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

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.

√ *Si $f : A \to B$ est un morphisme d'anneau unitaires, de noyau $I = \ker(f) \subseteq A$ et d'image $S = \mathrm{Im}(f) \subseteq B$, alors il existe un isomorphisme $g : A/I \to S$. Celui-ci est défini par $g(a + I) = f(a)$, pour toute classe $a + I$ de A/I.*

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

√ $x \equiv -27 \equiv 35 \pmod{62}$

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

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

√ *Avec la relation de Bézout* $\mathrm{pgcd}(14, 23) = 1 = 5 \times 14 - 3 * 69$ *on peut trouver* $x \equiv 171 \pmod{322}$ *de diverses manières, par exemple* $3 \times -69 + 10 \times 70 = 493 \equiv 171 \pmod{322}$ *(via* $70 \equiv 0 \pmod{14}$, $70 \equiv 1 \pmod{23}$, $-69 \equiv 1 \pmod{14}$, $-69 \equiv 0 \pmod{23}$ *et* $\mathrm{ppcm}(14, 23) = 14 \times 23 = 322$*).*

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.

√ *Clairement, si l'on multiplie un polynôme par n on multiplie tous ses coefficients par n, et le résultat est qu'ils sont tous divisible par n. Réciproquement si tous les coefficients de P sont divisibles par n, il suffit de les diviser tous par n pour trouver les coefficients d'un polynôme Q vérifiant $nQ = P$, ce qui montre que $P \in J$.*

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 $\mathbf{Z}[X]/J \cong B[X]$.

√ *Clairement f est surjectif, car pour $Q = \sum_i b_i X^i \in BX$ il suffit de prendre des représentants a_i de chaque classe b_i, pour obtenir $f(\sum_i a_i X^i) = \sum_i b_i X^i = Q$. Le noyau de f est l'ensemble des polynômes $P \in \mathbf{Z}[X]$ dont tous les coefficients sont congruents à 0 modulo n, qui forment l'idéal J d'après la question précédente. Le premier théorème d'isomorphisme dit alors que $\mathbf{Z}[X]/J$ est isomorphe à l'image de f c'est-à-dire à $B[X]$.*

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

√ *(n, P) est un idéal de $\mathbf{Z}[X]$ contenant J (car contenant n), et son image par f est engendré par $f(n) = 0$ et par $f(P)$; c'est l'idéal de $B[X]$ correspondant à (n, P) par la bijection naturelle entre idéaux de $\mathbf{Z}[X]$ contenant J et ceux de $\mathbf{Z}[X]/J \cong B[X]$. Les quotient par des idéaux correspondants sont isomorphes, ce qui donne ici $\mathbf{Z}[X]/(n, P) \cong B[X]/(f(P))$.*

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).

√ *On a $f(P) = X^3 + \pi(6)X^2 + \pi(4)$, et le quotient de $B[X]$ par ce polynôme est un espace vectoriel dur le corps $B = \mathbf{Z}/7\mathbf{Z}$ de dimension 3 (car les classes sont fidèlement représentées par des polynômes de degré[] < 3 dans $B[X]$, le reste commun de tous les éléments de la classe par $f(P)$). Le cardinal est alors $7^3 = 343$.*

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

√ *Puisque B est un corps, le quotient $B[X]/(f(P))$ est un corps si et seulement si $f(P)$ est irréductible dans $B[X]$. Puisque c'est un polynôme de degré 3, il doit avoir un facteur de degré 1 s'il est réductible, et donc une racine dans $B = \mathbf{Z}/7\mathbf{Z}$. Mais l'évaluation de $X^3 + \pi(6)X^2 + \pi(4)$ en tous les 7 éléments $X = \pi(0), \ldots, \pi(6)$ de B donne des valeurs non nulles (les classes de respectivement $4, 4, 1, 1, 3, 6, 2$), donc il est sans racines, et irréductible comme voulu.*

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 $P[b]$.

$\surd$ *Les restes sont de degré*$[] < 1$, *et donc des polynômes constants. Si* $P = (X-a)Q + r$, *application aux deux côtés de cette égalité du morphisme d'anneaux d'évaluation en* $X := a$ *donne* $P[a] = 0Q[a] + r = r$.

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).

$\surd$ *C'est le passage de* f *au quotient* $K[X]/I$, *qui est possible si* $I \subseteq \ker(f)$. *Puisque clairement* $f((X-a)(X-b)) = (0,0)$ *et* $(X-a)(X-b)$ *est générateur de* I, *on a en effet* $I \subseteq \ker(f)$.

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

$\surd$ *Par définition* $\ker(f)$ *est formé des polynômes ayant à la fois* a *et* b *comme racines, donc de ceux divisible par* $X-a$ *et par* $X-b$, *mais ce sont précisément les multiplies de* $\mathrm{ppcm}(X-a, X-b) = (X-a)(X-b)$ *(car* $X-a$ *et* $X-b$ *sont premiers entre eux), donc* $\ker(f) = I$ *et* $\tilde{f}$ *est injectif. Sa surjectivité est aussi conséquence du fait que* $X-a$ *et* $X-b$ *sont premiers entre eux, car si* $S(X-a)+T(X-b) = 1$ *est une relation de Bézout alors* $f(S(X-a)) = (0,1)$ *et* $f(T(X-b)) = (0,1)$, *d'où* f *et donc* $\tilde{f}$ *est surjectif. (On aurait aussi pu invoque la dimension :* $\dim_K(K[X]/I) = 2$ *et c'est aussi la* K*-dimension de* $K \times K$, *donc une application linéaire injective est automatiquement surjective.*

d. Rappeler pourquoi toute classe de polynômes dans $K[X]/I$ s'écrit de manière unique comme la classe $\pi(c_0 + c_1 X)$ 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 $c_0 + c_1 X$ le reste de la division de P par $(X-a)(X-b)$.

$\surd$ *Si* $R = c_0 + c_1 X$ *est ce reste, alors* $P \equiv R \pmod{I}$, *et donc* $\pi(P) = \pi(R)$. *Aussi* R *est l'unique polynôme de degré* $< 2 = \deg((X-a)(X-b))$ *avec* $P \equiv R \pmod{I}$, *d'où l'unicité.*

e. Décrire ce reste $c_0 + c_1 X$ 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 $C = \pi(c_0 + c_1 X)$ de la classe $C \in K[X]/I$ telle que $\tilde{f}(C) = (x, y)$.)

$\surd$ *On a* $x = P[a] = R[a] = c_0 + c_1 a$ *et* $y = P[b] = R[b] = c_0 + c_1 b$, *donc* $c_1 = \frac{x-y}{a-b}$, *et* $c_0 = P[a] - c_1 a$; *on trouve*

$$R = -\frac{bx + ay}{a-b} + \frac{x-y}{a-b} X.$$

Fin.