Examen Arithmétique et algèbre commutative vendredi 3 mai 2013
9h00–12h00

Un polycopié/résumé du cours est (seul) autorisé comme document.

1. Dans cette partie on cherche à trouver tous les nombres naturels n à trois chiffres décimaux (où on admet la possibilité d'avoir le chiffre '0' comme premier chiffre) tel que les trois derniers chiffres de n^2 sont ceux du nombre n lui-même (dans l'ordre).

a. Justifier que les solutions de ce problème correspondent aux solutions de l'équation $x^2 = x$ pour x dans l'anneau $\mathbf{Z}/1000\mathbf{Z}$.

b. Comment le théorème chinois permet-il de trouver ces solutions si l'on suppose connues les solutions de la même équation $x^2 = x$ mais avec x pris dans l'anneau $\mathbf{Z}/8\mathbf{Z}$ et également celles pour l'équation avec x pris dans l'anneau $\mathbf{Z}/125\mathbf{Z}$, ? Si ces deux problèmes possèdent respectivement k et l solutions, combien de solutions aura le problème avec $x \in \mathbf{Z}/1000\mathbf{Z}$?

c. Trouver des coefficients de Bezout s, t tels que $\mathrm{pgcd}(8, 125) = 1 = 8s + 125t$.

d. Trouver les solutions de $x^2 = x$ avec $x \in \mathbf{Z}/8\mathbf{Z}$.

e. Argumenter que pour que la classe $x = m_{125} \in \mathbf{Z}/125\mathbf{Z}$ d'un entier m modulo 125 soit une solution de $x^2 = x$, il est nécessaire que la classe $x' = m_{25} \in \mathbf{Z}/25\mathbf{Z}$ du même nombre modulo 25 soit une solution de $(x')^2 = x'$, et que pour cela il est nécessaire que la classe $x'' = m_5 \in \mathbf{Z}/5\mathbf{Z}$ de m modulo 5 soit une solution de $(x'')^2 = x''$.

f. Utiliser cela pour trouver successivement toutes les solutions de $x^2 = x$ pour $x \in \mathbf{Z}/5\mathbf{Z}$, ensuite celles pour $x \in \mathbf{Z}/25\mathbf{Z}$, et finalement celles pour $x \in \mathbf{Z}/125\mathbf{Z}$.

g. Conclure en donnant tous les nombres n vérifiant la condition de l'introduction de cette partie.

2. Soit R un anneau commutatif, et $a \in R$.

a. Montrer que si a est nilpotent (c'est-à-dire $a^n = 0$ pour un certain $n \in \mathbf{N}$) et $\mathfrak{p} \subseteq R$ est un idéal premier, alors $a \in \mathfrak{p}$.

b. On rappelle que l'anneau des séries formelles $R[[X]]$ contient des expressions formelles $\sum_{i=0}^{\infty} c_i X^i$ sans condition sur suite des coefficients $c_i \in R$, avec les opérations définies comme dans $R[X]$. Vérifier que pour $a \in R$ quelconque, la série formelle $1 - aX$ (dont les coefficients de X^i pour $i > 1$ sont tous nuls) possède dans $R[[X]]$ un inverse, à savoir la série géométrique $\sum_{i=0}^{\infty} a^i X^i$.

c. On suppose maintenant que $a \in R$ n'est pas nilpotent. Montrer que $1 - aX$ n'est pas inversible dans $R[X]$ (bien qu'il soit inversible dans $R[[X]]$). [Utiliser que l'inverse d'un élément est unique.]

d. Dans cette situation, indiquer un idéal propre $I \subseteq R[X]$ tel que $1 - aX \in I$.

On admet qu'il existe dans $R[X]$ un idéal maximal qui contient cet idéal I (le théorème de Krull affirme cela pour tout idéal propre); on désigne par $\mathfrak{m}$ un tel idéal maximal de $R[X]$.

e. Expliquer que $a \notin \mathfrak{m}$ pour le polynôme constant $a \in R \subseteq R[X]$.

f. En déduire (toujours sous l'hypothèse que $a \in R$ n'est pas nilpotent) que l'anneau R contient un idéal premier $\mathfrak{p}$ avec $a \notin \mathfrak{p}$. (Attention qu'ici on *ne parle plus* de l'anneau $R[X]$.)

3. Soit p un nombre premier avec $p \neq 2$. On pose $K = \mathbf{Z}/p\mathbf{Z}$, un corps fini à p éléments.

a. Pour $a \in K^\times$, montrer que a est racine du polynôme $X^2 + 1 \in K[X]$ si et seulement si l'ordre multiplicatif de a est 4 (c'est-à-dire $a^4 = 1$ pendant que $a^m \neq 1$ pour $0 < m < 4$).

b. Combien d'éléments possède l'anneau $R = K[X]/(X^2 + 1)$?

c. Soit $A = \mathbf{Z}[i] \cong \mathbf{Z}[X]/(X^2 + 1)$ l'anneau des entiers de Gauss. Montrer que $R \cong A/pA$.

d. Montrer que si $p \equiv 3 \pmod 4$, alors $X^2 + 1 \in K[X]$ est un polynôme irréductible.

e. Montrer que si $p \equiv 1 \pmod 4$, alors il existe $u \in K$ tel que $X^2 + 1 = (X - u)(X + u)$ dans $K[X]$.

f. Montrer que R est un corps si et seulement si $p \equiv 3 \pmod 4$.

g. Dans le cas de la question *e*, c'est-à-dire $p \equiv 1 \pmod 4$, appliquer le théorème chinois (théorème 2.1.8 du cours, mais avec $K[X]$ à la place de $\mathbf{Z}$) pour déduire que R est isomorphe à $K \times K$.

h. Ce qui précède montre que dans le cas $p \equiv 1 \pmod 4$ il existe un isomorphisme $A/pA \xrightarrow{\sim} K \times K$. Décrire explicitement cet isomorphisme (en termes de $u \in \mathbf{Z}/p\mathbf{Z}$ de la question *e*).

Fin.