DOMAINE : Algèbre
NIVEAU : Avancé
CONTENU : Exercices

AUTEUR : Samuel BACH
STAGE : Montpellier 2013

Exercices sur les polynômes

Exercice 1 Soit $P, Q \in \mathbb{R}[X]$ deux polynômes réels non constants ayant les mêmes racines, et tels que $P-1$ et $Q-1$ aussi. Montrer que $P = Q$.

Solution de l'exercice 1 Soit p_0 et p_1 le nombre de racines distinctes respectivement de P et $P-1$. Soit n le degré de P, qu'on peut supposer par symétrie supérieur ou égal à celui de Q. Comme P et $P-1$ sont premiers entre eux, ils n'ont aucune racine commune. On remarque que $P - Q = (P-1) - (Q-1)$, donc ce polynôme admet comme racines à la fois les racines de P et celles de $P-1$, donc $p_0 + p_1$ racines. Il suffit de montrer que ce nombre est strictement supérieur à n pour conclure que $P - Q$ est le polynôme nul, soit $P = Q$.

Pour cela, on étudie les racines multiples en considérant le polynôme dérivé $P' = (P-1)'$. Soit $D_0 = \gcd(P, P')$ et $D_1 = \gcd(P-1, P')$. On sait que $\deg(D_i) = n - p_i$. Par ailleurs, D_0 et D_1 sont premiers entre eux car P et $P-1$ le sont, et divisent P' donc $D_0 D_1$ divise P' d'où en considérant les degrés : $n - p_1 + n - p_2 \geqslant n - 1$ soit $p_0 + p_1 > n$, □.

Exercice 2 Soit $a_i \in \mathbb{Z}, i = 1, \ldots, n$ des entiers deux à deux distincts, et soit $P := \prod_{i=1}^{n}(X - a_i) - 1$. Montrer que P est irréductible dans $\mathbb{Z}[X]$.

Solution de l'exercice 2 Supposons par l'absurde qu'il existe $Q, R \in \mathbb{Z}[X]$ non constants tels que $P = QR$. Alors $P(a_i) = Q(a_i)R(a_i) = -1$ donc $Q(a_i) = \pm 1$ et $R(a_i) = -Q(a_i)$ soit $(Q+R)(a_i) = 0$. Comme Q et R sont de degrés strictement inférieurs à n, on obtient $Q + R = 0$ donc $P = -Q^2$, donc P est négatif sur les réels. Ceci est absurde car P tend vers $+\infty$ en $+\infty$.

Exercice 3 Soit $p = 3q + 1$ un nombre premier ($q \in \mathbb{Z}$). Montrer que -3 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

Solution de l'exercice 3 D'après le petit théorème de Fermat, le polynôme $X^{3q} - 1$ est scindé à racines simples dans $\mathbb{Z}/p\mathbb{Z}$ (ses racines sont les inversibles de

$\mathbb{Z}/p\mathbb{Z}$), donc le polynôme X^2+X+1 aussi car il divise X^3-1 qui divise $X^{3q}-1$. Soit j une racine de X^2+X+1. Alors -3 est le carré de $2j+1$ car $(2j+1)^2 = 4j^2+4j+1 = 4(j^2+j+1)-3 = -3$. Pour penser à cette formule, il suffit de « résoudre »l'équation $j^2+j+1=0$, qui donne $j = \frac{-1\pm\sqrt{-3}}{2}$.

Exercice 4 Calculer $\sum_{i=1}^{n}\prod_{j\neq i}\frac{X-a_j}{a_i-a_j}$ pour $a_1,\ldots,a_n \in \mathbb{R}$ deux à deux distincts.

Solution de l'exercice 4 Ce polynôme est de degré au plus $n-1$ et vaut 1 en a_i donc est identiquement égal à 1.

Exercice 5 Soit $A \in \mathbb{R}[X]$ un polynôme réel, montrer qu'il existe $P, Q \in \mathbb{R}[X]$ tels que $A = P^2+Q^2$ si et seulement si pour tout réel x, $A(x) \geqslant 0$.

Solution de l'exercice 5 Le sens direct est immédiat. Supposons que pour tout $x \in \mathbb{R}$, on a $A(x) \geqslant 0$. Le polynôme réel A se décompose en produit de facteurs irréductibles de degré 1 et de degré 2. Toute racine a une multiplicité paire sinon le polynôme change de signe en la racine. Ainsi, le produit des facteurs de degré 1 de A est un carré donc une somme de deux carrés (le second étant 0). Un polynôme irréductible P de degré 2 se met sous forme canonique $(X+a)^2+b$ avec $b \geqslant 0$ car le polynôme est irréductible dans $\mathbb{R}$, d'où $P = (X+a)^2+c^2$ où $b = c^2$, donc P est une somme de deux carrés.

Ainsi, A est le produit de sommes de deux carrés, donc est une somme de deux carrés, par l'identité de Lagrange

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2+(ad+bc)^2.$$

Exercice 6 Montrer $X^2-X+1 \mid (X-1)^{n+2}+X^{2n+1}$ pour tout $n \in \mathbb{N}$.

Solution de l'exercice 6 On raisonne modulo X^2-X+1. On a alors $X^2 \equiv X-1$ donc $(X-1)^{n+2}+X^{2n+1} \equiv X^{2n+4}+X^{2n+1} \equiv X^{2n+1}(X^3+1) \equiv 0$ car X^2-X+1 divise X^3+1.

Exercice 7 Montrer que l'ensemble des réels x vérifiant $\sum_{k=1}^{70}\frac{k}{x-k} \geqslant \frac{5}{4}$ est réunion d'intervalles dont la somme des longueurs vaut 1988.

Solution de l'exercice 7 L'inégalité est équivalente, après multiplication par $Q(x)^2 = (\prod_{k=1}^{70}(x-k))^2$ et passage du second membre dans le premier, à $P(x) \geqslant 0$ où $P(X) = Q(X)R(X)$ avec $R(X) = 4\sum_{k=1}^{70} k\prod_{1\leqslant i\neq k\leqslant 70}(X-i) - 5Q(X)$.

On remarque $R(1) < 0$, $R(2) > 0$, $R(3) < 0$, ..., $R(70) > 0$ et $R(+\infty) = -\infty$ donc R a pour racines les r_i tels que $1 < r_1 < 2 < r_2 < \cdots < 70 < r_{70}$, et P a

pour racines les r_i et les entiers compris entre 1 et 70 inclus. Or P est négatif en $\pm\infty$ donc P est positif sur la réunion des intervalles $[k, r_k]$ pour $1 \leqslant k \leqslant 70$, dont la longueur totale vaut $\sum_{i=1}^{70}(r_i - i)$. Par les relations coefficients racines, on déduit du coefficient de X^{69} dans R que $\sum_{i=1}^{70} r_i = \frac{9}{5}\sum_{i=1}^{70} i$ donc la longueur totale des intervalles vaut $\frac{4}{5}\sum_{i=1}^{70} i = 1988$.

Exercice 8 Si P est un polynôme à coefficients entiers, on note $w(P)$ le nombre de ses coefficients impairs. Soit $Q_i = (1+x)^i$. Montrer que pour tout suite d'entiers $0 \leqslant i_1 < i_2 < \cdots < i_n$, $w(Q_{i_1} + \cdots + Q_{i_n}) \geqslant w(Q_{i_1})$.

Solution de l'exercice 8 On remarque $w(P \pm Q) \leqslant w(P) + w(Q)$ (inégalité triangulaire), et en ce qui concerne la multiplication, si $\deg(P) < k$ alors $w((1+X^k)P) = w(P) + w(PX^k) = 2w(P)$ $(*)$. En calculant $w(Q_i)$ pour des i petits, on remarque l'égalité polynômiale dans $\mathbb{Z}/2\mathbb{Z}$ suivante, qui se démontre facilement : $(1+X)^{2^k} \equiv 1 + X^{2^k}[2]$, qui nous permet de simplifier le calcul de w, car si $i = 2^k + i'$ avec $i' < 2^k$, $w(Q_i) = w((1+X^{2^k})(1+X)^{i'}) = 2w(Q_{i'})$. Cela va nous permettre de procéder par récurrence sur i_n.

On suppose le résultat acquis pour $i_n < N$ et on considère le cas $i_n = N$. Soit k tel que $2^k \leqslant N < 2^{k+1}$. Si $i_1 \geqslant 2^k$, posons $i_l = 2^k + i'_l$, alors d'après le calcul précédent, $w(Q_{i_1}+\cdots+Q_{i_n}) = 2w(Q_{i'_1}+\cdots+Q_{i'_n})$, $w(Q_{i_n}) = 2w(Q_{i'_n})$ et par hypothèse de récurrence, $w(Q_{i'_1}+\cdots+Q_{i'_n}) \geqslant w(Q_{i'_1})$ donc en multipliant par 2, on obtient $w(Q_{i_1}+\cdots+Q_{i_n}) \geqslant w(Q_{i_1})$.

Si $i_1 < 2^k$ soit r tel que $i_r < 2^k \leqslant i_{r+1}$, alors $w(Q_{i_1}+\cdots+Q_{i_n}) = w(\sum_{1\leqslant l\leqslant r} Q_{i_l} + \sum_{r<l\leqslant n} Q_{i'_l}) + w(\sum_{r<l\leqslant n} Q_{i'_l}) \geqslant w(\sum_{1\leqslant l\leqslant r} Q_{i_l}) \geqslant w(Q_{i_1})$ en appliquant successivemen la remarque $(*)$, l'inégalité triangulaire, et l'hypothèse de récurrence, ce qui conclut.

Exercice 9 Trouver les couples (n, m) tels que $n > 2$, $m > 2$, et il existe une infinité d'entiers naturels k tels que $k^n + k^2 - 1$ divise $k^m + k - 1$.

Solution de l'exercice 9 Si (n, m) est un tel couple, soit $P_n(X) = X^n + X^2 - 1$ et $P_m(X) = X^m + X - 1$, alors le reste R dans la division euclidienne de P_m par P_n est de degré strictement inférieur à n, et s'il est non nul, pour une infinité d'entiers k, $P_n(k)$ divise $R(k)$ et $|P_n(k)| \leqslant |R(k)|$, ce qui est impossible car P_n domine R d'où $R = 0$ et P_n divise P_m. En travaillant modulo $X^n + X^2 - 1$, on a $\frac{X^n}{1+X} \equiv 1 - X$ ($1 + X$ est inversible car -1 n'est pas racine de $X^n + X^2 - 1$) et $X^m + X - 1 \equiv 0$ donc $X^m \equiv 1 - X$, d'où $X^{m+1} + X^m - X^n \equiv 0$ d'où $P_k(X) = X^{k+1} + X^k - 1$ est divisible par P_n où $k = m - n$. Si $k + 1 = n$ alors P_n divise $P_k - P_n = X^{n-1} - X^2$ donc $n = 3$, et $m = 5$ qui convient. Sinon, $k \geqslant n$, et pour $x \in]0; 1[$ $x^{k+1} < x^n$ et $x^k < x^2$ car $n > 2$, d'où $P_k(x) < P_n(x)$, ce qui absurde car $P_n(0) = -1$ et

$P_n(1) = 1$ donc P_n a une racine sur $]0;1[$ que P_k ne partage pas.

Ainsi, seul le couple $(3,5)$ convient.