Corrigé Contrôle continu 6L23 : Arithmétique dans les anneaux vendredi 16 mars 2012
10h00–12h00

1. Dans cette partie on fixe $n \in \mathbf{N} - \{0\}$ et on étudiera les idéaux de $\mathbf{Z}/n\mathbf{Z}$.

a. Rappeler pourquoi les idéaux de $\mathbf{Z}/n\mathbf{Z}$ sont en bijection avec les idéaux de $\mathbf{Z}$ contenant $n\mathbf{Z}$ (il suffit de citer un résultat général). Décrire concrètement quels sont ces idéaux de $\mathbf{Z}$, et de $\mathbf{Z}/n\mathbf{Z}$.

$\surd$ *Les idéaux d'un anneau quotient R/I sont en bijection avec les idéaux de R qui contiennent I (proposition 1.3.3). Dans le cas $R = \mathbf{Z}$ et $I = n\mathbf{Z}$ cela donne une bijection entre les idéaux de $\mathbf{Z}/n\mathbf{Z}$ et les idéaux de $\mathbf{Z}$ contenant $n\mathbf{Z}$. Concrètement ce sont les idéaux $d\mathbf{Z}$ où d est un diviseur de n (et on peut se limiter aux diviseurs $d > 0$ pour éviter de décrire l'idéal $d\mathbf{Z} = -d\mathbf{Z}$ deux fois).*

b. Soit d un diviseur de n, exhiber soigneusement un isomorphisme entre les deux anneaux quotient $(\mathbf{Z}/n\mathbf{Z})/(d\mathbf{Z}/n\mathbf{Z})$ et $\mathbf{Z}/d\mathbf{Z}$.

$\surd$ *Comme le noyau $d\mathbf{Z}$ de la projection canonique $\pi_d : \mathbf{Z} \to \mathbf{Z}/d\mathbf{Z}$ contient $n\mathbf{Z}$, cette projection induit un morphisme d'anneaux $\overline{\pi_d} : \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/d\mathbf{Z}$, qui est l'unique morphisme tel que $\pi_d = \overline{\pi_d} \circ \pi_n$. Le noyau de $\overline{\pi_d}$ est formé des images par π_n des éléments du noyau $d\mathbf{Z}$ de π_d; ces images forment précisément l'idéal $d\mathbf{Z}/n\mathbf{Z}$ de $\mathbf{Z}/n\mathbf{Z}$. Par le théorème d'isomorphisme (corollaire 1.3.4) il existe en isomorphisme canonique $(\mathbf{Z}/n\mathbf{Z})/\ker(\overline{\pi_d}) \to \overline{\pi_d}(\mathbf{Z}/n\mathbf{Z})$. Mais comme $\overline{\pi_d}$ est surjectif vers $\mathbf{Z}/d\mathbf{Z}$ (sinon $\pi_d = \overline{\pi_d} \circ \pi_n$ ne pouvait pas être surjectif, comme il l'est), on a $\overline{\pi_d}(\mathbf{Z}/n\mathbf{Z}) = \mathbf{Z}/d\mathbf{Z}$, et l'isomorphisme canonique $(\mathbf{Z}/n\mathbf{Z})/(d\mathbf{Z}/n\mathbf{Z}) \to \mathbf{Z}/d\mathbf{Z}$ est celui demandé dans la question.*

Soit $n = p_1^{k_1} \dots p_r^{k_r}$ la factorisation de n, avec p_i des nombres premiers distincts, et les $k_i > 0$.

c. Déduire de la question b une description des idéaux premiers de $\mathbf{Z}/n\mathbf{Z}$ en termes des p_i.

$\surd$ *Un idéal I de R est premier si et seulement si R/I est intègre, donc d'après l'isomorphisme de la question b, un idéal $d\mathbf{Z}/n\mathbf{Z}$ de $\mathbf{Z}/n\mathbf{Z}$ est premier si et seulement si $\mathbf{Z}/d\mathbf{Z}$ est intègre, ce qui est le cas si et seulement si d est un nombre premier. Donc $\mathbf{Z}/n\mathbf{Z}$ possède précisément r idéaux premiers, à savoir $p_i\mathbf{Z}/n\mathbf{Z}$ pour $i = 1, \dots, r$.*

d. Calculer $\mathrm{Nilrad}(\mathbf{Z}/n\mathbf{Z})$, l'intersection de tous les idéaux premiers de $\mathbf{Z}/n\mathbf{Z}$, en fonction des p_i.

$\surd$ *Pour que l'image de x dans $\mathbf{Z}/n\mathbf{Z}$ appartienne à $p_i\mathbf{Z}/n\mathbf{Z}$ il est suffisant en nécessaire que $x \in p_i\mathbf{Z}$. Les x dont l'image appartient à l'intersection de tous les idéaux premiers $p_i\mathbf{Z}/n\mathbf{Z}$ sont donc les entiers divisible par tous les p_i à la fois, et donc par leur ppcm qui est en fait leur produit $p_1 \dots p_r$. Alors $\mathrm{Nilrad}(\mathbf{Z}/n\mathbf{Z}) = p_1 \dots p_r\mathbf{Z}/n\mathbf{Z}$.*

e. Donner un morphisme d'anneaux $\mathbf{Z}/n\mathbf{Z} \to (\mathbf{Z}/p_1^{k_1}\mathbf{Z}) \times \dots \times (\mathbf{Z}/p_r^{k_r}\mathbf{Z})$, et montrer que c'est un isomorphisme.

$\surd$ *Comme $p_i^{k_i}$ divise n pour tout i, on a un morphisme $\mathbf{Z}/n\mathbf{Z} \to (\mathbf{Z}/p_1^{k_1}\mathbf{Z}) \times \dots \times (\mathbf{Z}/p_r^{k_r}\mathbf{Z})$ donné par*

$$\pi : x \mapsto (\overline{\pi_{p_1^{k_1}}}(x), \dots, \overline{\pi_{p_r^{k_r}}}(x))$$

avec les $\overline{\pi_d}$ de la question a. (Une autre méthode d'obtenir ce morphisme est de commencer avec un morphisme $\mathbf{Z} \to (\mathbf{Z}/p_1^{k_1}\mathbf{Z}) \times \dots \times (\mathbf{Z}/p_r^{k_r}\mathbf{Z})$ donné par $x \mapsto (\pi_{p_1^{k_1}}(x), \dots, \pi_{p_r^{k_r}}(x))$, et de constater que son noyau est $n\mathbf{Z}$, d'où il passe au quotient $\mathbf{Z}/n\mathbf{Z}$.) Ce morphisme est injectif car son noyau est formé des classes modulo n des $x \in \mathbf{Z}$ qui sont divisible par tous les $p_i^{k_i}$, mais comme ceux-ci sont premiers entre eux deux à deux un tel x doit être divisible par n, et la seule classe de 0 (et de n) forme le noyau. Le morphisme est aussi surjectif car l'anneau $(\mathbf{Z}/p_1^{k_1}\mathbf{Z}) \times \dots \times (\mathbf{Z}/p_r^{k_r}\mathbf{Z})$ possède $p_1^{k_1} \dots p_r^{k_r} = n$ éléments, tout comme $\mathbf{Z}/n\mathbf{Z}$. Il s'agit donc d'un isomorphisme.

f. En déduire que l'image $\bar{x}$ dans $\mathbf{Z}/n\mathbf{Z}$ de $x \in \mathbf{Z}$ est nilpotent si et seulement si chaque p_i divise x (dans $\mathbf{Z}$). Comparer l'ensemble des éléments nilpotents de $\mathbf{Z}/n\mathbf{Z}$ et l'ensemble $\mathrm{Nilrad}(\mathbf{Z}/n\mathbf{Z})$.

$\surd$ *L'élément $\bar{x}$ est nilpotent si et seulement si son image dans $(\mathbf{Z}/p_1^{k_1}\mathbf{Z}) \times \dots \times (\mathbf{Z}/p_r^{k_r}\mathbf{Z})$ est nilpotent, ce qui est le cas si chaque p_i divise x (car alors $\pi_{p_i^{k_i}}(x)^{k_i} = \pi_{p_i^{k_i}}(x^{k_i}) = 0$ dans $\mathbf{Z}/p_i^{k_i}\mathbf{Z}$). En revanche si l'un des p_i ne divise pas x alors l'image de x dans $\mathbf{Z}/pZ$ est inversible, ainsi que toutes ses puissances; les puissances de $\bar{x}$ sont alors non-nulles dans $\mathbf{Z}/n\mathbf{Z}$ à cause du morphisme $\mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$. Ainsi l'ensemble des éléments nilpotents de $\mathbf{Z}/n\mathbf{Z}$ est précisément* $\mathrm{Nilrad}(\mathbf{Z}/n\mathbf{Z})$.

2. Soit K un corps commutatif. On rappelle que $K[X, X^{-1}]$ désigne l'anneau des polynômes de Laurent en X à coefficients dans K. Tout élément de $K[X, X^{-1}]$ peut être écrit sous la forme d'une somme $\sum_{i=-N}^{N} a_i X^i$ avec les $a_i \in K$, et N suffisamment grand (mais fini), et on a les définitions naturelles de l'addition et de la multiplication de telles expressions (notamment on a $X \cdot X^{-1} = X^0 = 1$). On considérera ici l'anneau $K[X]$ comme un sous-anneau de $K[X, X^{-1}]$ (pour $P \in K[X]$, son coefficient de X^i est nul pour tout $i < 0$).

a. Montrer que pour tout $L \in K[X, X^{-1}]$ non nul, il existe un unique $i \in \mathbf{Z}$ et $P \in K[X]$ avec coefficient constant non nul, tels que $L = X^i P$.

$\surd$ *Soit $k \in \mathbf{Z}$ minimal tel que le coefficient de X^k dans L soit non nul ; alors $X^{-k}L \in K[X]$, et il est de coefficient constant non nul. Réciproquement si $P \in K[X]$ est de coefficient constant non nul, alors i est minimal tel que le coefficient de X^i dans $X^i P$ est non nul, quel que soit i. Pour obtenir $L = X^i P$ il est donc nécessaire que $i = k$, et $P = X^{-k}L$, ce qui donne l'unique solution demandée.*

b. Dans cette situation montrer que L est inversible dans $K[X, X^{-1}]$ si et seulement si P est inversible dans $K[X]$. Décrire ensuite l'ensemble des éléments inversibles de $K[X, X^{-1}]$.

$\surd$ *Si $L = X^i P$ est inversible dans $K[X, X^{-1}]$ avec inverse $L^{-1} = X^j Q$, où $P, Q \in K[X]$ sont des polynômes à coefficient constant non nul, alors $1 = LL^{-1} = X^{i+j}PQ$. Mais comme PQ est un polynôme à coefficient constant non nul, cela nécessite $X^{i+j} = 1$ et donc $PQ = 1$; ainsi P est inversible dans $K[X]$. Réciproquement si P est inversible dans $K[X]$, il l'est aussi dans $K[X, X^{-1}]$, et tout $X^i P$, étant produit de deux inversibles dans $K[X, X^{-1}]$ sera inversible. Comme les seuls polynômes inversibles dans $K[X]$ sont les polynômes constants non nuls, les inversible de $K[X, X^{-1}]$ sont les éléments cX^i avec $c \in K^\times$ et $i \in \mathbf{Z}$.*

On propose maintenant de montrer que $K[X, X^{-1}]$ est un anneau principal (c'est-à-dire que tous ses idéaux sont des idéaux principaux). Soit donc J un idéal de $K[X, X^{-1}]$.

c. Expliquer pourquoi il existe un polynôme $P \in K[X]$ tel que $J \cap K[X]$ soit l'idéal principal (P) de $K[X]$ engendré par P.

$\surd$ *$J \cap K[X]$ est un idéal de $K[X]$ (cas d'une intersection d'un idéal et un sous-anneau; aussi c'est le noyau de la composée $K[X] \to K[X, X^{-1}] \to K[X, X^{-1}]/J$). Comme $K[X]$ est un anneau principal, il existe P tel que $(P) = J \cap K[X]$.*

d. Expliquer que $PK[X, X^{-1}]$, c'est-à-dire l'idéal principal de $K[X, X^{-1}]$ engendré par P, est inclus dans J.

$\surd$ *Par construction $P \in J \cap K[X] \subseteq J$, donc ses multiples dans $K[X, X^{-1}]$, les éléments de $PK[X, X^{-1}]$ sont aussi dans l'idéal J.*

e. Réciproquement, soit $Q \in J \subseteq K[X, X^{-1}]$. Montrer qu'il existe $k \in \mathbf{N}$ tel que $X^k Q \in J \cap K[X]$.

$\surd$ *En écrivant $Q = X^i Q'$ avec $Q' \in K[X]$ comme dans la question a, on a $Q' \in J \cap K[X]$. Il suffit donc de prendre $k = -i$, de sorte que $Q' = X^{-i}Q = X^k Q \in J \cap K[X]$.*

f. En déduire que $Q \in PK[X, X^{-1}]$, et conclure.

$\surd$ *Comme $Q' \in J \cap K[X] = (P)$, il existe un polynôme $S \in K[X]$ tel que $Q' = SP$, alors $Q = X^k Q' = X^K SP \in PK[X, X^{-1}]$. Ainsi on a montré $J \subseteq PK[X, X^{-1}]$, et donc (l'autre inclusion étant déjà établie) $J = PK[X, X^{-1}]$. Comme J était un idéal quelconque de $K[X, X^{-1}]$, on a montré que tout tel idéal est de la forme $PK[X, X^{-1}]$, ou en fait on peut prendre $P \in K[X]$.*

Fin.