Corrigé Contrôle continu 6L23 : Arithmétique dans les anneaux jeudi 10 mars 2011
10h00–12h00

1. Soit K un corps commutatif, et $K[X]$ son anneau des polynômes. On rappelle que tous les idéaux de $K[X]$ sont principaux ; l'idéal de $K[X]$ engendré par $P \in K[X]$ sera noté (P).

a. Pour $a \in K$ quelconque, montrer que l'anneau quotient $K[X]/(X-a)$ est isomorphe à K. (Indication: on pourra considérer le morphisme $K[X] \to K$ de substitution de a pour X).

√ *Un résultat du cours (1.5.6) dit que $(X-a)$ est le noyau de ce morphisme de substitution. Comme ce morphisme est évidemment surjectif, l'isomorphisme cherché découle du théorème d'isomorphisme (1.3.4) : $f(R) \cong R/\ker(f)$. On pourra aussi raisonner que toute classe modulo $(X-a)$ possède un unique représentant dans K, le reste de n'importe que élément de la classe après division par $X-a$.*

b. Dans cette question on considère le polynôme $P = X^3 - 1 \in \mathbf{R}[X]$.

i. Trouver les racines de P dans $\mathbf{R}$, et décomposer P en facteurs irréductibles dans $\mathbf{R}[X]$.

√ *Il est clair que 1 est une racine de P dans $\mathbf{R}$, et le quotient $P/(X-1) = X^2 + X + 1$ est un polynôme quadratique de discriminant $-3 < 0$, qui ne possède donc pas de racines réelles. Comme ce quotient est de degré 2, l'absence de racines dans $\mathbf{R}$, et donc de facteurs de degré 1, montre qu'il est irréductible, donc $P = (X-1)(X^2+X+1)$ est la factorisation cherchée.*

ii. On note P_1 le facteur irréductible de degré 1 de P dans $\mathbf{R}[X]$, et P_2 celui de degré 2. On note j la racine de P_2 dans $\mathbf{C}$ de partie imaginaire positive. Montrer que le noyau du morphisme $\mathbf{R}[X] \to \mathbf{C}$ de substitution de j pour X est (P_2).

√ *Par définition de racine, le morphisme ϕ annule $P_2 = X^2+X+1$, donc son noyau contient (P_2). Montrons que réciproquement tout élément Q du noyau est un multiple de P_2 (c'est-à-dire, $Q \in (P_2)$). Soit $R \in \mathbf{R}[X]$ le reste de division de Q par P_2. Alors $\deg_X(R) < \deg_X(P_2) = 2$ et $\phi(R) = \phi(Q) = 0$ (car $\phi(P_2) = 0$). Si l'on écrit $R = a + bX$ avec $a, b \in \mathbf{R}$ on a $0 = \phi(R) = a + bj$; or comme $j \in \mathbf{C} \setminus \mathbf{R}$, le couple $(1, j)$ est $\mathbf{R}$-linéairement indépendant, donc l'équation $a + bj = 0$ avec $a, b \in \mathbf{R}$ implique $a = b = 0$, c'est-à-dire $R = 0$, donc $Q \in (P_2)$.*

iii. Définir un morphisme d'anneaux $\mathbf{R}[X] \to \mathbf{R} \times \mathbf{C}$ dont le noyau est (P), et montrer qu'il est surjectif (pour qu'une application vers un produit direct d'anneaux soit un morphisme d'anneaux, il faut et il suffit que ses composantes soient des morphismes d'anneaux).

√ *On définit le morphisme $\pi : Q \mapsto (\rho(Q), \phi(Q))$ où $\rho : Q \mapsto Q[X := 1] \in \mathbf{R}$ et $\phi : Q \mapsto Q[X := j] \in \mathbf{C}$ sont les morphismes des question précédentes. Le noyau de ce morphisme est l'intersection $(P_1) \cap (P_2)$ des noyaux de ρ et ϕ, qui est engendré par $\operatorname{ppcm}(P_1, P_2) = P_1 P_2 = P$ (car P_1, P_2 n'ont pas de facteur commun). On a $\pi(P_1) = (0, j-1)$, $\pi(P_2) = (3, 0)$ et $\pi(3 - P_2) = (0, 3)$, quel trois images sont clairement $\mathbf{R}$-linéairement indépendantes dans $\mathbf{R} \times \mathbf{C}$, ce qui montre que π, qui est certainement $\mathbf{R}$-linéaire, est surjectif. (Un argument un peu plus explicite utilise des coefficients de Bezout $S, T \in \mathbf{R}[X]$ tels que $P_1 S + P_2 T = \operatorname{pgcd}(P_1, P_2) = 1$: on a $\pi(P_1 S) = (0, 1)$ et $\pi(P_2 T) = (1, 0)$, donc $\pi(bP_1 S + (b + cX)P_2 T) = (a, b + cj) \in \mathbf{R} \times \mathbf{C}$ pour $a, b, c \in \mathbf{R}$. On pourra prendre $T = \frac{1}{3}$, $S = -\frac{1}{3}(X+2)$ pour être complètement explicite.)*

iv. Montrer que $\mathbf{R}[X]$ contient exactement 2 idéaux propres qui contiennent strictement (P) qu'on décrira explicitement, et montrer que ce sont des idéaux premiers. (P) est-il premier ?

√ *Les idéaux qui contiennent (P) correspondent (1.3.3) aux idéaux de $\mathbf{R}[X]/(P) \cong \mathbf{R} \times \mathbf{C}$. Si un idéal d'un produit direct $R \times S$ contient (x, y), il contient aussi $(1, 0) \times (x, y) = (x, 0)$ et $(0, 1) \times (x, y) = (0, y)$, et réciproquement s'il contient $(x, 0)$ et $(0, y)$ il contient $(x, 0) + (0, y) = (x, y)$. Par conséquent un sous-ensemble du produit est un idéal si et seulement s'il est le produit de ses projections sur les facteurs, qui sont tous les deux des idéaux de ces facteurs (vérification immédiate). Or les seuls idéaux des corps $\mathbf{R}$ et $\mathbf{C}$ sont l'idéal $\{0\}$ et le corps entier. En combinant on a 4 idéaux de $\mathbf{R} \times \mathbf{C}$, dont l'idéal nul et $\mathbf{R} \times \mathbf{C}$ tout entier ; il reste les deux idéaux propres $\mathbf{R} \times \{0\}$ et $\{0\} \times \mathbf{C}$. Ces idéaux étant maximaux, ils sont aussi premiers. Ils correspondent dans $\mathbf{R}[X]$ aux idéaux (P_2) et (P_1) respectivement, qui sont effectivement propres, premiers, et contiennent strictement (P). Quant à (P), il n'est pas premier car le quotient $\mathbf{R}[X]/(P) \cong \mathbf{R} \times \mathbf{C}$ n'est pas intègre. On aurait aussi pu raisonner (et c'est plus simple quand on sait que $\mathbf{R}[X]$ est factoriel) que les idéaux qui contiennent strictement (P) sont engendrés par des diviseurs stricts de P, où on trouve (à association près) seulement les éléments (premiers) P_1 et P_2 (et le diviseur trivial 1, mais qui engendre un idéal malpropre).*

c. On revient sur la cas général d'un corps commutatif K. Soit $P \in K[X]$ quelconque. Montrer que l'idéal (P) est maximal si et seulement si P est irréductible dans $K[X]$.

√ *Si $P \in K$, l'idéal (P) n'est pas maximal et P n'est pas irréductible. On peut donc supposer $P \notin K$. Un autre polynôme $Q \notin K$ divise P strictement si et seulement si (Q) contient (P) strictement. Dire qu'un tel Q n'existe pas (c'est-à-dire P irréductible) veut dire que (P) est maximal parmi les idéaux principaux propres, donc (tous les idéaux étant principaux) que (P) est un idéal maximal.*

d. On suppose maintenant $P \in K[X]$ irréductible et $k \geq 2$ un entier. Montrer que tout idéal premier de $K[X]/(P^k)$ contient l'image de P, et en déduire qu'il n'y a qu'un tel idéal premier.

√ *Soit $\overline{P}$ l'image de P dans $K[X]/(P^k)$. Si $\mathfrak{p}$ est un idéal premier de $K[X]/(P^k)$, alors $\overline{P}^k = 0 \in \mathfrak{p}$ implique que l'un au moins des k facteurs à gauche appartient à $\mathfrak{p}$, et on a donc $\overline{P} \in \mathfrak{p}$. Par conséquent $\mathfrak{p}$ contient $(\overline{P})$, qui (car il correspond à l'idéal (P) de $K[X]$, toujours via 1.3.3) est un idéal maximal d'après la question précédente, et $\mathfrak{p} = (\overline{P})$ est le seul idéal premier de $K[X]/(P^k)$.*

2. Soit p, q deux nombres premiers distincts, et $k, l \geq 1$ deux entiers ; on pose $n = p^k q^l$.

a. Déterminer dans l'anneau $\mathbf{Z}/p^k\mathbf{Z}$ l'ensemble des éléments inversibles, et prouver que tous les autres éléments sont nilpotents.

√ *Pour que l'image de $a \in \mathbf{Z}$ modulo p^k soit inversible, il faut et il suffit que $\operatorname{pgcd}(a, p^k) = 1$, c'est à dire que p ne divise pas a. Tous les autres éléments de $\mathbf{Z}/p^k\mathbf{Z}$ sont l'image d'un multiple px de p, et la classe de $(px)^k = p^k x^k$ dans $\mathbf{Z}/p^k\mathbf{Z}$ est nulle, donc ces éléments sont nilpotents.*

b. Montrer que l'unique morphisme d'anneaux $\phi : \mathbf{Z} \to \mathbf{Z}/p^k\mathbf{Z} \times \mathbf{Z}/q^l\mathbf{Z}$ est surjectif, et déterminer son noyau.

√ *Comme p ne divise pas q^l, l'image de q^l dans $\mathbf{Z} \to \mathbf{Z}/p^k\mathbf{Z}$ est inversible, disons $q^l a \equiv 1 \pmod{p^k}$, et on a donc $\phi(q^l a) = (1, 0)$. Mais alors $\phi(1 - q^l a) = (0, 1)$, et comme l'image de ϕ est un sous-groupe additif, ϕ est surjectif. Son noyau est formé par les multiples communs de p^k et q^l, c'est-à-dire par les multiples de $\operatorname{ppcm}(p^k, q^l) = p^k q^l = n$. Ce dernier fait implique aussi la surjectivité, car $\#\mathbf{Z}/n\mathbf{Z} = n = \#(\mathbf{Z}/p^k\mathbf{Z} \times \mathbf{Z}/q^l\mathbf{Z})$. Ou on peut utiliser le théorème chinois, car $\operatorname{pgcd}(p^k, q^l) = 1$.*

c. Montrer que dans $\mathbf{Z}/n\mathbf{Z}$, l'élément 0 est le seul élément nilpotent si et seulement si $k = l = 1$.

√ *D'après ce qui précède, on a $\mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z} \to \mathbf{Z}/p^k\mathbf{Z} \times \mathbf{Z}/q^l\mathbf{Z}$. Un élément $(x, y) \in \mathbf{Z}/p^k\mathbf{Z} \times \mathbf{Z}/q^l\mathbf{Z}$ est nilpotent si et seulement si x et y le sont dans leurs facteurs respectifs. Les nilpotents dans ces facteurs sont les (images de) multiples respectivement de p et de q, et pour qu'il y en ait distinct de (la classe de) 0 il faut et il suffit que $k > 1$ respectivement $l > 1$. L'une des deux conditions suffit pour avoir un nilpotent non nul dans $\mathbf{Z}/p^k\mathbf{Z} \times \mathbf{Z}/q^l\mathbf{Z}$, et donc dans $\mathbf{Z}/n\mathbf{Z}$, car dans ce cas on pourra choisir $(x, y) \neq (0, 0)$. Une preuve alternative est d'observer que l'image de pq dans $\mathbf{Z}/n\mathbf{Z}$ est nilpotent, car $(pq)^{\max(k,l)} \equiv 0 \pmod{p^k q^l}$, donc on aura des nilpotents non nuls dans $\mathbf{Z}/n\mathbf{Z}$ si $pq < p^k q^l$, c'est-à-dire si $(k, l) \neq (1, 1)$. Si $n = pq$, un nilpotent dans $\mathbf{Z}/n\mathbf{Z}$ doit être l'image d'un élément $a \in \mathbf{Z}$ tel que $pq \mid a^m$ pour un certain m, donc a doit être divisible par p et par q, et donc par $\operatorname{ppcm}(p, q) = pq = n$, et l'image de a dans $\mathbf{Z}/n\mathbf{Z}$ sera nul.*

d. Déterminer tous les idéaux de $\mathbf{Z}/n\mathbf{Z}$. De combien d'idéaux s'agit il au total ?

√ *D'après ce qui est dit à la question **1** b iv, il suffit d'étudier les idéaux de $\mathbf{Z}/p^k\mathbf{Z}$ et de $\mathbf{Z}/q^l\mathbf{Z}$ séparément. Or, les idéaux de $\mathbf{Z}/p^k\mathbf{Z}$ sont tous principaux (car leurs pré-images dans $\mathbf{Z}$ le sont), et comme les (classes de) nombres non divisibles par p sont inversibles dans $\mathbf{Z}/p^k\mathbf{Z}$, chaque élément engendre le même idéal qu'une puissance de (la classe de) p. Il y a donc $k + 1$ idéaux de $\mathbf{Z}/p^k\mathbf{Z}$, engendrés par (les classes de) $1, p, p^2, \ldots, p^k \equiv 0$, et combinés avec les $l + 1$ idéaux de $\mathbf{Z}/q^l\mathbf{Z}$ cela donne $(k + 1)(l + 1)$ idéaux de $\mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}/p^k\mathbf{Z} \times \mathbf{Z}/q^l\mathbf{Z}$, engendrés par les images de $\{ p^i q^j \mid 0 \leq i \leq k, 0 \leq j \leq l \}$. On aurait aussi pu raisonner directement qu'un idéal de $\mathbf{Z}/n\mathbf{Z}$ est engendré par l'image d'un diviseur positif de $n = p^k q^l$, dont on vient de donner l'ensemble complet.*

e. Montrer que $\mathbf{Z}/n\mathbf{Z}$ contient exactement deux idéaux premiers, qu'on précisera.

√ *Pour qu'un idéal de $R \times S$ soit premier, il faut que sa projection sur l'un des deux facteurs soit surjectif (sinon le quotient par l'idéal serait un produit direct d'anneaux non triviaux, qui n'est jamais intègre) et que sa projection sur l'autre soit un idéal premier. Or le seul idéal de $\mathbf{Z}/p^k\mathbf{Z}$ est celui engendré par la classe de p (avec quotient le corps $\mathbf{Z}/p\mathbf{Z}$) ; les deux idéaux premiers de $\mathbf{Z}/n\mathbf{Z}$ sont donc ceux engendrés par les classes de p et de q. Encore une fois, on aurait pu chercher les idéaux premiers de $\mathbf{Z}$ contenant $n\mathbf{Z}$, qui sont engendrés par les seuls facteurs premiers p et q de n.*

f. Montrer que l'intersection de ces idéaux premiers est égale à l'ensemble des éléments nilpotents.

√ *L'intersection des deux idéaux premiers est l'idéal de $\mathbf{Z}/n\mathbf{Z}$ engendré par la classe de pq, et un élément de $\mathbf{Z}/n\mathbf{Z}$ est nilpotent si c'est la classe d'un nombre à la fois divisible par p et par q. C'est bien le même ensemble.*

Fin.