Corrigé Examen Arithmétique et algèbre commutative jeudi 29 juin 2017
9h00–12h00

1. *Question de cours.* Soit A un anneau commutatif, et I un idéal de A.

a. Décrire une correspondance entre les idéaux de l'anneau quotient A/I et certains idéaux de A.

b. Montrer que si I est un idéal maximal, alors I est un idéal premier.

2. *a.* Résoudre pour $x \in \mathbf{Z}$ la congruence $19x \equiv 28 \pmod{45}$.

$\surd$ $x \equiv 37 \pmod{45}$

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

$$\begin{cases} x \equiv 2 \pmod{25} \\ x \equiv 13 \pmod{28} \end{cases}.$$

$\surd$ $x \equiv 377 \pmod{700}$

3. Dans l'anneau $\mathbf{R}[X]$, soient $P = X^3 + 2$ et $Q = X - 1$.

a. Montrer que l'anneau quotient $\mathbf{R}[X]/(PQ)$ n'est pas un anneau intègre.

$\surd$ *Dans l'anneau quotient les classes de P et de Q ne sont pas nulles, mais leur produit, la classe de PQ, est nulle. L'anneau quotient admet donc des diviseurs de zéro, et n'est pas une anneau intègre.*

b. Montrer que P et Q sont premiers entre eux dans $\mathbf{R}[X]$.

$\surd$ *Comme Q est de degré 1 et donc irréductible, la condition que P et Q soient premiers entre eux est équivalente à celle que Q ne divise pas P ; or le reste de la division euclidienne de P par Q est $P[X := 1] = 3 \neq 0$, donc P ne divise effectivement pas Q.*

c. Trouver (des coefficients de Bézout) $S, T \in \mathbf{R}[X]$ tels que $1 = SP + TQ$, ainsi que $\deg S < 1$ et $\deg T < 3$ (ces deux dernières conditions sont données uniquement pour vous indiquer à quoi ressembleront S, T; elles seront automatiquement vérifiées si vous trouvez S, T par la bonne méthode).

$\surd$ *L'algorithme d'Euclide commence avec la division euclidienne de P par Q qu'on a déjà fait, avec reste 3 qui est inversible, donc la division suivante sera exacte et n'a pas besoin d'être fait. On aura $\operatorname{pgcd}(P, Q) = 1 = \frac{1}{3} \times 3$. Pour avoir les coefficients de Bézout, il faut connaître aussi le quotient dans la division euclidienne de P par Q ; c'est $X^2 + X + 1$. Ainsi $1 = \frac{1}{3} \times (P - (X^2 + X + 1)Q)$ donc les coefficients de Bézout sont $S = \frac{1}{3}$ et $T = \frac{1}{3}(-X^2 - X - 1)$.*

d. Soient $f : \mathbf{R}[X] :\to \mathbf{R}[X]/(P)$ et $g : \mathbf{P}[X] \to \mathbf{R}[X]/(Q)$ les projections canoniques. Trouver un polynôme $C \in \mathbf{R}[X]$ tel qu'on ait à la fois $f(C) = 0 \in \mathbf{R}[X]/(P)$ et $g(C) = 1 \in \mathbf{R}[X]/(Q)$.

$\surd$ *Les conditions s'écrivent $C \equiv 0 \pmod{P}$ et $C \equiv 1 \pmod{Q}$. La relation de Bézout qu'on a trouvée montre que $C = SP = \frac{1}{3}(X^3 + 2)$ vérifie ce système de congruences.*

4. Soit $A[X]$ l'anneau de polynômes en X à coefficients dans un anneau commutatif A.

a. Montrer que pour tout $n \in \mathbf{N}$, le polynôme $X^n - 1 \in A[X]$ s'écrit comme un multiple $(X-1)Q$ de $X - 1$, en détaillant le polynôme $Q \in A[X]$ (autrement dit le quotient $(X^n - 1)/(X - 1)$).

$\surd$ $Q = X^{n-1} + X^{n-2} + \cdots + X + 1$ *convient.*

b. Montrer que pour tout $a \in A$, l'élément $a^n - 1$ est un multiple dans A de $a - 1$.

$\surd$ *En appliquant le morphisme $A[X] \to A$ donné par $P \mapsto P[a]$ (évaluation en $X = a$), la relation $X^n - 1 = (X-1)(X^{n-1} + X^{n-2} + \cdots + X + 1)$ on obtient $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$.*

Soit maintenant $a \in A$ un élément *nilpotent*, c'est-à-dire il existe $k \in \mathbf{N}$ tel que $a^k = 0$.

c. Déduire de la question précédente que $a - 1$ est inversible dans A.

$\surd$ *En fixant $k \in \mathbf{N}_{>0}$ tel que $a^k = 0$ on a $1 = -(a^k - 1) = -(a-1)(a^{k-1} + a^{k-2} + \cdots + a + 1)$, donc $a - 1$ est inversible.*

d. Soit $\mathfrak{p}$ un idéal premier de $A[X]$. Montrer que $\mathfrak{p} \cap A$ est un idéal premier de A.

$\surd$ *Comme $\mathfrak{p}$ est un idéal premier de $A[X]$, l'anneau quotient $A[X]/\mathfrak{p}$ est un anneau intègre. Le noyau du morphisme composé $A \hookrightarrow A[X] \to A[X]/\mathfrak{p}$ (la seconde étape étant la projection canonique) est donc un idéal premier de A, et c'est l'image réciproque par la première étape du noyau $\mathfrak{p}$ de la second étape ; puisque la première étape est une inclusion d'anneaux, cette image réciproque est $\mathfrak{p} \cap A$. (Bien sûr, l'application directe de la définition d'un idéal premier marche aussi.)*

e. Montrer que $a \in \mathfrak{p} \cap A$.

$\surd$ *Puisque $a^k = 0 \in \mathfrak{p} \cap A$ pour un certain k, et $\mathfrak{p} \cap A$ est un idéal premier, l'un au moins des k facteurs a est déjà dans $\mathfrak{p} \cap A$ (et évidemment ces facteurs sont identiques, donc dès qu'un facteur est dans l'idéal, ils le sont tous), et c'est ce qu'on cherchait à montrer.*

5. Soit $p \in \mathbf{N}$ un nombre premier impair (donc $p \neq 2$), et $K = \mathbf{Z}/p\mathbf{Z}$, l'anneau (fini) des entiers modulo p, qui est en fait un corps. Dans $K[X]$ on peut décomposer $X^4 - 1 = (X^2 - 1)(X^2 + 1) = (X - 1)(X + 1)(X^2 + 1)$ (c'est vrai dans n'importe quel anneau de polynômes) ; notre première considération sera si ce dernier facteur $X^2 + 1$ est réductible (se décompose encore en un produit de facteurs de degré 1) ou non dans $K[X]$.

a. Montrer que $X^2 + 1$ est réductible si et seulement si il existe $a \in \mathbf{Z}$ tels que $a^2 + 1 \equiv 0 \pmod{p}$.

b. Montrer que $a \in \mathbf{Z}$ vérifie $a^2 + 1 \equiv 0 \pmod{p}$ si et seulement si sa classe $\bar{a} \in \mathbf{Z}/p\mathbf{Z}$ est d'ordre multiplicatif 4 dans le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$, autrement dit $(\bar{a})^4 = \bar{1}$ mais $(\bar{a})^2 \neq \bar{1}$ dans $\mathbf{Z}/p\mathbf{Z}$.

c. En utilisant le résultat du cours que $(\mathbf{Z}/p\mathbf{Z})^\times$ est un groupe *cyclique*, montrer que $X^2 + 1$ est réductible dans $K[X]$ si et seulement si $p - 1$ est divisible par 4 (autrement dit $p \equiv 1 \pmod{4}$).

On suppose désormais que $p \equiv 1 \pmod{4}$, et que $a \in \mathbf{Z}$ vérifie $a^2 + 1 \equiv 0 \pmod{p}$. Soit $R = \mathbf{Z}[\mathbf{i}]$ l'anneau des entiers de Gauss, dont on sait (admet) que c'est un anneau euclidien. Dans R on peut décomposer $a^2+1 = (a+\mathbf{i})(a-\mathbf{i})$. On pose $d = \operatorname{pgcd}(a+\mathbf{i}, p) \in R$, le pgcd dans le sens de l'anneau R.

d. Montrer que d est un diviseur strict (donc ni inversible, ni associé à p lui même) de p dans R. En particulier p, vu comme élément de $R = \mathbf{Z}[\mathbf{i}]$, est réductible (pendant qu'il est premier dans $\mathbf{Z}$).

Fin.