left(\mathbb{Z}/9\mathbb{Z}\right)$ et $\mathbb{U}\left(\mathbb{Z}/7\mathbb{Z}\right)$ sont-ils isomorphes ?

EXERCICE 5 ($-\overline{1}$ est-il un carré dans le corps $\mathbb{Z}/p\mathbb{Z}$?).

Soit p un nombre premier, $p\geqslant 3$.

1. Combien y a-t-il de carrés de $\overline{1}$ dans le corps $K=\mathbb{Z}/p\mathbb{Z}$?
2. Montrer qu'un élément x de $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ est un carré si et seulement si $x^{\frac{p-1}{2}}=\overline{1}$.
3. Quels sont les nombres premiers p pour lesquels $-\overline{1}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$?
4. En déduire qu'il existe une infinité de nombres premiers de la forme $4k+1$, $k\in\mathbb{N}$.

EXERCICE 6.

Établir $\forall n\geqslant 3, \varphi(n)\geqslant \dfrac{n\ln 2}{\ln n+\ln 2}$

EXERCICE 7 (Indicatrice d'Euler).

On note φ la fonction indicatrice d'Euler. Soit $n\in\mathbb{N}^*$

1. Montrer que si H est un sous-groupe de $\left(\mathbb{Z}/n\mathbb{Z},+\right)$, il existe a divisant n vérifiant $H=\{k.\overline{a}\ ,\ k\in\mathbb{Z}\}$.
2. Observer que si $d\mid n$ il existe un unique sous-groupe de $\left(\mathbb{Z}/n\mathbb{Z},+\right)$ d'ordre d.
3. Justifier que si $d\mid n$ le groupe $\left(\mathbb{Z}/n\mathbb{Z},+\right)$ possède exactement $\varphi(d)$ éléments d'ordre d.
4. Montrer que: $\forall n\in\mathbb{N}^\star, \sum\limits_{d\mid n}\varphi(d)=n$.

EXERCICE 8.

Soient $T=(t_{i,j})_{1\leqslant i,j\leqslant n}\in\mathrm{M}_n(\mathbb{R})$ déterminée par $t_{i,j}=\begin{cases}1 & \text{si } i \text{ divise } j\\ 0 & \text{sinon}\end{cases}$ et $D=\mathrm{diag}(\varphi(1),\ldots,\varphi(n))\in\mathrm{M}_n(\mathbb{R})$. Où φ la fonction indicatrice d'Euler.

1. Calculer le coefficient d'indice (i,j) de la matrice ${}^tTDT$ en fonction de $\mathrm{pgcd}(i,j)$;
2. En déduire la valeur du déterminant de la matrice de Smith $S=(\mathbf{pgcd}(i,j))_{1\leqslant i,j\leqslant n}$

EXERCICE 9 (Centrale MP).

Soit A un anneau commutatif. Si I est un idéal de A, on appelle radical de I l'ensemble $\sqrt{I}$ défini par

$$\sqrt{I} = \{x \in A;\ \exists n \geqslant 1,\ x^n \in I\}$$

1. Montrer que $\sqrt{I}$ est un idéal de A contenant I.
2. Soient I, J deux idéaux de A et $p \geqslant 1$. Montrer que
$$\sqrt{I.J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J},\ \text{et } \sqrt{I^p} = \sqrt{I}.$$
3. Si $A = \mathbb{Z}$ et $I = k\mathbb{Z}$, $k \geqslant 1$, déterminer le radical de I.

EXERCICE 10.

Soit $(A, +, \times)$ un anneau commutatif et I un idéal de A

— On dit que I est premier si: $\forall x, y \in A, \quad xy \in I \implies x \in I$ ou $y \in I$

— On dit que I est maximal si: $\forall J$ idéal de A tel que $I \subset J$, on a $J = I$ ou $J = A$

1. Déterminer les idéaux premiers de $\mathbb{Z}$.
2. Soit I un idéal et $x \in A \backslash I$. Soit J l'idéal engendré par I et x. Montrer que
$$J = \{a \in A;\ \exists i \in I,\ \exists k \in A,\ a = i + kx\}.$$
3. En déduire que tout idéal maximal est premier.
4. Montrer que si tous les idéaux de A sont premiers, alors A est un corps.

EXERCICE 11 (Centrale MP).

Soient $\mathbb{K}$ un corps, A un sous-anneau de $\mathbb{K}$ tel que $\forall x \in \mathbb{K},\ x \in A$ ou $x^{-1} \in A$.
Soit M l'ensemble des éléments non inversibles de A, c'est-à-dire

$$M = \left\{x \in A \text{ non nul} \mid x^{-1} \notin A\right\} \cup \{0\}.$$

1. Montrer que M est un idéal de A.
2. Montrer que tout idéal de A distinct de A est contenu dans M.

EXERCICE 12 (Centrale MP).

Soit p un nombre premier. On pose $Z_p = \left\{\frac{a}{b} \mid a \in \mathbb{Z},\ b \in \mathbb{N}^*,\ p \text{ ne divise pas } b\right\}$ et

$$J_p = \left\{\frac{a}{b} \mid a \in \mathbb{Z},\ b \in \mathbb{N}^*,\ p \text{ divise } a \text{ et ne divise pas } b\right\}$$

1. Montrer que Z_p est un sous-anneau de $\mathbb{Q}$. Quels sont ses éléments inversibles?
2. Montrer que J_p est un idéal de Z_p, et que tout idéal de Z_p autre que Z_p est inclus dans J_p.
3. Démontrer que les seuls idéaux autres que $\{0\}$ de Z_p sont de la forme $p^\alpha Z_p$, avec $\alpha \in \mathbb{N}$.

EXERCICE 13 (Suite décroissante d'idéaux).

Soit A un anneau principal et intègre tel que tout suite décroissante d'idéaux est stationnaire. Montrer que A est un corps.

EXERCICE 14 (Principalité de $A[X]$).

Soit A un anneau. Montrer que $A[X]$ est principal si et seulement si A est un corps.

EXERCICE 15.

Soit A un anneau commutatif non nul dont les seuls idéaux sont $\{0\}$ et A. Montrer que A est un corps.

EXERCICE 16.

Les parties $\mathcal{I} = \{P \in \mathbb{R}[X] : P'(0) = 0\}$ et $\mathcal{J} = \{P \in \mathbb{R}[X] : P(0) = P'(0) = 0\}$ sont-elles des idéaux de $\mathbb{R}[X]$? Dans l'affirmative, en donner un générateur

EXERCICE 17 (Caractéristique d'un anneau).

Soit $(A, +, \times)$ un anneau d'unité 1_A et de neutre 0_A. On considère l'application $f : \left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & A \\ n & \longmapsto & n.1_A \end{array} \right.$

1. Montrer que f est l'unique morphisme d'anneaux de $\mathbb{Z}$ dans A et justifier l'existence d'un unique entier $p \in \mathbb{N}$ tel que $\mathrm{Ker} f = p\mathbb{Z}$. Le nombre p est appelé la caractérstique de A et noté $\mathrm{car}\,(A)$
2. Montrer que si A est intègre, alors $\mathrm{car}\,(A)$ est soit nulle, soit un nombre premier
3. Soit $\mathbb{K}$ un corps fini. Montrer qu'il existe p premier et $\alpha \in \mathbb{N}^*$ tel que **Card** $(\mathbb{K}) = p^\alpha$

EXERCICE 18 (Système de congruence).

Soit $n \in \mathbb{N}^*$ et $P_1, P_2, \dots, P_n$ des polynômes à coefficients réels, premiers entre eux deux à deux. Montrer que pour tout choix de $A_1, \dots, A_n$ d'autres polynômes, il existe un polynôme A tel que $\forall i,\ P_i | (A - A_i)$.

EXERCICE 19.

Déterminer les polynômes de $\mathbb{C}[X]$ tels que $P(X^2) = P(X)P(X+1)$.

EXERCICE 20.

Former la décomposition primaire dans $\mathbb{R}[X]$ de $P = X^{2n+1} - 1$ (avec $n \in \mathbb{N}$).

EXERCICE 21.

Pour $n \in \mathbb{N}$, on note $P_n = X^n - 1$. Trouver le PGCD de P_n et P_m.

EXERCICE 22.

Quels sont les polynômes $P \in \mathbb{C}[X]$ tels que P' divise P ?

EXERCICE 23 (Mines. MP 2018).

Soit $P \in \mathbb{R}[X]$, tel que $\forall x \in \mathbb{R},\ P(x) \geqslant 0$. Montrer qu'il existe $B, C \in \mathbb{R}[X]$ de même degré tels que $P = B^2 + C^2$.

EXERCICE 24 (Irréductibilité sur $\mathbb{Z}$).

1. Montrer que les polynômes $X^2 - X - 1$ et $X^3 - X - 1$ sont irréductibles sur $\mathbb{Z}$.
2. Soit $n \in \mathbb{N}^*$ et $a_1, \dots, a_n$ des entiers relatifs deux à deux distincts. Définissons Φ par
$$\Phi = (X - a_1) \dots (X - a_n) - 1$$
On remarque que $\Phi \in \mathbb{Z}[X]$. Le but de la question est de montrer qu'il est irréductible sur $\mathbb{Z}$. Supposons qu'il existe P et Q dans $\mathbb{Z}[X]$ de degré supérieur ou égal à 1 et vérifiant $\Phi = PQ$.
   (a) Montrer que $a_1, \dots, a_n$ sont des racines de $P + Q$.
   (b) En déduire que $\Phi = -P^2$.
   (c) Conclure.
3. Soit n un entier naturel impair et soit $a_1, \dots, a_n$ des entiers relatifs deux à deux distincts. Montrer que $(X - a_1) \dots (X - a_n) + 1$ est irréductible dans $\mathbb{Z}$.

EXERCICE 25 (Critère d'Eisenstein).

1. Soit $\Phi \in \mathbb{Z}[X]$ pour lequel il existe des polynômes P et Q de degré supérieur ou égal à 1 et à coefficients rationnels tels que $\Phi = PQ$. Montrer qu'il existe deux polynômes P_0 et Q_0 de $\mathbb{Z}[X]$ proportionnels respectivement à P et Q et tels que $\Phi = P_0 Q_0$.

2. Soit $\Phi \in \mathbb{Z}[X]$. Montrer que Φ est irréductible sur $\mathbb{Q}$ si, et seulement si, Φ est irréductible sur $\mathbb{Z}$.
3. Soit $\Phi = \sum_{k=0}^{n} a_k X^k$ un polynôme non constant de $\mathbb{Z}[X]$. On suppose qu'il existe un nombre premier p tel que :
   - p ne divise pas a_n
   - p divise a_i pour $i \in \{0, \dots, n-1\}$
   - p^2 ne divise pas a_0

   Montrer que Φ est irréductible sur $\mathbb{Q}$.

EXERCICE 26 (Théorème de Lucas**).**

1. Soit $P \in \mathbb{C}[X]$, de degré $n \geqslant 2$. Montrer que les racines de P' appartiennent à l'enveloppe convexe des racines de P.
2. Que dire sur les racines de P' si $P \in \mathbb{R}[X]$ a toutes ses racines réelles ? Localiser ces racines.

EXERCICE 27.

Soit A un anneau commutatif. A quelle condition est-il vrai que $\forall n \in \mathbb{N}^*$, tout polynôme $P \in A[X]$ de degré n admet au plus n racines ?

EXERCICE 28 (Polynômes de Bezout**).**

Déterminer deux polynômes U et V vérifiant $UX^n + V(1-X)^m = 1$ et $\deg(U) < m$ et $\deg(V) < n$.