Examen 6L23 : Arithmétique dans les anneaux jeudi 16 juin 2011
9h00–12h00

Le polycopié du cours est l'unique document autorisé.

Vous pouvez utiliser tout résultat du cours, ainsi que les énoncés des question précédentes.

Les parties sont indépendantes.

1. Dans cet exercice K désigne d'abord un corps commutatif quelconque, qui sera spécialisé ensuite par $K = \mathbf{Q}$ ou par $K = \mathbf{R}$. On considérera d'abord une matrice carrée quelconque $A \in \mathcal{M}_n(K)$, qui sera spécialisée ensuite par une matrice spécifique dans $\mathcal{M}_2(K)$.

a. On considère ici $\mathcal{M}_n(K)$ comme une espace vectoriel sur K (structure définie par l'addition et multiplication scalaire des matrices uniquement), espace dans lequel les puissances A^i de A pour $i \in \mathbf{N}$ sont des vecteurs. Pourquoi la famille infinie $A^0 = \mathrm{id}, A^1 = A, A^2, A^3, \ldots$ de vecteurs ne peut-elle pas être libre ?

b. D'après la question précédente il existe $d \in \mathbf{N}$ telle que la famille $A^0, A^1, \ldots, A^d$ soit liée ; on prend d minimal, de sorte que la famille $A^0, A^1, \ldots, A^{d-1}$ soit libre. Montrer qu'il existe un d-uplet unique de coefficients $c_0, \ldots, c_{d-1} \in K$ tels que $c_0 A^0 + \cdots + c_{d-1} A^{d-1} = A^d$.

c. On sait que l'application $f : K[X] \to \mathcal{M}_n(K)$ vérifiant $f(\sum_{i=0}^k a_i X^i) = \sum_{i=0}^k a_i A^i$ (substitution de A pour X, notée $f(P) = P(A)$) est un morphisme d'anneaux. Décrire $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$.

d. Quelle est la relation entre le polynôme minimal de A et les réponses aux questions *b,c* ?

e. Sous quelle condition le sous-anneau commutatif $K[A] = \mathrm{Im}(f)$ de $\mathcal{M}_n(K)$ est-il un corps ?

f. On spécialise maintenant $A = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right) \in \mathcal{M}_2(K)$. Déterminer d et $c_0, \ldots, c_{d-1}$ de la question *b*.

g. On suppose que $K = \mathbf{Q}$ ou $K = \mathbf{R}$ (les deux cas se traitent simultanément), montrer qu'un morphisme d'anneaux $g : K[A] \to \mathbf{R}$, avec $g(\lambda\,\mathrm{id}) = \lambda$ pour tout $\lambda \in K$, est déterminé par $g(A) \in \mathbf{R}$. Déduire de la relation $c_0 A^0 + \cdots + c_{d-1} A^{d-1} = A^d$, qui est explicitée dans la question précédente, que seulement deux valeurs pour $g(A)$ sont possibles, qu'on spécifiera.

h. Montrer que $K[A]$ est un corps si $K = \mathbf{Q}$. Indiquer un sous-corps de $\mathbf{R}$ auquel il est isomorphe.

i. Maintenant on spécialise $K = \mathbf{R}$. Montrer que dans ce cas $K[A]$ n'est pas un anneau intègre.

j. Soient g_+, g_- les deux morphismes d'anneaux $\mathbf{R}[A] \to \mathbf{R}$ qui sont possibles d'après la question *f*. Montrer que $g_\pm : \mathbf{R}[A] \to \mathbf{R} \times \mathbf{R}$ donné par $g_\pm(x) = (g_+(x), g_-(x))$ est un isomorphisme d'anneaux, et décrire son morphisme inverse.

2. Dans cet exercice K est un corps commutatif qui sera spécialisé à la question *d*.

a. On suppose que deux polynômes $P, Q \in K[X]$ sont premiers entre eux. Montrer que l'idéal de $K[X]$ engendré par P et Q est égal à $K[X]$ tout entier.

b. La question précédente implique par le lemme chinois pour les idéaux (vu en TD) que le morphisme d'anneaux $f : K[X] \to K[X]/(P) \times K[X]/(Q)$, qui associe à un polynôme la paire de sa classe modulo P et celle modulo Q, est surjectif. Conclure qu'on a un isomorphisme $K[X]/\mathrm{Ker}(f) \to K[X]/(P) \times K[X]/(Q)$, et donner explicitement ce noyau $\mathrm{Ker}(f)$.

c. Soit $p > 2$ un nombre premier. Montrer que $a \in \mathbf{Z}/p\mathbf{Z}$ est un carré dans $\mathbf{Z}/p\mathbf{Z}$ (et donc la classe d'un carré k^2 avec $k \in \mathbf{Z}$) si et seulement si $a^{\frac{p-1}{2}} \in \{\overline{0}, \overline{1}\} \subseteq \mathbf{Z}/p\mathbf{Z}$. Combien de solutions a possède l'équation $a^{\frac{p-1}{2}} = \overline{0}$? Et $a^{\frac{p-1}{2}} = \overline{1}$? *(Utiliser la structure connue du groupe* $(\mathbf{Z}/p\mathbf{Z})^\times$*.)*

d. Soit maintenant $K = \mathbf{Z}/p\mathbf{Z}$, $Q = X^2 + bX + c \in K[X]$ un polynôme quadratique unitaire, et $\Delta = b^2 - 4c \in K$ son discriminant. Montrer que (1) si $\Delta = 0$ alors Q est le carré d'un polynôme de degré 1 ; (2) si $\Delta^{\frac{p-1}{2}} = \overline{1}$ alors Q est le produit de deux polynômes distincts de degré 1 ; (3) sinon on a l'égalité $\Delta^{\frac{p-1}{2}} = \overline{p-1} \in K$, et Q est irréductible dans $K[X]$.

e. Montrer que l'anneau $A = K[X]/(Q)$ a p^2 éléments, et que selon les trois cas décrits on a: (1) A contient au moins un élément nilpotent non nul ; (2) A contient des diviseurs de zéro mais pas d'éléments nilpotents non nuls ; (3) A est un corps commutatif.

f. On considère un nombre $n \in \mathbf{Z}$ dont la classe modulo p n'est pas un carré dans $\mathbf{Z}/p\mathbf{Z}$. Alors l'anneau commutatif $R = \mathbf{Z}[\sqrt{n}] \cong \mathbf{Z}[X]/(X^2 - n)$ est intègre et contient $\mathbf{Z}$ et donc le nombre p. Montrer p est un élément irréductible et même premier de l'anneau R.

continué au verso

3. Cet exercice considère la résolution d'un système de relations de congruence dans $\mathbf{Z}$. L'outil principal est l'algorithme d'Euclide étendu, qui calcule pour deux entiers a, b à la fois $d = \text{pgcd}(a, b)$ et des coefficients s, t d'une relation de Bezout $d = sa+tb$. Cet algorithme assez élémentaire a été mentionné dans le cours (en haut de page 22), mais n'a pas été le sujet d'exercices de TD. On rappelle que l'idée de base est de déterminer pour toutes les valeurs intermédiaires (restes) dans l'algorithme d'Euclide aussi des coefficients qui les expriment en combinaison linéaire de a et b. Si toutefois vous n'arrivez pas à déterminer correctement les coefficients de Bezout nécessaires, vous pouvez les nommer et exprimer les résultats suivants symboliquement en termes de ces coefficients.

On considère les deux congruences suivantes, pour $x \in \mathbf{Z}$:

$$74x \equiv 22 \pmod{84} \tag{1}$$
$$x \equiv 67 \pmod{130} \tag{2}$$

a. Argumenter, après le calcul seulement d'un pgcd dans $\mathbf{Z}$, que la congruence (1) possède des solutions. Que peut-on dire (sans le calculer explicitement) de l'ensemble de ses solutions ?

b. Déterminer l'inverse de (la classe de) 37 dans $\mathbf{Z}/42\mathbf{Z}$.

c. Trouver une solution particulière de la congruence (1), et décrire ensuite l'ensemble de toutes ses solutions.

d. On considère maintenant le système des deux congruences (1) et (2), dont la première a été simplifiée dans les questions précédentes pour donner un système de la forme

$$x \equiv a_1 \pmod{n_1} \tag{3}$$
$$x \equiv a_2 \pmod{n_2} \tag{4}$$

avec $a_1, a_2, n_1, n_2 \in \mathbf{Z}$ (en fait $a_2 = 67$, $n_2 = 130$). Calculer $d = \text{pgcd}(n_1, n_2)$ et déduire de chacune des congruences une congruence modulo d. Les deux congruences sont-elles compatibles ?

e. Si r est le reste modulo d que toute solution du système doit avoir (trouvé dans la question précédente), on peut introduire une nouvelle variable $x' = \frac{x-r}{d}$. Donner un système de congruences pour x' de la forme

$$x' \equiv a'_1 \pmod{n'_1} \tag{5}$$
$$x' \equiv a'_2 \pmod{n'_2} \tag{6}$$

où en plus n'_1 et n'_2 sont premiers entre eux.

f. Montrer que si $y \in \mathbf{Z}$ vérifie $y \equiv 0 \pmod{n'_1}$ et $y \equiv 1 \pmod{n'_2}$, alors l'ensemble des solutions du système ((5),(6)) est formé des x' vérifiant $x' \equiv a'_1 + y(a'_2 - a'_1) \pmod{n'_1 n'_2}$.

g. Trouver un tel y à l'aide d'une relation de Bezout pour n'_1, n'_2.

h. Terminer en donnant les solutions du système ((1),(2)) du départ.

Fin.