Examen Arithmétique et algèbre commutative jeudi 28 juin 2018
13h30–16h30

L'usage de tout document et de tout matériel électronique est interdit. La notation prendra en compte la clarté et la rigueur des raisonnements, toutes les réponses doivent être justifiées. Tous les anneaux considérés sont unitaires. Le sujet contient 4 parties indépendantes.

1. *Question de cours.* Donner l'énoncé du premier théorème d'isomorphisme pour les anneaux commutatifs, et décrire comment l'isomorphisme dont parle ce théorème est défini.

2. *a.* Résoudre pour $x \in \mathbf{Z}$ la congruence $39x \equiv 1 \pmod{62}$.

b. Résoudre pour $x \in \mathbf{Z}$ le système de congruences

$$\begin{cases} x \equiv 3 & \pmod{14} \\ x \equiv 10 & \pmod{23} \end{cases} .$$

3. Soit $n \in \mathbf{Z}$ un entier non nul, $I = n\mathbf{Z}$ l'idéal de $\mathbf{Z}$ engendré par n, et J l'idéal de $\mathbf{Z}[X]$ engendré par n (considéré comme polynôme constant). On pose $B = \mathbf{Z}/n\mathbf{Z}$, avec $\pi : \mathbf{Z} \to B$ la projection canonique (réduction modulo n).

a. Montrer que J est égal à l'ensemble de polynômes de $\mathbf{Z}[X]$ dont les coefficients sont tous divisibles par n.

b. Soit $f : \mathbf{Z}[X] \to B[X]$ l'application définie par $f(\sum_i a_i X^i) = \sum_i \pi(a_i) X^i$ (réduction de tous les coefficients d'un polynôme modulo n), dont on admet que c'est un morphisme d'anneaux. Utiliser le premier théorème d'isomorphisme pour montrer que $\mathbf{Z}[X]/J \cong B[X]$.

c. Pour $P \in \mathbf{Z}[X]$ quelconque, montrer que $\mathbf{Z}[X]/(n, P)$ est isomorphe à $B[X]/(f(P))$.

d. On prend maintenant $n = 7$ est $P = 14X^4 + X^3 - X^2 + 4$. Montrer que l'anneau $\mathbf{Z}[X]/(n, P)$ est fini, et déterminer son cardinal (nombre d'éléments).

e. Montrer que cet anneau $\mathbf{Z}[X]/(n, P)$ est un corps.

4. Soit K un corps, et $a, b \in K$ deux éléments distincts. On définit l'idéal I de $K[X]$ comme celui engendré par le produit $(X - a)(X - b) = X^2 - (a + b)X + ab$, donc $I = ((X - a)(X - b))$.

a. Rappeler pourquoi les restes de la division de $P \in K[X]$ par $X - a$, respectivement par $X - b$, sont des polynômes constants, dont les valeurs respectives sont données par les évaluations $P[a]$ respectivement $P[b]$.

b. L'application $f : K[X] \to K \times K$ donnée par $P \mapsto (P[a], P[b])$ est un morphisme d'anneaux. Montrer qu'il existe une application unique $\tilde{f} : K[X]/I \to K \times K$ telle que $f = \tilde{f} \circ \pi$ pour la projection canonique $\pi : K[X] \to K[X]/I$ (c'est-à-dire, avec $f(P) = \tilde{f}(\pi(P))$ pour tout P).

c. Montrer que $\tilde{f}$ est un isomorphisme d'anneaux (entre $K[X]/I$ et l'anneau produit $K \times K$).

d. Rappeler pourquoi toute classe de polynômes dans $K[X]/I$ s'écrit de manière unique comme la classe $\pi(c_0 + c_1X)$ d'un polynôme de degré < 2, et que si on fait ceci pour la classe $\pi(P)$ d'un polynôme P, alors il faut prendre pour $c_0 + c_1X$ le reste de la division de P par $(X - a)(X - b)$.

e. Décrire ce reste $c_0 + c_1X$ en termes (seulement) des évaluations $x = P[a]$ et $y = P[b]$. (Il s'agit ici essentiellement de décrire l'application réciproque de $\tilde{f}$: pour $(x, y) = (P[a], P[b]) \in K \times K$ donnés, trouver la description $C = \pi(c_0 + c_1X)$ de la classe $C \in K[X]/I$ telle que $\tilde{f}(C) = (x, y)$.)

Fin.