MHT201 année 2010-2011

DM N° 1

Exercice 1. Soient $(A, B, R_1, R_2) \in (\mathbb{R}[X])^4$ quatre polynômes, tels que le degré de R_1 est strictement inférieur au degré de A, et que le degré de R_2 est strictement inférieur au degré de B.

1. Prouver qu'il existe $P \in \mathbb{R}[X]$ tel que le reste de la division euclidienne de P par A soit R_1 et que le reste de la division euclidienne de P par B soit R_2, si et seulement si le PGCD de A et de B divise $R_1 - R_2$.
2. Trouver un polynôme de degré aussi petit que possible dont le reste de la division par $X^4 - 2X^3 - 2X^2 + 10X - 7$ soit égal à $X^2 + X + 1$ et dont le reste de la division par $X^4 - 2X^3 - 3X^2 + 13X - 10$ soit égal à $2X^2 - 3$.

Corrigé : 1. Il existe $P \in \mathbb{R}[X]$ tel que le reste de la division euclidienne de P par A soit R_1 et que le reste de la division euclidienne de P par B soit R_2 si et seulement si on a degré$(R_1) <$ degré(A), degré$(R_2) <$ degré(A) et il existe $Q_1 \in \mathbb{R}[X]$ tel que $P = AQ_1 + R_1$ et $Q_2 \in \mathbb{R}[X]$ tel que $P = BQ_2 + R_2$. Il existe un tel polynôme P si et seulement s'il existe des polynômes Q_1 et Q_2 satisfaisant l'égalité $AQ_1 - BQ_2 = R_2 - R_1$. D'après le théorème de Bézout, il existe de tels polynômes Q_1 et Q_2 si et seulement si le PGCD de A et B divise $R_1 - R_2$.

2. Posons $A = X^4 - 2X^3 - 2X^2 + 10X - 7$, $B = X^4 - 2X^3 - 3X^2 + 13X - 10$, $R_1 = X^2 + X + 1$ et $R_2 = 2X^2 - 3$. Commen ?ns par calculer le PGCD de A et B par l'algorithme d'Euclide.

$A = B + X^2 - 3X + 3$,
$B = (X^2 + X - 3)(X^2 - 3X + 3) + X - 1$,
$X^2 - 3X + 3 = (X - 2)(X - 1) + 1$.

le PGCD de A et B est 1, il divise $R_1 - R_2$. D'après la question 1., l'ensemble S des polynômes $P \in \mathbb{R}[X]$ tel que le reste de la division euclidienne de P par A est R_1 et le reste de la division euclidienne de P par B est R_2 est un ensemble non vide. Nous devons trouver un élément de S de degré minimal.

On remonte l'algorithme d'Euclide pour trouver U_0 et V_0 tels que $AU_0 - BV_0 = R_2 - R_1$.

$1 = X^2 - 3X + 3 - (X - 2)(X - 1)$,
$1 = X^2 - 3X + 3 - (X - 2)(B - (X^2 + X - 3)(X^2 - 3X + 3))$,
$1 = (X^2 - 3X + 3)(X^3 - X^2 + 5X + 7) - (X - 2)B$,
$1 = (A - B)(X^3 - X^2 + 5X + 7) - (X - 2)B$,
$1 = A(X^3 - X^2 + 5X + 7) - B(X^3 - X^2 - 4X + 5)$.

On a donc :

$$R_2 - R_1 = A(X^3 - X^2 + 5X + 7)(R_2 - R_1) - B(X^3 - X^2 - 4X + 5)(R_2 - R_1),$$

soit :

$$A(X^3 - X^2 + 5X + 7)(X^2 - X - 4) + R_1 = B(X^3 - X^2 - 4X + 5)(X^2 - X - 4) + R_2.$$

Posons :

$$P_0 = A(X^5 - 2X^4 - 8X^3 + 16X^2 + 13X - 28) + R_1,$$

le reste de la division de P_0 par A est égal à R_1 et le reste de la division de P_0 par B est égal à R_2, on a donc $P_0 \in S$. Soit $P \in \mathbb{R}[X]$ un polynôme, P appartient ? S si et seulement si $P_0 - P$ est divisible par A et par B. Comme A et B sont premiers entre eux, cela équivaut ? $P_0 - P$ est divisible par le produit AB, d'après le théorème de Gauss. Donc P appartient ? S si et seulement s'il existe un polynôme $K \in \mathbb{R}[X]$ tel que $P_0 - P = ABK$, c'est ? dire :

$$P = A(X^5 - 2X^4 - 8X^3 + 16X^2 + 13X - 28 - BK) + X^2 + X + 1.$$

Le degré de P est minimal si le degré de $X^5 - 2X^4 - 8X^3 + 16X^2 + 13X - 28 - BK$ est minimal, c'est ? dire si K est le quotient de la division euclidienne de $X^5 - 2X^4 - 8X^3 + 16X^2 + 13X - 28$ par B et $X^5 - 2X^4 - 8X^3 + 16X^2 + 13X - 28 - BK$ est le reste de la division euclidienne de $X^5 - 2X^4 - 8X^3 + 16X^2 + 13X - 28$ par B. En calculant ce reste, on trouve

$$P = A(-5X^3 + 3X^2 + 23X - 28) + X^2 + X + 1,$$

$$P = -5X^7 + 13X^6 + 27X^5 - 130X^4 + 75X^3 + 266X^2 - 440X + 197,$$

ce polynôme satisfait aux conditions de l'énoncé.

Exercice 2. Soit $A \in \mathbb{C}[X]$ et $B \in \mathbb{C}[X]$.

1. A-t-on $\text{PGCD}(A, B) = 1 \iff \text{PGCD}(A + B, AB) = 1$?
2. A-t-on $\text{PGCD}(A, B) = \text{PGCD}(A + B, AB)$?

Corrigé : 1. On va prouver $\text{PGCD}(A, B) = 1 \iff \text{PGCD}(A + B, AB) = 1$, en montrant les deux implications suivantes : $\text{PGCD}(A, B) = 1 \Rightarrow \text{PGCD}(A + B, AB) = 1$ et $\text{PGCD}(A + B, AB) = 1 \Rightarrow \text{PGCD}(A, B) = 1$

Supposons que $\text{PGCD}(A + B, AB) = 1$. Comme il est clair que $\text{PGCD}(A, B)$ divise $A + B$ et AB, on a $\text{PGCD}(A, B)$ divise $\text{PGCD}(A + B, AB)$. Donc $\text{PGCD}(A, B) = 1$

Supposons que $\text{PGCD}(A, B) = 1$, alors $\text{PGCD}(A + B, A) = \text{PGCD}(A, B) = 1$ et $\text{PGCD}(A + B, B) = \text{PGCD}(A, B) = 1$ c'est- ?-dire $A + B$ est premier avec A et avec B, $A + B$ est premier avec le produit AB. Finalement $\text{PGCD}(A + B, AB) = 1$

2. Non, il peut arriver que $\text{PGCD}(A, B)$ soit différent de $\text{PGCD}(A + B, AB)$. Nous allons le prouver par un contre exemple. Prenons $A = X$ et $B = X(X - 1)$, on a $\text{PGCD}(A, B) = X$ et $\text{PGCD}(A + B, AB) = \text{PGCD}(X^2, X^2(X - 1)) = X^2$.

Exercice 3.

1. Soit $P(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ un polynôme à coefficients dans $\mathbb{Z} \subset \mathbb{Q}$ tel que $a_0 \neq 0$. Soit $\alpha = \frac{p}{q} \in \mathbb{Q}$ une racine rationnelle de $P(X)$ avec $p, q \in \mathbb{Z}$ et $(p, q) = 1$. Montrer qu'on a $q|a_n$ et $p|a_0$.
2. Considérer le polynôme $P(X) = 4X^5 - 3X^3 - 7X^2 - 3X \in \mathbb{Q}[X]$. Montrer que ce polynôme admet trois racines dans le corps $\mathbb{Q}$. En déduire l'ensemble des solutions de $P(X) = 0$ dans $\mathbb{C}$.

Corrigé : 1. Remarquons d'abord que $n \geq 1$. Comme $\alpha = \frac{p}{q}$ est racine de P, on a $P(\alpha) = 0$. Donc

$$0 = q^n P(\alpha) = a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n.$$

On en déduit $p|\,(a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n)$. Donc $p|a_0 q^n$. Or $(p, q) = 1$, on trouve $p|a_0$. De la même manière, on a $q|a_n$.

2. Comme le coefficient constant du polynôme P est nul, le nombre 0 est donc une racine de P. Considérons ensuite le polynôme

$$P_1(X) := \frac{P(X)}{X} = 4X^4 - 3X^2 - 7X - 3,$$

d'après la question 1 de cet exercice, les racines rationnelles de P_1 sont contenues dans l'ensemble suivant :

$$\{\pm 1, \pm 3, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{3}{2}, \pm\frac{3}{4}\}.$$

Avec un calcul direct, on trouve que les racines rationnelles sont $-\frac{1}{2}$ et $\frac{3}{2}$. On obtient ainsi un facteur de degré 2 de P_1, à savoir $f(X) := 4(X - \frac{-1}{2})(X - \frac{3}{2}) = (2X + 1)(2X - 3) = 4X^2 - 4X - 3$. En effectuant la division euclidienne de P_1 par f, on a

$$P_1(X) = f(X) \cdot (X^2 + X + 1).$$

Donc

$$P(X) = X(2X + 1)(2X - 3)(X^2 + X + 1),$$

d'où l'ensemble des solutions de P : $\{0, \frac{-1}{2}, \frac{3}{2}, \frac{-1+\sqrt{3}i}{2}, \frac{-1-\sqrt{3}i}{2}\}$

Exercice 4. D'une manière générale, soit $z \in \mathbb{C}$ un nombre complexe, on note par $\bar{z}$ son conjugué complexe.

1. Soit $\zeta \in \mathbb{C}$ une racine complexe de l'équation $z^5 = 1$ telle que $\zeta \neq 1$. Montrer que les 4 solutions différentes dans $\mathbb{C}$ du polynôme $f(X) = X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$ sont : $\zeta, \zeta^2, \zeta^3, \zeta^4$. En particulier, si z_0 est une racine de $f(X)$, on a $z_0\bar{z_0} = 1$.
2. Montrer que le polynôme $f(X)$ est irréductible dans $\mathbb{Q}[X]$, en suivant les étapes suivantes :

(a) Soient $P(X) \in \mathbb{R}[X]$ un polynôme réel, et $z_0 \in \mathbb{C}$ une racine complexe de P. Montrer que $\bar{z_0}$ est également racine de $P(X)$.

(b) Montrer qu'on ne peut pas décomposer $f(X)$ en un produit de deux facteurs de degré 2 dans $\mathbb{Q}[X]$.

(c) Montrer que le polynôme $f(X)$ est irréductible dans $\mathbb{Q}[X]$.

3. Notons $I = \{g(X) \in \mathbb{Q}[X] \mid g(\zeta) = 0\} \subset \mathbb{Q}[X]$, qui est donc un idéal de $\mathbb{Q}[X]$.

(a) (Question de cours) Montrer I est un idéal principal, en utilisant la division euclidienne.

(b) Trouver un générateur de l'idéal I.

Corrigé : 1. Comme ζ est racine de l'équation $z^5 = 1$, soit $i \in \mathbf{Z}$, on a $(\zeta^i)^5 = (\zeta^5)^i = 1$. En plus, comme $\zeta \neq 1$, et 5 est un premier, on sait $\zeta^i \neq 1$ quelque soit $1 \leq i \leq 4$. D'autre part, $X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1)$, on en déduit que les ζ^i $(1 \leq i \leq 4)$ sont racines distinctes du polynôme f. Or f est un polynôme de degré 4, les racines complexes de f sont $\zeta, \zeta^2, \zeta^3, \zeta^4$. En particulier, soit z_0 une racine de f, on a $z_0\overline{z_0} = 1$.

2. (a) Ecrivons $P(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{R}[X]$ avec $a_i \in \mathbb{R}$. Comme $z_0 \in \mathbb{C}$ est racine de P, on a $P(z_0) = 0$. D'où

$$0 = \overline{P(z_0)} = \overline{a_n z_0^n + a_{n-1}z_0^{n-1} + \cdots + a_1 z_0 + a_0} = a_n\overline{z_0}^n + a_{n-1}\overline{z_0}^{n-1} + \cdots + a_1\overline{z_0} + a_0 = P(\overline{z_0}).$$

C'est-à-dire, le conjugué complexe $\overline{z_0}$ de z_0 est également racine de P. Ceci finit la preuve.

2. (b) On raisonne par l'absurde. Soit $f(X) = (aX^2 + bX + c)(a'X^2 + b'X + c')$ une décomposition en produit de deux facteurs de degré 2 dans $\mathbb{Q}[X]$. On a donc $a, b, c, a', b', c' \in \mathbb{Q}$. Clairement, on peut supposer $a = a' = 1$. Notons $g(X) = X^2 + bX + c \in \mathbb{Q}[X]$. Soit z_0 une racine de $g(X)$, comme $g|f$, z_0 est aussi racine de f. D'après la première question, on a $z_0\overline{z_0} = 1$. D'autre part, compte tenu de 2 (a), on a $g(X) = (X - z_0)(X - \overline{z_0}) = X^2 - (z_0 + \overline{z_0})X + z_0\overline{z_0} = X^2 + bX + c$. Donc $c = 1$. De la même manière, $c' = 1$. D'où

$$f(X) = (X^2 + bX + 1)(X^2 + b'X + 1) = X^4 + (b + b')X^3 + (2 + bb')X^2 + (b + b')X + 1.$$

On obtient ainsi un système d'équations :

$$\begin{cases} b + b' = 1 \\ 2 + bb' = 1 \end{cases}$$

En résolvant ce système, on a

$$\begin{cases} b = \frac{1+\sqrt{5}}{2} \\ b' = \frac{1-\sqrt{5}}{2} \end{cases} \quad \text{ou} \quad \begin{cases} b = \frac{1-\sqrt{5}}{2} \\ b' = \frac{1+\sqrt{5}}{2} \end{cases}.$$

En particulier, il n'y a pas de nombres rationnels b b' tels que

$$f(X) = (X^2 + bX + 1)(X^2 + b'X + 1).$$

C'est-à-dire, on ne peux pas décomposer $f(X)$ en produit de deux facteurs de degré 2 dans $\mathbb{Q}[X]$.

2. (c) En vertu de 2. (b), pour vérifier l'irréductibilité du polynôme f, il suffit de montrer que f n'admet pas de facteur de degré 1 dans $\mathbb{Q}[X]$, ou d'une manière équivalente, que f n'admet pas de racine rationnelle. Or d'après la question 1 de exo. 3, on sait que les racines rationnelles possibles sont ± 1, mais avec un calcul direct, on trouve $f(1) \neq 0, f(-1) \neq 0$. Ceci signifie que f n'a pas de racine dans $\mathbb{Q}$. D'où l'irréductibilité de f.

3. (a) Considérons l'ensemble suivant $\mathcal{D} := \{\deg(g) \mid g \in I - \{0\}\}$. Comme c'est un sous ensemble de $\mathbf{Z}_{\geq 1}$, il existe dans $\mathcal{D}$ un élément minimal, disons $n_0 \in \mathcal{D}$. Soit $g_0 \in I$ un élément de I de degré n_0, et montrons que l'idéal I est engendré par g_0. Quelque soit $g \in I - \{0\}$ un élément non nul, en utlisant la division euclidienne de g par g_0, il existe deux polynômes $h, r \in \mathbb{Q}[X]$ tels que $g = hg_0 + r$, et que $\deg(r) < \deg(g_0) = n_0$. Or par définition, $g_0 \in I$, on trouve $r = g - g_0 h \in I$. Donc $r = 0$ compte tenu de la définition de l'entier n_0. C'est-à-dire $g = hg_0$. Donc l'idéal I est principal, et est engendré par l'élément g_0.

3. (b) Soit g_0 un générateur de l'idéal I. Par définition, $f \in I$, il existe donc $h \in \mathbb{Q}[X]$ tel que $f = hg_0$. Or d'après la question 2, le polynôme f est irréductible. On a ou bien $\deg(h) = 0$, ou bien $\deg(g_0) = 0$. Comme $I \subsetneqq \mathbb{Q}[X]$ (par exemple, le polynôme $X \notin I$), on a $\deg(g_0) > 0$, ce qui entraîne $\deg(h) = 0$. Donc $h = a \in \mathbb{Q} - \{0\}$, par conséquent, $g_0 = a^{-1} \cdot f$. En particulier, $f = X^4 + X^3 + X^2 + X + 1$ est un générateur de I.