**Examen Anneaux et Arithmétique - Corrigé**
**L3, Module E04, semestre 2 (2005-2006)**

**Exercice 1.** Soient

$$P = 3X^2 + 4X + 1,$$

$$Q = 3X^2 + X + 1,$$

deux éléments de $K[X]$, où $K$ est un corps. Dire si la classe de $P$ est inversible dans $K[X]/(Q)$, et si oui précisez son inverse, dans les cas suivants :
a)$K = \mathbb{Q}$.
b)$K = \mathbb{Z}/3\mathbb{Z}$.
c)$K = \mathbb{Z}/7\mathbb{Z}$.

**Réponse :** :
a) Utilisions l'algorithme d'Euclide :

$$P = Q + 3X,$$

et

$$Q = 3X(X + 1/3) + 1,$$

et on obtient donc

$$(X + 4/3)Q + P(-X - 1/3) = 1.$$

Modulo $Q$, on a ainsi :

$$P(-X - 1/3) = 1\,[Q],$$

donc l'inverse de $P$ est $-X - 1/3$, et en particulier $P$ est inversible.
b) $P = Q + 3X = Q$ car $3 = 0$, donc

$$P = 0\,[Q],$$

et n'est donc pas inversible.
c) Les calculs suivants ont lieu dans $\mathbb{Z}/7\mathbb{Z}$. On pourrait appliquer l'algorithme d'Euclide comme en a), mais en gardant à l'esprit que dans $\mathbb{Z}/7\mathbb{Z}$, l'inverse de 3 est 5, pour obtenir l'équation

$$(X + 6)Q + (-X + 2)P = 1,$$

et en conclure que l'inverse de $P$ est $2 - X$. On peut aussi faire la manière suivante (la question a) peut se résoudre de même) : tout élément de $\mathbb{Z}/7\mathbb{Z}[X]/(Q)$ a un

unique représentant de degré $< 2$, $aX + b$ avec $a, b \in \mathbb{Z}/7\mathbb{Z}$. On cherche donc $a, b$ tels que

$$P(aX + b) = 1\,[Q],$$

c'est à dire

$$3X(aX + b) = 1\,[Q],$$

donc $Q$ divise $3aX^2 + 3bX - 1$, il existe un polynôme $\lambda$ tel que

$$3aX^2 + 3bX - 1 = \lambda(3X^2 + X + 1),$$

donc lambda est de degré 0 nécessairement (une constante) et l'identification des termes de même degré donne :

$$3a = 3\lambda,\ 3b = \lambda,\ -1 = \lambda,$$

ce qui donne $a = -1, 3b = -1 = 6$ donc $a = -1$ et $b = 2$. L'inverse de $P$ est donc $-X + 2$.

**Exercice 2.** Résoudre l'équation d'inconnue $X$ :

$$X^3 = 2$$

dans les anneaux suivants :
a) $\mathbb{Z}/5\mathbb{Z}$,
b) $\mathbb{Z}/35\mathbb{Z}$,
c) $\mathbb{Z}/25\mathbb{Z}$,
d) $\mathbb{Z}/125\mathbb{Z}$.

**Réponse :** :
a) On élève au cube les nombres $0, 1, 2, 3, 4$ modulo 5 (qui énumèrent toutes les classes modulo 5) et on obtient $0, 1, 3, 2, 4$. L'unique solution est donc $X = 3$.
b) Par le théorème chinois, une solution dans $\mathbb{Z}/35\mathbb{Z}$ correspond à un couple de solution dans $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$ respectivement. Cherchons les solutions modulo 7 : les cubes de $0, 1, 2, 3, 4, 5, 6$ sont $0, 1, 1, 6, 1, 6, 6$ (astuce : pour simplifier les calculs, remarquer que $(-x)^3 = -x^3$, il est donc ainsi inutile de calculer $6^3$ car c'est $(-1)^3 = -1 = 6\,[7]$, de même pour $4^3$ et $5^3$). L'équation $X^3 = 2$ n'a donc pas de solution modulo 7 donc pas de solution modulo 35.
c) Comme 2 et l'exposant 3 sont tous deux premier à 25, le résultat de cours s'applique et on sait que toute solution modulo 5 se relève en une unique solution modulo 25. Comme il n'y a que la solution $X = 3$ modulo 5, cherchons l'unique solution modulo 25 , qui est alors congrue à 3 modulo 5 :

$$X = 3 + 5k\,[25],$$

$$X^3 = 27 + 3 * 9 * 5k + 3 * 3 * 5^2 * k^2 + 5^3 k^3 \, [25],$$

ou encore , en remplaceant $X^3$ par 2 et en utilisant $27 = 2$ ainsi que $25 = 0$,

$$2 = 2 + 10k + 0 + 0 \, [25].$$

donc $10k = 0$ donc $5k = 0$ car 2 est inversible. On en conlut que $X = 3 + 0 = 3$ est solution modulo 25 (ce qu'on pouvait voir directement en calculant $3^3 = 27 = 2$ modulo 25).
c) De même on cherche $X$ sous la forme

$$X = 3 + 25k \, [125],$$

et en élevant au cube

$$X^3 = 27 + 3 * 9 * 25k \, [125],$$

Comme $X^3 = 2$ on a

$$-25 = 27 * 25k \, [125],$$

d'où, comme $27 * 25k = 2 * 25k$,

$$25k = (-3) * 25 = 2 * 25,$$

donc finalement la solution est $X = 53$.
(Surtout, ne jamais simplifier par 25, car 25 n'est pas inversible dans $\mathbb{Z}/125\mathbb{Z}$.)
**Exercice 3.**
Montrez que l'anneau quotient

$$\mathbb{Z}[X, Y]/(X^3 + X^2Y^2 + XY^3 + Y),$$

est un anneau intègre.

**Réponse :** :
Soit $P = X^3 + X^2Y^2 + XY^3 + Y$. Comme $\mathbb{Z}[X, Y]$ est factoriel, les irréductibles sont premiers donc si $P$ est irréductible, alors $(P)$ est un idéal premier et $\mathbb{Z}[X, Y]/(P)$ est intègre. Il est donc suffisant de montrer que $P$ est irréductible. Pour cela on va appliquer le critère d'Eisenstein à l'anneau factoriel $\mathbb{Z}[Y]$ et à $P$ vu comme au polynôme de la variable $X$, et à l'irréductible $Y$ de $\mathbb{Z}[Y]$. En effet, en la variable $X$, $P$ est unitaire donc primitif, ses coefficients non dominants sont divisibles par $Y$ et le dernier coefficient n'est pas divisible par $Y^2$. Il est donc irréductible dans $\mathbb{Z}[Y][X] = \mathbb{Z}[X, Y]$, ce qu'il fallait démontrer.

**Problème.**
Soit $A_{\mathbb{C}}$ l'ensemble des polynômes trigonométriques complexes, c'est à dire des fonctions $f$ de $\mathbb{R}$ dans $\mathbb{C}$ qui admettent une écriture

$$f(x) = \sum_{n=-k}^{k} a_n e^{inx},$$

pour un certain entier $k$ et des nombres complexes $a_n$. On notera que, les nombres $a_n$ étant les coefficients de Fourier de $f$, ils sont bien définis de manière unique par $f$ pour tout $n$. Définissons $A_{\mathbb{R}}$ comme le sous-ensemble des polynômes trigonométriques réels, c'est à dire de telles fonctions à valeurs réelles.
1) Montrez que $A_{\mathbb{C}}$ et $A_{\mathbb{R}}$, munis de l'addition et la multiplication ponctuelle, sont des anneaux.
**Réponse :**
Montrons que $A_{\mathbb{C}}$ est un sous-anneau de l'anneau des fonctions de $\mathbb{R}$ dans $\mathbb{C}$.
i)La différence de deux combinaisons linéaires d'exponentielles $e^{inx}$ est encore une combinaison linéaire d'exponentielles.
ii) Le produit de deux telles combinaisons linéaires est encore de la même forme :

$$\left(\sum_{|k|\leq N} a_k e^{ikx}\right)\left(\sum_{|k|\leq N} b_k e^{ikx}\right) = \sum_{|n|\leq 2N}\left(\sum_{k=-N}^{N} a_k b_{n-k}\right) e^{inx}.$$

iii) La fonction constante égale à 1 est bien de cette forme :

$$1 = 1.e^{i0x}.$$

Montrons que $A_{\mathbb{R}}$ est un sous-anneau de l'anneau $A_{\mathbb{C}}$.
i) La différence de deux fonctions à valeurs réelles est encore à valeurs réelles.
ii) Le produit de deux fonctions à valeurs réelles est encore à valeurs réelles.
iii) La fonction constante égale à 1 est bien à valeurs réelles.
*Remarque :* en dépit du nom ambigu "polynômes trigonométriques", il était faux de dire que c'était des polynômes, par exemple la fonction $x \mapsto e^{ix}$ n'étant bien évidemment pas polynomiale.

2) Montrez que $f \in A_{\mathbb{R}}$ si et seulement si pour tout $n$, on a $a_{-n} = \overline{a_n}$.
**Réponse :**
Soit

$$f(x) = \sum_{n=-N}^{N} a_n e^{inx}.$$

Alors pour tout $x$, on a $f(x) = \overline{f(x)}$ si et seulement si

$$\sum_{n=-N}^{N} a_n e^{inx} = \sum_{n=-N}^{N} \overline{a_n} e^{-inx},$$

et en changeant les indices dans le membre de droite (en posant $k = -n$), c'est équivalent à

$$\sum_{n=-N}^{N} a_n e^{inx} = \sum_{k=-N}^{N} \overline{a_{-k}} e^{ikx}.$$

Ces deux fonctions ont donc même coefficients de Fourier, par l'unicité (rappelée dans l'énoncé), on obtient que $a_n = \overline{a_{-n}}$. Réciproquement si cette dernière égalité est vérifiée, la dernière équation est vraie et elle est équivalente au fait que $f$ soit à valeurs réelles.

3) On défini le degré $d(f)$ du polynôme trigonométrique $f \in A_{\mathbb{C}} - \{0\}$ comme le plus grand entier $m$ tel que ($a_m \neq 0$ ou $a_{-m} \neq 0$). Montrez que si $f, g \in A_{\mathbb{R}}$ sont tous deux non nuls, on a

$$d(fg) = d(f) + d(g).$$

Cette égalité est-elle encore vérifiée en général dans $A_{\mathbb{C}}$ ?

**Réponse :**

Soient $f, g \in A_{\mathbb{R}}$. Ecrivons

$$f(x) = \sum_{n=-d(f)}^{d(f)} a_n e^{inx},\ g(x) = \sum_{n=-d(g)}^{d(g)} b_n e^{inx}.$$

Alors

$$f(x)g(x) = \sum_{|n|\leq d(f), |m|\leq d(g)} a_n b_m e^{i(n+m)x},$$

et ainsi

$$f(x)g(x) = \sum_{k} \left( \sum_{n+m=k} a_n b_m \right) e^{ikx}.$$

Si $|k| > d(f)+d(g)$ est la somme de deux entiers $n, m$, alors $|n| > d(f)$ ou $|m| > d(g)$ donc dans tous les cas $a_n b_m = 0$, d'où si $|k| > d(f)+d(g)$ alors $\sum_{n+m=k} a_n b_m = 0$. Pour $k = d(f) + d(g)$, si $k = n + m$ alors $n > d(f)$ ou $m > d(g)$ à moins que $n = d(f)$ et $m = d(g)$. Ainsi

$$\sum_{n+m=k} a_n b_m = a_{d(f)} b_{d(g)},$$

produit de deux nombres, dont nous allons prouver qu'ils sont tous deux non nuls. Par définition du degré, $a_{d(f)}$ ou $a_{-d(f)}$ est non nuls. Comme ces deux nombres sont conjugués car $f$ est réelle (question 2)), ils sont en fait tous les deux non nuls. De même $b_{d(g)}$ est non nul. Donc le coefficient $d(g)+d(f)$ est non nuls et ceux de plus grand degré le sont, le degré de $fg$ est donc la somme des degrés de $f$ et $g$.
C'est faux dans $A_{\mathbb{C}}$ car $e^{ix}e^{-ix}=1$, or les deux termes de gauche sont de degré 1 et celui de droite de degré 0.

4) Déterminez l'ensemble des inversibles de l'anneau $A_{\mathbb{R}}$.

**Réponse :**

Si $fg=1$ alors $d(f)+d(g)=d(1)=0$ donc $d(f)=d(g)=0$. Les inversibles sont donc de degré nul, c'est à dire des constantes non nullles ; Réciproquement, toute constante non nulle est inversible. Les inversibles sont donc les fonctions constantes non nulles.

5) Montrez que les trois fonctions suivantes sont dans $A_{\mathbb{R}}$ et sont irréductibles dans cet anneau : $sin(x), 1+cos(x), 1-cos(x)$.

**Réponse :**

On a

$$sin(x) = (e^{ix}-e^{-ix})/(2i),$$
$$1+cox(x) = e^{-ix}/2+1+e^{ix}/2,$$
$$1-cox(x) = -e^{-ix}/2+1-e^{ix}/2,$$

Donc $sin, 1-cos, 1+cos$ sont bien dans $A_{\mathbb{C}}$, et sont clairement à valeurs réelles, donc dans $A_{\mathbb{R}}$.
Supposons $fg=sin$ , alors $d(f)+d(g)=d(sin)=1$ donc $d(f)$ ou $d(g)$ doit être nul, donc une constante non nulle, c'est à dire un inversible par la question précédente. Donc $sin$ est irréductible. De même, $1+cos$ et $1-cos$ sont de degré 1 et le même raisonnement s'applique.

6) Montrez, en considérant l'égalité

$$sin^2(x) = (1-cos(x))(1+cos(x)),$$

que $A_{\mathbb{R}}$ n'est pas factoriel.

**Réponse :**

Montrons que la décomposition en irréductible de $sin^2$ n'est pas unique, à permutation, et à association près des termes. Nous devons donc vérifier que $1+cos(x)$n'est

pas associé à $sin(x)$. Sinon il existerait un inversible $\lambda$ tel que

$$sin(x) = \lambda(1 + cos(x)).$$

Cet inversible est une constante , par la question 4), et donc pour $x = 0$ on obtient $0 = \lambda * 2$ donc $\lambda = 0$ donc $sin(x) = 0$ pour tout $x$, contradiction. Donc $sin(x)$ et $1+cos(x)$ ne sont pas associé et ainsi $sin(x)*sin(x)$ et $(1-cos(x))(1+cos(x))$ sont deux décomposition non équivalente en produit d'irréductibles du même élément, et donc $A_{\mathbb{R}}$ n'est pas factoriel.