À rendre pour le mardi 26 septembre

DM NORMAL

EXERCICE

Soit A un anneau commutatif.
Soit I un idéal de l'anneau A, on appelle radical de A l'ensemble
$\sqrt{I} = \{x \in A : \exists n \in \mathbb{N}^* \ / \ x^n \in I\}$.

1. Montrer que $\sqrt{I}$ est un idéal et qu'il contient I.

2. ***a.*** Soit I et J des idéaux de A. Montrer que : $I \subset J \Rightarrow \sqrt{I} \subset \sqrt{J}$.

b. Soit I et J des idéaux de A. Montrer que : $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

c. Soit I un idéal de A. Montrer que $\sqrt{\sqrt{I}} = \sqrt{I}$.

3. Application dans $\mathbb{Z}$: on donne $m = \prod_{i=1}^{k} p_i$ et $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ où $k \in \mathbb{N}^*$ et, pour tout i de 1 à k, p_i est un nombre premier, $\alpha_i \in \mathbb{N} \setminus \{0\}$ et $p_1 < p_2 < \cdots < p_k$.
Montrer que $m\mathbb{Z} = \sqrt{n\mathbb{Z}}$.

PROBLÈME

- PREMIÈRE PARTIE -

1. Lister les éléments inversibles (en précisant leur inverse) de $\mathbb{Z}/6\mathbb{Z}$ et ceux de $\mathbb{Z}/13\mathbb{Z}$.

2. Soit $p \in \mathbb{N}^* \setminus \{1, 2, 3, 4\}$. Montrer que si p et $p+2$ sont premiers, alors $p \equiv -1[6]$.

3. Montrer que l'équation $x^2 - \overline{5} = 0$ n'a pas de solutions dans $\mathbb{Z}/13\mathbb{Z}[X]$.

4. Écrire un programme PYTHON qui renvoie l'ordre de tout entier k dans $(\mathcal{U}(\mathbb{Z}/97\mathbb{Z}), \times)$ (il s'agit de déterminer le plus petit entier non nul l tel que $k^l \equiv 1[97]$. Attention si k est divisible par 97).

- DEUXIÈME PARTIE -

Si $\mathbb{K}$ est un corps, nous munissons $\mathcal{M}_n(\mathbb{K})$, l'ensemble des matrices à valeurs dans $\mathbb{K}$, des opérations usuelles sur les matrices. Nous admettons que $(\mathcal{M}_n(\mathbb{K}), +, \cdot)$ est anneau.
On note $K_{13} = \left\{ \begin{pmatrix} x & \overline{5}y \\ y & x \end{pmatrix}, \ x, y \in \mathbb{Z}/13\mathbb{Z} \right\}$ que l'on munit donc des lois $+$ et $\cdot$ habituelles sur les matrices.

1. On pose $M = \begin{pmatrix} \overline{0} & \overline{5} \\ \overline{1} & \overline{0} \end{pmatrix}$. Calculer M^2.

2. Montrer que $(K_{13}, +, \cdot)$ est un corps à 169 éléments.

3. Soit $H_{13} = \left\{ \begin{pmatrix} x & \overline{0} \\ \overline{0} & x \end{pmatrix}, \ x \in \mathbb{Z}/13\mathbb{Z} \right\}$ un sous-ensemble de K_{13}. Montrer que $(H_{13}, +, \cdot)$ est un sous-corps de K_{13}.

4. Montrer que $f : x \mapsto \begin{pmatrix} x & \overline{0} \\ \overline{0} & x \end{pmatrix}$ est un isomorphisme d'anneaux entre $\mathbb{Z}/13\mathbb{Z}$ et H_{13}.

5. On pose $a = \begin{pmatrix} \overline{5} & \overline{0} \\ \overline{0} & \overline{5} \end{pmatrix}$ Trouver les éléments α de K_{13} tels que $\alpha^2 = a$.

- TROISIÈME PARTIE

Soit $(G, .)$ un groupe commutatif fini, x un élément de G, on note $o(x)$ l'ordre de l'élément x de G. On notera 1 l'élément neutre de G. Rappelons que l'ordre de x est caractérisé par : $x^n = 1 \Leftrightarrow o(x) \mid n$.

1. Soit $x \in G$, $l \in \mathbb{N}^*$ tels que $o(x) = l$. Vérifier que x^{-1} est aussi d'ordre l.

2. Soit $x \in G$ d'ordre m. Soit d un diviseur de m. Montrer que $o(x^d) = \dfrac{m}{d}$.

3. Soient maintenant a et b deux éléments de G d'ordre m et n respectivement. Montrer que si $m \wedge n = 1$, alors $o(a.b) = mn$.

4. Soient maintenant a et b deux éléments de G d'ordre m et n respectivement, mais m et n ne sont pas premiers entre eux.

- ***a.*** Construire deux nombres m' et n' tels que $m'n' = m \vee n$, $m'|m$, $n'|n$ et m' et n' premiers entre eux (on pourra s'intéresser à la décomposition en facteurs premiers de m et n).
- ***b.*** En déduire qu'il existe c dans G tel que $o(c) = m \vee n$.

5. Considérons le ppcm r des ordres des éléments de G. r est parfois appelé l'exposant de G, c'est le plus petit $n \in \mathbb{N}^*$ tel que : $\forall x \in G,\ x^n = 1$, . Montrer qu'il existe $c \in G$, tel que $o(c) = r$.

6. Soit $(F, +, .)$ est un corps. Soit $P : x \mapsto \sum_{k=0}^{n} a_k x^k$, avec $a_0, ..., a_{n-1} \in F$ et $a_n \in F \setminus \{0\}$, qui est une fonction dite polynomiale.

- ***a.*** Soit $x_0 \in F$ tel que $P(x_0) = 0$. Montrer qu'il existe une fonction polynomiale $Q : x \mapsto b_{n-1}x^{n-1} + ... + b_0$, avec $b_0, ..., b_{n-2} \in F$ et $b_{n-1} \in F \setminus \{0\}$ tel que :

$$\forall x \in F,\ P(x) = (x - x_0)Q(x).$$

- ***b.*** Montrer par récurrence sur n que P s'annule au plus n fois sur F.

7. Soit $(F, +, .)$ un corps et $(G, .)$ un sous-groupe fini de $(F^*, .)$, montrer que G est cyclique, avec $F^* = F \setminus \{0\}$.

8.

- ***a.*** Montrer que $(K_{13}^*, \cdot)$ est un groupe cyclique isomorphe à $(\mathbb{Z}/168\mathbb{Z}, +)$. En déduire le nombre de générateurs de K_{13}^*.
- ***b.*** Montrer que l'ordre de α (vu dans la partie précédente) dans $(K_{13}^*, \cdot)$ vaut 8.
- ***c.*** Montrer que $\overline{3}$ est un élément d'ordre 3 dans $((\mathbb{Z}/13\mathbb{Z})^*, \times)$. En déduire un élément d'ordre 3 dans K_{13}.
- ***d.*** Montrer que $\begin{pmatrix} \overline{4} & \overline{20} \\ \overline{4} & \overline{4} \end{pmatrix}$ est un élément d'ordre 7 dans $(K_{13}^*, \cdot)$
- ***e.*** En déduire un générateur du groupe $(K_{13}^*, \cdot)$.

DM DIFFICILE

EXERCICE

On note $\pi_n : \left\{ \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ k & \mapsto & \overline{k} \end{array} \right.$.

On admettra le résultat suivant : soit G un groupe fini et H un sous-groupe de G. Alors $|H|$ divise $|G|$. Il résulte du théorème chinois que si $n \in \mathbb{N}^*, n \geqslant 2$ s'écrit $n = m_1 \dots m_r$ où $m_i = p_i^{\alpha_i}$ avec les p_i premiers distincts et les α_i dans $\mathbb{N}^*$, les anneaux $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_r\mathbb{Z}$ sont isomorphes. Il s'ensuit l'isomorphisme entre les groupes multiplicatifs E_n et $E_{m_1} \times \dots \times E_{m_r}$ où $E_k = \mathcal{U}(\mathbb{Z}/k\mathbb{Z})$ (les inversibles de $\mathbb{Z}/k\mathbb{Z}$) . Nous allons étudier la structure de E_{p^α} pour p entier naturel premier et $\alpha \in \mathbb{N}^*$.

1. Cas où $\alpha = 1$.

- ***a.*** Montrer que si $n \in \mathbb{N}^*$, tout sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ est cylique.
- ***b.*** Soit $n \in \mathbb{N}^*$. Montrer que pour tout diviseur d de n, il existe un unique sous-groupe C_d de $(\mathbb{Z}/n\mathbb{Z}, +)$ de cardinal d; C_d est le groupe cyclique engendré par $\pi_n\left(\frac{n}{d}\right)$.
- ***c.*** En déduire que pour $n \in \mathbb{N}^*$, on a : $n = \sum_{d|n} \varphi(d)$, avec φ l'indicatrice d'Euler (on constatera que tout élément d'ordre d dans $(\mathbb{Z}/n\mathbb{Z}, +)$ est inclus dans C_d).
- ***d.*** Soit $(G,.)$ un groupe de cardinal n vérifiant : si $d \mid n$ alors le cardinal de $\left\{x \in G \mid x^d = 1_G\right\}$ est inférieur ou égal à d. Montrer que G est cyclique. On pourra considérer l'ensemble H_d des x de G d'ordre égal à d.
- ***e.*** Soit $\mathbb{K}$ un corps. Soit $P : x \mapsto \sum_{k=0}^{n} a_k x^k$, avec $a_0, ..., a_{n-1} \in \mathbb{K}$ et $a_n \in \mathbb{K}^*$. Montrer que P s'annule au plus n fois sur $\mathbb{K}$ (on pourra raisonner par récurrence sur n).
- ***f.*** En déduire des deux questions précédentes que si $(\mathbb{K}, +,.)$ est un corps fini de cardinal n, alors $(\mathbb{K}^*, .)$ est un groupe cyclique isomorphe à $(\mathbb{Z}/(n-1)\mathbb{Z}, +)$.
- ***g.*** Que dire de E_p si p est un nombre premier ?

2. Cas où p est premier et impair.

- ***a.*** Montrer que : $\forall k \in \mathbb{N}, (1+p)^{p^k} \equiv 1 + p^{k+1} \left[\mathrm{mod} p^{k+2}\right]$.
- ***b.*** Déterminer l'ordre de $(1+p)$ dans E_{p^α} où $\alpha \in \mathbb{N}^*$.
- ***c.*** Soient a et b deux éléments d'ordre p et q d'un groupe $(G,.)$. Si $a.b = b.a$ et si $p \wedge q = 1$, montrer que $a.b$ est d'ordre pq.
- ***d.*** Montrer que $(E_{p^\alpha}, .)$ est un groupe cyclique.

3. Cas où $p = 2$.

- ***a.*** Montrer que : $\forall k \in \mathbb{N}, 5^{2^k} \equiv 1 + 2^{k+2} \left[\mathrm{mod} 2^{k+3}\right]$.
- ***b.*** Quel est l'ordre de 5 dans E_{2^α} où α est entier et $\alpha \geqslant 3$?
- ***c.*** Montrer que $(E_{2^\alpha}, .)$ n'est pas cyclique pour $\alpha \geqslant 3$.

4.

- ***a.*** Soient $(H,.)$ et $(K,.)$ deux groupes finis $h \in H, k \in K$. Montrer que l'ordre de (h,k) dans le groupe $(H \times K,.)$ est le ppcm des ordres de h et k.
- ***b.*** Montrer que le groupe produit de deux groupes cycliques H et K est cyclique si, et seulement si, leurs cardinaux sont premiers entre eux.
- ***c.*** Déterminer $n \in \mathbb{N}, n \geqslant 2$ tel que $(E_n, .)$ soit cyclique.

PROBLÈME

Soient K un sous-corps de $\mathbb{R}$ et α un réel algébrique sur le corps K(ce qui signifie qu'il existe $Q \in K[X]$ non nul tel que $Q(\alpha) = 0$) ; désignons par $\mathcal{I}(\alpha)$ l'ensemble des polynômes P appartenant à $K[X]$ qui admettent α comme racine :

$$\mathcal{I}(\alpha) = \{P | P \in K[X], P(\alpha) = 0\} .$$

1. *$\mathcal{I}(\alpha)$ est un idéal de $K[X]$*

a. Démontrer que $\mathcal{I}(\alpha)$ est un idéal de $K[X]$. En déduire l'existence d'un polynôme M_α unitaire (le coefficient du terme de M_α de plus haut degré est égal à 1) unique tel que $\mathcal{I}(\alpha)$ soit l'ensemble des polynômes de $K[X]$ proportionnels à M_α dans $K[X]$, soit :
$\mathcal{I}(\alpha) = \{P \ / \ \exists Q \in K[X],\ P = M_\alpha.Q\}$.

b. Démontrer que, pour qu'un polynôme P, appartenant à $K[X]$, unitaire et irréductible dans $K[X]$, soit le polynôme M_α il faut et il suffit que le réel α soit racine du polynôme P.

Par définition le polynôme M_α est le *polynôme minimal* de α sur K, le degré du polynôme M_α, noté $d(\alpha, K)$, est le *degré* de α sur K. Soit $K[\alpha]$ le K-espace vectoriel engendré par la famille des réels $1, \alpha, \ldots, \alpha^q, \ldots$: $K[\alpha] = \{x \ / \ x = \sum_{p=0}^{q} x_p \alpha^p,\ q \in \mathbb{N},\ x_p \in K\}$. Il est admis que l'ensemble $K[\alpha]$ est, pour les lois de composition somme et produit, un anneau.

2. *Le degré de α sur K est égal à 1*

Le réel α et le corps K étant donnés, démontrer l'équivalence entre les affirmations suivantes :
i. le réel α appartient à K,
ii. le degré de α sur K est égal à 1 ;
iii. $K[\alpha]$ est égal à K.

3. *Dans cette question le degré de α sur K est égal à 2*

a. Préciser $\dim_K K[\alpha]$; démontrer que $K[\alpha]$ est un corps.

b. Démontrer qu'il existe un réel k ($k > 0$) appartenant au corps K tel que les deux corps $K[\alpha]$ et $K[\sqrt{k}]$ soient égaux.

Par définition, dans ce cas ($d(\alpha, K) = 2$), $K[\alpha]$ est *une extension quadratique* de K.

4. *Dans cette question le degré de α sur K est égal à un entier $n \geq 2$*

a. Démontrer qu'à tout réel x appartenant à l'espace vectoriel $K[\alpha]$ est associé de manière unique un polynôme R de degré inférieur ou égal à $n-1$ appartenant à $K[X]$ tel que : $x = R(\alpha)$. En déduire une base du K-espace vectoriel $K[\alpha]$ et sa dimension.

b. Démontrer que, pour tout réel x (différent de 0) de $K[\alpha]$, le polynôme R ainsi associé est premier avec le polynôme minimal M_α. En déduire l'existence d'un polynôme U de $K[X]$ tel que la relation $U(\alpha).R(\alpha) = 1$ ait lieu.

c. Démontrer que l'anneau $K[\alpha]$ est un corps.

d. Démontrer que l'ensemble $K[\alpha]$ est le plus petit corps admettant α comme élément, contenant K et contenu dans $\mathbb{R}$ ($\alpha \in K[\alpha], K \subset K[\alpha] \subset \mathbb{R}$).

Le corps K est maintenant le corps des rationnels $\mathbb{Q}$. Considérons la suite des polynômes définis, pour tout réel x et pour tout entier naturel n, par les relations :

$$P_0(x) = 1,\ P_1(x) = 2x + 1,\ P_{n+2}(x) = 2xP_{n+1}(x) - P_n(x)\ .$$

Soit Q_n le polynôme défini par la relation $Q_n(x) = P_n(\frac{x}{2})$.

5. *Propriétés générales des polynômes P_n*

a. Déterminer le degré du polynôme P_n, $n \geq 0$; préciser le coefficient du terme de plus haut degré et le terme constant. Déterminer les polynômes : P_2, P_3, P_4. Démontrer que les coefficients des polynômes Q_n (pour $n \geq 0$) sont des entiers relatifs.

b. Démontrer que les seules racines rationnelles possibles du polynôme Q_n sont les entiers 1 et -1. Exprimer l'expression $Q_{n+3}(x) + xQ_n(x)$ en fonction du polynôme $Q_{n+1}(x)$. En déduire que les racines rationnelles éventuelles des polynômes Q_{n+3} et Q_n sont les mêmes. Préciser les polynômes P_n qui ont une racine rationnelle.

6. *Racines du polynôme P_n*

Soit θ un réel donné compris strictement entre 0 et π ($0 < \theta < \pi$). Considérons la suite $(u_n)_{n\geq 0}$ définie par la donnée de u_0 et de u_1 et la relation de récurrence :

$$\text{pour tout entier naturel } n, \quad u_{n+2} = 2u_{n+1}\cos\theta - u_n\,.$$

a. Déterminer l'expression du terme général u_n de la suite ci-dessus en fonction des réels n, θ et de deux scalaires λ et μ déterminés par θ, u_0 et u_1.

b. Utiliser les résultats précédents pour exprimer le réel $v_n = P_n(\cos\theta)$ en fonction des réels n et θ. En déduire toutes les racines du polynôme P_n notées $x_{k,n}$, $1 \leq k \leq n$.

c. Démontrer que les trois nombres réels $\cos(\frac{2\pi}{5}), \cos(\frac{2\pi}{7})$ et $\cos(\frac{2\pi}{9})$ sont algébriques sur $\mathbb{Q}$. Déterminer leur polynôme minimal.

7. *Dans cette question le réel α est le nombre algébrique sur $\mathbb{Q}$,* $\cos(\frac{2\pi}{9})$

a. Démontrer que la dimension de l'espace vectoriel $\mathbb{Q}[\alpha]$ est 3 et qu'une de ses bases est $B = (1, \alpha, \alpha^2)$. Donner l'expression dans cette base des réels $\cos(\frac{4\pi}{9}), \cos(\frac{8\pi}{9})$.

b. Soit f un endomorphisme non nul de l'espace vectoriel $\mathbb{Q}[\alpha]$; supposons que, pour tout couple de réels x et y appartenant à $\mathbb{Q}[\alpha]$, la relation $f(x.y) = f(x).f(y)$ ait lieu.

Déterminer les différentes images possibles des réels 1 et α dans la base B. En déduire que l'ensemble de ces endomorphismes est, pour la loi de composition des endomorphismes, un groupe à trois éléments f_1, f_2, f_3. Déterminer les matrices associées à ces endomorphismes f_1, f_2, f_3 dans la base B.

8. *Exemple de nombres transcendants sur* $\mathbb{Q}$ Soit S un polynôme, appartenant à $\mathbb{Q}[X]$, de degré $n \geq 2$, irréductible sur $\mathbb{Q}$.

a. Démontrer qu'il existe un entier naturel C_S (différent de 0) tel que pour tout rationnel $r = \dfrac{p}{q}$ (le couple (p, q) appartenant à $\mathbb{Z} \in \mathbb{N}^*$) il vienne : $|S(r)| \geq \dfrac{1}{C_S q^n}$.

b. Supposons que le réel α soit une racine de S. Déduire du résultat précédent l'existence d'une constante K, strictement positive, telle que pour tout rationnel $r = \dfrac{p}{q}$ appartenant à l'intervalle $[\alpha - 1, \alpha + 1]$, l'inégalité $|\alpha - r| \geq \dfrac{K}{q^n}$ ait lieu.

c. Soit $(t_n)_{n\in\mathbb{N}}$ la suite des réels définis par la relation : $t_n = \displaystyle\sum_{k=0}^{n} 10^{-k!}$, $n \geq 0$.

Démontrer que la suite $(t_n)_{n\in\mathbb{N}}$ est convergente ; soit t sa limite. Établir l'inégalité : $|t - t_n| \leq 2.10^{-(n+1)!}$. En déduire que le réel t est transcendant sur $\mathbb{Q}$.