CPGE My Youssef, Rabat

بِسمِ اللَّهِ الرَّحمَنِ الرَّحِيمِ
وَ قُلِ إِعمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُم وَ رَسُولُهُ وَ المُؤ مِنُون

صَدَقَ اللَّهُ العَظِيم

Feuille d'exercices: *Arithmétique dans* $\mathbb{Z}$ *et* $\mathbb{K}[X]$

19 septembre 2009

Blague et mathématicien du jour
• **La blague. Un homme se jette du 8 ème etage d'un imeuble. Ses cheveux arrivent en bas 2 minutes plus tard. Pourquoi ?**
Réponse : Il utilise un shampoing anti-chute des cheveux.
• **Le mathématicien. *Julius Wilhelm Richard Dedekind* (1831-1916) est un mathématicien allemand. Il vécut célibataire avec sa soeur jusqu'à sa mort. Il fut élève de *Gauss*, mais aussi trés proche de *Dirichlet* et l'un des premiers mathématiciens à accepter les travaux de *Cantor*.**

1 Notion d'idéal.

Exercice 1 . Quelques ideaux particuliers.
Soit A un anneau commutatif et $\mathcal{I}$ un idéal de A.

1) ***Idéal premier.* On dit que $\mathcal{I}$ est un idéal premier si et seulement si $\mathcal{I}$ est différent de A, et pour tous a et b de A, on a**

$$ab \in \mathcal{I} \text{ et } a \notin \mathcal{I} \Longrightarrow b \in \mathcal{I}.$$

Montrer que $\mathcal{I}$ est un idéal premier de A si et seulement si $A/\mathcal{I}$ est intègre.

2) ***Idéal maximal.* $\mathcal{I}$ est dit maximal quand il n'existe que deux idéaux contenant $\mathcal{I}$ à savoir A et $\mathcal{I}$ lui même.**
Montrer que :

a) Tout idéal maximal est nécessairement premier.

b) $\mathcal{I}$ est un idéal maximal de A si et seulement si $A/\mathcal{I}$ est un corps.

Exercice 2 . Idéaux et morphismes d'anneaux.
Soit A, B deux anneaux commutatifs, $\varphi : A \longrightarrow A$ un morphisme d'anneaux et $\mathcal{I}, \mathcal{J}$ deux idéaux de A et B respectivement.

1) a) Montrer que $\varphi^{-1}(\mathcal{J})$ est un idéal de A.

b) Montrer que si $\mathcal{J}$ est premier, alors $\varphi^{-1}(\mathcal{J})$ est aussi premier.

c) Montrer à l'aide d'un contre-exemple, que ce résultat n'est pas vrai dans le cas des idéaux maximaux.

2) a) On suppose que φ est surjectif, montrer alors que $\varphi(\mathcal{I})$ est un idéal de B.

b) Montrer à l'aide d'un contre-exemple, que ce résultat n'est pas toujours vrai quand φ n'est pas surjective.

*Exercice 3 . **Radical d'un idéal.***
Soit A un anneau commutatif et $\mathcal{I}$ un idéal de A, on appelle *radical* de $\mathcal{I}$, noté

$$\sqrt{\mathcal{I}} = \{x \in A / \ \exists n \in \mathbb{N} \text{ tel que } x^n \in \mathcal{I}\}$$

1) Déterminer $\sqrt{30\mathbb{Z}}$.

2) Soient $\mathcal{I}$ et $\mathcal{J}$ deux idéaux de A. Montrer les propriétés suivantes :

a) $\mathcal{I} \subset \sqrt{\mathcal{I}}$.
b) $\sqrt{\sqrt{\mathcal{I}}} = \sqrt{\mathcal{I}}$.
c) $\sqrt{\mathcal{I}\mathcal{J}} = \sqrt{\mathcal{I} \cap \mathcal{J}} = \sqrt{\mathcal{I}} \cap \sqrt{\mathcal{J}}$.
d) $\sqrt{\mathcal{I} + \mathcal{J}} = \sqrt{\sqrt{\mathcal{I}} + \sqrt{\mathcal{J}}}$.
e) $\sqrt{\mathcal{I}} = A \Longleftrightarrow \mathcal{I} = A$.

*Exercice 4 . **Théorème de factorisation.***

1) ***Idéaux à droite de*** $\mathcal{L}(E)$

a) Soient E, F, G trois espaces vectoriels, soient $w \in \mathcal{L}(E,G)$ et $v \in \mathcal{L}(F,G)$. Montrer l'équivalence :

$$\text{Im } w \subset \text{Im } v \Longleftrightarrow \exists u \in \mathcal{L}(E,F) \quad w = v \circ u \ .$$

b) Soient $u_1, \cdots, u_k$ et v des endomorphismes d'un espace vectoriel E tels que $\text{Im } v \subset \sum_{i=1}^{k} \text{Im } u_i$. Montrer qu'il existe des endomorphismes $a_1, \cdots, a_k$ de E tels que $v = \sum_{i=1}^{k} u_i \circ a_i$.

c) Soit E un $\mathbb{R}$-espace vectoriel de dimension finie. Montrer que les idéaux à droite de l'algèbre $\mathcal{L}(E)$ sont les ensembles de la forme $\mathcal{I}_F = \{u \in \mathcal{L}(E) \mid \text{Im } u \subset F\}$, où F est un sous-espace vectoriel de E.

2) ***Idéaux à gauche de*** $\mathcal{L}(E)$

a) Soient E, F, G trois espaces vectoriels, soient $w \in \mathcal{L}(E,G)$ et $u \in \mathcal{L}(E,F)$. Montrer l'équivalence

$$\ker u \subset \ker w \Longleftrightarrow \exists v \in \mathcal{L}(F,G) \quad w = v \circ u \ .$$

b) Soient $u_1, \cdots, u_k$ et v des endomorphismes d'un espace vectoriel E tels que $\bigcap_{i=1}^{k} \ker u_i \subset \ker v$. Montrer qu'il existe des endomorphismes $a_1, \cdots, a_k$ de E tels que $v = \sum_{i=1}^{k} a_i \circ u_i$.

c) Soit E un $\mathbb{R}$-espace vectoriel de dimension finie. Montrer que les idéaux à gauche de l'algèbre $\mathcal{L}(E)$ sont les ensembles de la forme $\mathcal{J}_F = \{u \in \mathcal{L}(E) \mid F \subset \ker u\}$, où F est un sous-espace vectoriel de E.

*Exercice 5 . **Nilradical.***
Soit A un anneau commutatif. Le *nilradical* de A est l'ensemble,

$$nil(A) = \{a \in A \ \exists n \in \mathbb{N} \text{ tel que } a^n = 0_A\}$$

c'est-à-dire l'ensemble des nilpotents de A. Montrer que :

1) $nil(A)$ est un idéal de A.

2) Si $\mathcal{I}$ est un idéal premier de A, alors $nil(A) \subset \mathcal{I}$.

3) $nil(A/nil(A)) = \{0_A\}$.

2 Arithmétique.

*Exercice 6 . **Fonction indicatrice d'Euler.***
l'indicateur d'Euler d'un entier positif n, noté $\varphi(n)$ est défini comme étant le nombre d'entiers positifs inférieurs ou égaux à n et premiers avec n.

1) **Justifier la relation $\varphi(n) = \text{card}\,(Z/n\mathbb{Z})^*$, où $(Z/n\mathbb{Z})^*$ désigne l'ensemble des éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$.**
2) **Montrer que p premier si et seulement si $\varphi(p) = p - 1$.**
3) **Soit p premier et $\alpha \in \mathbb{N}$. Donner tous les multiples de p inférieurs à p^α, puis en déduire que : $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.**
4) **Soit n et m premiers entre eux.**
   a) **Construire un isomophisme $\psi : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/nm\mathbb{Z}$**
   b) **Montrer $\forall (a,b) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, on a (a,b) est inversible dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ si et seulement si $\psi(a,b)$ est inversible dans $\mathbb{Z}/nm\mathbb{Z}$.**
   c) **En déduire que $\varphi(nm) = \varphi(n)\varphi(m)$.**
5) **Soit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ où p_i sont des nombres premiers, en déduire $\varphi(n)$.**
   Calculer $\varphi(180)$.
6) **Soit $a \in \mathbb{N}^*$ premier avec n,**
   a) **Montrer que l'application : $\phi : \begin{array}{ccc} (Z/n\mathbb{Z})^* & \longrightarrow & (Z/n\mathbb{Z})^* \\ x & \longmapsto & ax \end{array}$ est bien définie et bijective.**
   b) **En déduire que $\displaystyle\prod_{x \in U} x = \prod_{x \in U} \phi(x)$.**
   c) **En déduire que : $a^{\varphi(n)} \equiv 1 \pmod{n}$ Théorème d'Euler.**

*Exercice 7 . **Cryptographie-RSA.***
Soit p et q deux nombres premiers, on pose $n = pq$. Soit M un entier naturel premier avec pq, qui représente le message à décoder, et C le message codé envoyé.

1) **Dites pourquoi $\varphi(n) = (p-1)(q-1)$.**
2) **Soit e premier avec $\varphi(n)$, justifier l'existence de $d \in \mathbb{Z}$ tel que $ed \equiv 1 \pmod{\varphi(n)}$.**
3) **Le message M est codé en C tel que $C \equiv M^e \pmod{n}$.**
   En déduire que : $C^d \equiv M \pmod{n}$.
   Indication : On pourra penser à utiliser le théorème d'Euler.
4) ***Application numérique* : On prend $p = 3, q = 5$ et $M = 7$, donner les messages codé C et décodé D.**
   On prend cette fois $M = 12$, que remarquez vous aprés avoir fait les calcul. Expliquer ce phénomène et dite comment y remedier.

*Exercice 8 . **Application du théorème chinois.***
Une bande de 17 pirates dispose d'un butin composé de N pièces d'or d'égale valeur. Ils décident de se le partager également et de donner le reste au cuisinier (non pirate). Celui ci reçoit 3 pièces.
Mais une rixe éclate et 6 pirates sont tués. Tout le butin est reconstitué et partagé entre les survivants comme précédemment ; le cuisinier reçoit alors 4 pièces.
Dans un naufrage ultérieur, seuls le butin, 6 pirates et le cuisinier sont sauvés. Le butin est à nouveau partagé de la même manière et le cuisinier reçoit 5 pièces.
Quelle est alors la fortune minimale que peut espérer le cuisinier lorsqu'il décide d'empoisonner le reste des pirates ?
***Réponse* : 785**

3 Polynôme minimal et éléments propres.

*Exercice 9 . **Endomorphisme nilpotent.***

1) Soit E un $\mathbb{K}$-espace vectoriel de dimension finie égale à n et $u \in \mathcal{L}(E)$ tel que $\deg \pi_u = p$.
Montrer que $(u^k)_{0\leq k\leq m}$ est libre dans $\mathcal{L}(E)$, $\forall m \leq p-1$.

2) On suppose maintenant que u est nilpotent d'indice $q \in \mathbb{N}^*$.

a) Montrer que $d \leq q$.

b) Montrer que $\exists x_0 \in E$ tel que $(u^k(x_0))_{0\leq k\leq q-1}$ est libre dans E.

c) En déduire que $q \leq n$.

d) Montrer que $(u^k)_{0\leq k\leq q-1}$ est libre dans $\mathcal{L}(E)$.

*Exercice 10 . **Matrice stochastique.***

Soit A une matrice stochastique de $\mathcal{M}_n(\mathbb{R})$ à coéfficients strictement positifs, i.e.

$$\begin{aligned} &a_{i,j} > 0 \qquad \forall i,j \in [\![1,n]\!] \\ &\sum_{j=1}^{n} a_{i,j} = 1 \quad \forall i \in [\![1,n]\!] \end{aligned}$$

Montrer les résultats suivants :

1) 1 est valeur propre de A et que E_1 le sous-espace propre associé est de dimension ègale à 1.

2) Pour toute valeur propre $\lambda \in \mathbb{C}$ de A, on a : $|\lambda| \leq 1$.

3) Si λ est valeur propre telle que $|\lambda| = 1$ alors $\lambda = 1$.

*Exercice 11 . **Nombres algébriques.***

Un nombre complexe z est dit *algébrique* s'il est solution d'une équation polynômiale à coefficients dans $\mathbb{Z}$. Dans le cas contraire on dit qu'il est *transcendant*.

1) Montrer que tout nombre rationnel est algébrique.

2) Donner un exemple de nombre réel transandent.

3) Soit $z \in \mathbb{C}$.

a) Montrer que z est algébrique si et seulement si $\exists P \in \mathbb{Q}[X]$ tel que $P(z) = 0$. On dit alors que P est un polynôme annulateur pour z.

b) Montrer que l'ensemble $\mathcal{I}_z = \{P \in \mathbb{Q}[X] \text{ tel que } P(z) = 0\}$ est soit vide, soit un idéal de $\mathbb{Q}[X]$.

c) En déduire que tout nombre algébrique z, admet un unique polynôme annulateur unitaire de degré minimal qui divise tous les autres polynômes annulateurs. On le note π_z.

4) Donner les polynômes minimaux suivants : $\pi_{\sqrt{2}}$ et π_j où $j = \mathrm{e}^{\frac{2i\pi}{3}}$.

Fin
à la prochaine