UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 2

Corrigé rapide du contrôle continu du 10 mars 2017

Questions de cours

1) Le théorème de Bezout s'énonce ainsi : Deux polynômes A et B de $\mathbb{K}[X]$ sont premiers entre eux **si et seulement s'il** existe des polynômes U et V dans $\mathbb{K}[X]$ tels que $AU + BV = 1$.

2) Puisque A et B sont premiers entre eux, on peut considérer deux polynômes U et V tels que $AU+BV = 1$ donc $ACU + BCV = C$. Or $A|ACU$ et $A|BC$ donc $A|BCV$. Par suite $A|ACU + BCV = C$.

3) Soit A un polynôme de degré 1 de $\mathbb{K}[X]$. Il s'agit de montrer que A a exactement deux diviseurs unitaires. Soit donc B un tel diviseur. On peut alors écrire $A = B.A_1$ et on en déduit $1 = \deg(A) = \deg(B)+\deg(A_1)$ et donc :
- ou bien $\deg(B) = 0$ et alors $B = 1$,
- ou bien $\deg(B) = 1$ et alors $\deg(A_1) = 0$. A_1 est alors une constante non nulle c et $B = \frac{1}{c}A$.

Exercice n°1

Si un tel polynôme B existe, il est nécessairement de degré 2. Quitte à considérer $-B$ (qui est alors solution), on peut même le supposer de coefficient dominant positif donc de la forme $B = 2X^2 + \alpha X + \beta$. Réciproquement, si B est de cette forme alors $B^2 = 4X^4 + 4\alpha X^3 + (\alpha^2 + 4\beta)X^2 + 2\alpha\beta X + \beta^2$ et donc $A = B^2$ si et seulement si

$$\begin{cases} a &= 4\alpha \\ -11 &= \alpha^2 + 4\beta \\ b &= 2\alpha\beta \\ 9 &= \beta^2 \end{cases} \quad \text{ou encore} \quad \begin{cases} \beta &= -3 \\ \alpha &= 1 \\ b &= -6 \\ a &= 4 \end{cases} \quad \text{ou} \quad \begin{cases} \beta &= -3 \\ \alpha &= -1 \\ b &= 6 \\ a &= -4 \end{cases}.$$

(Le cas $\beta = 3$ conduit à $\alpha^2 = -23$ qui est impossible dans $\mathbb{R}$.)

Il y a donc finalement deux couples (a, b) solutions : $(4, -6)$ et $(-4, 6)$.

Exercice n°2

1) a) D'après les propriétés du degré, $\deg(A(X^2)) = 2\deg(A)$ et $\deg((X^3+1)A(X)) = \deg((X^3+1))+\deg(A)$ et on a donc $2\deg(A) = 3 + \deg(A)$ soit $\deg(A) = 3$.

b) En évaluant l'égalité polynomiale en 1, on obtient $A(1^2) = (1^3+1)A(1)$ donc $A(1) = 2A(1)$ et $A(1) = 0$. D'autre part, on obtient par dérivation $2XA'(X^2) = 3X^2A(X) + (X^3 + 1)A'(X)$ et, en dérivant à nouveau, $2A'(X^2) + 4X^2A''(X^2) = 6XA(X) + 6X^2A'(X) + (X^3 + 1)A''(X)$.
En évaluant en 0, on en déduit $0 = A'(0)$ et $2A'(0) = A''(0)$ soit $A''(0) = 0$.

c) Puisque A est de degré 3 (question a)), la formule de Taylor pour A en 0 s'écrit

$$A = \sum_{k=0}^{3} \frac{A^{(k)}(0)}{k!}X^k = A(0) + A'(0)X + \frac{A''(0)}{2}X^2 + \frac{A^{(3)}(0)}{6}X^3$$

donc, compte tenu de la question précédente, $A(X) = A(0) + \dfrac{A^{(3)}(0)}{6}X^3$. En notant $a = \text{coefdom}(A)$, on a $a \neq 0$ et $A^{(3)} = 6a$ (car A est de degré 3). La dernière égalité s'écrit donc $A(X) = A(0) + aX^3$ et comme $A(1) = 0$, $A(0) = -a$ et $A(X) = a(X^3 - 1)$.

2) Le polynôme nul est clairement solution et la question précédente montre que toute autre solution est nécessairement de la forme $a(X^3-1)$ ($a \in \mathbb{R}^*$). Réciproquement, si $A = a(X^3-1)$ alors $A(X^2) = a(X^6-1)$ et $(X^3+1)A(X) = (X^3+1)a(X^3-1) = a(X^6-1)$. On a donc bien $A(X^2) = (X^3+1)A(X)$. En conclusion, l'ensemble des polynômes A de $\mathbb{R}[X]$ tels que $A(X^2) = (X^3+1)A(X)$ est exactement $\{a(X^3-1),\, a \in \mathbb{R}\}$.

Exercice n°3

1) On pose la division :

$$\begin{array}{rrll|l}
2X^4 & +2X^3+3X^2+X+1 & & & X^3-1 \\
\cline{5-5}
2X^4 & -2X & & & 2X+2 \\
\cline{1-2}
 & 2X^3+3X^2+3X+1 & & & \\
 & 2X^3 \quad - \quad 2 & & & \\
\cline{2-2}
 & 3X^2+3X+3 & & &
\end{array}$$

La division euclidienne de A par B s'écrit donc $A = B.(2X + 2) + (3X^2 + 3X + 3)$.

2) On poursuit alors les divisions euclidiennes (algorithme de Euclide) et on obtient

$$B = (3X^2 + 3X + 3)(\frac{1}{3}X - \frac{1}{3}) + 0$$

Dans cet algorithme le dernier reste non nul $(3X^2 + 3X + 3)$ est un *pgcd* de A et B. En particulier $\text{pgcd}(A, B) = X^2 + X + 1$.
On obtient un couple de coefficients de Bezout en remontant l'algorithme précédent. On obtient ici immédiatement $3X^2 + 3X + 3 = A - B.(2X + 2)$ et on peut donc choisir $U_0 = \dfrac{1}{3}$ et $V_0 = -\dfrac{1}{3}(2X + 2)$.

3) La question 2) montre que A et B sont divisibles par $X^2 + X + 1$. Les divisions euclidiennes donnent $A = (X^2 + X + 1)(2X^2 + 1) = 2(X^2 + X + 1)(X^2 + \frac{1}{2})$ et $B = (X^2 + X + 1)(X - 1)$. Ce sont les décompositions en facteurs irréductibles cherchées car :

- $X - 1$ est irréductible (c'est un polynôme de degré 1) et unitaire,
- $X^2 + X + 1$ et $X^2 + \frac{1}{2}$ sont irréductibles dans $\mathbb{R}[X]$ (comme polynômes de degré deux à discriminants strictement négatifs) et unitaires.

4) On sait que $\dfrac{1}{\text{coefdom}(AB)}(AB) = \text{pgcd}(A, B)\text{ppcm}(A, B)$ et un *ppcm* de A et B est donc

$$(X^2 + X + 1)(X - 1)(2X^2 + 1) = 2X^5 + X^3 - 2X^2 - 1.$$

5) On pose $A_0 = 2X^2 + 1$ et $B_0 = X - 1$. Après simplification par D, l'équation $AU + BV = D$ s'écrit $A_0U + B_0V = 1$ et (U_0, V_0) en est une solution. Si (U, V) est un autre couple solution alors $A_0U + B_0V = 1 = A_0U_0 + B_0V_0$ donc $A_0(U_0 - U) = B_0.(V - V_0)$. A_0 divise donc $B_0.(V - V_0)$. Or, A_0 est premier avec B_0 (car $D = \text{pgcd}(A, B) = \text{pgcd}(A_0D, B_0D) = D\text{pgcd}(A_0, B_0)$) donc (lemme de Gauss) A_0 divise $V - V_0$.
On peut alors écrire $V - V_0 = A_0Q$ pour un certain polynôme Q et donc, en reportant dans la dernière égalité écrite, $A_0(U_0 - U) = B_0.A_0Q$. Comme $A_0 \neq 0$, on a $U_0 - U = B_0Q$ soit $U = U_0 - B_0Q$.
Réciproquement, pour tout polynôme Q, $A_0.(U_0 - B_0Q) + B_0.(V_0 + A_0Q) = A_0.U_0 + B_0.V_0 = 1$.
En conclusion, l'ensemble des couples (U, V) cherchés est $\{(U_0 - B_0Q, V_0 + A_0Q),\ Q \in \mathbb{R}[X]\}$.