Quelques trucs sur les polynômes

Janvier 2003
(révision 27 Octobre 2013)

Table des matières

1 Racines et factorisation

Lemme 1.1 (Factorisation par la méthode de Hörner) *Soit un polynôme $P(X) = \sum_{k=0}^{n} a_k X^k$, et soit x un nombre fixé.*
Définissons u_n, u_{n-1}, ..., u_0 par :

$$\begin{array}{rcll} u_n & = & a_n & \\ u_{k-1} & = & xu_k + a_{k-1} & \text{pour } 1 \leq k \leq n \end{array}$$

Alors $P(x) = u_0$ et:

$$P(X) = u_0 + (X - x)\left(\sum_{k=1}^{n} u_k X^{k-1}\right)$$

Si de plus x est une racine de P, alors :

$$P(X) = (X - x)\left(\sum_{k=1}^{n} u_k X^{k-1}\right)$$

Preuve : On montre d'abord, par récurrence sur k allant de n à 0 :

$$\forall k \in \{0 \dots n\}, \quad u_k = \sum_{i=k}^{n} a_i x^{i-k}$$

En particulier, pour $k = 0$: $u_0 = \sum_{i=0}^{n} a_i x^i$, donc $P(x) = u_0$ et le premier point du lemme est montré.
Posons à présent:

$$\begin{array}{rcl} A(X) & = & (X - x)\left(\sum_{k=1}^{n} u_k X^{k-1}\right) + u_0 \\ & = & \sum_{k=1}^{n} u_k X^k - \sum_{k=1}^{n} x u_k X^{k-1} + u_0 \\ & = & \sum_{k=1}^{n} u_k X^k - \sum_{k=0}^{n-1} x u_{k+1} X^k \\ & = & u_n X^n + \sum_{k=1}^{n-1} (u_k - x u_{k+1}) X^k - x u_1 + u_0 \\ & = & u_n X^n + \sum_{k=1}^{n-1} (u_k - x u_{k+1}) X^k + (u_0 - x u_1) \\ & = & u_n X^n + \sum_{k=0}^{n-1} (u_k - x u_{k+1}) X^k \end{array}$$

Or, par définition de la suite u: $u_n = a_n$ et, pour k compris entre 0 et $n-1$, $u_k - x u_{k+1} = a_k$. On reporte dans $A(X)$:

$$A(X) = a_n X^n + \sum_{k=0}^{n-1} a_k X^k$$

C'est exactement $P(X)$, ce qui montre la première formule.
Dans le cas particulier où $P(x) = 0$, l'égalité $u_0 = P(x) = 0$ donne immédiatement la seconde formule. CQFD. ∎

Remarque : Ce lemme fournit un moyen de factoriser rapidement un polynôme dont on connaît une racine x. Il suffit de calculer dans l'ordre les coefficients u_n à u_0, en remplissant de gauche à droite un tableau comme dans l'exemple suivant où $P(X) = X^3 - 2X + 4X - 8$ et $P(2) = 0$.

k	3	2	1	0
Coefs a_k	1	-2	4	-8
$xu_{k+1} = 2u_{k+1}$	$-$	$2u_3 = 2$	$2u_2 = 0$	$2u_1 = 8$
$u_k = xu_{k+1} + a_k$	$u_3 = 1$	$u_2 = 0$	$u_1 = 4$	$P(2) = u_0 = 0$

On applique alors la formule du lemme en lisant la dernière ligne du tableau : $P(X) = (X-2)(u_3X^2 + u_2X^1 + u_1X^0) = (X-2)(X^2+4)$

Remarque : On peut, plus généralement, appliquer récursivement le lemme pour récrire un polynôme $P(X)$ sous la forme $Q(X-x)$ pour un x quelconque.
Cf l'exemple suivant pour $P(X) = X^3 + 2X^2 + 3X - 25$ et $x = 2$:

k	3	2	1	0
Coefsa_k	1	2	3	-25
$xu_{k+1} = 2u_{k+1}$	$-$	2	8	22
$u_k = xu_{k+1} + a_k$	1	4	11	-3
$xv_{k+1} = 2v_{k+1}$	$-$	2	12	
$v_k = xv_{k+1} + u_k$	1	6	23	
$xw_{k+1} = 2w_{k+1}$	$-$	2		
$w_k = xw_{k+1} + v_k$	1	8		
$xt_{k+1} = 2t_{k+1}$	$-$			
$t_k = xt_{k+1} + w_k$	1			

Les coefficients de la décomposition de P selon les $(X-2)^k$ sont donnés par le dernier terme de chaque ligne:

$$P(X) = (X-2)^3 + 8(X-2)^2 + 23(X-2) - 3$$

En effet, si l'on décompose par étapes:

$$\begin{array}{rcll} P(X) & = & U(X)(X-2) - 3 & \text{avec } U(X) = 1X^2 + 4X + 11 \\ U(X) & = & V(X)(X-2) + 23 & \text{avec } V(X) = 1X + 6 \\ V(X) & = & W(X)(X-2) + 8 & \text{avec } W(X) = 1 \end{array}$$

Lemme 1.2 *Soit un polynôme P à coefficients complexes. Alors toutes les racines de sa dérivée P' appartiennent à l'enveloppe convexe des racines de P.*

Preuve : Il suffit de prouver que toute racine r de P' peut s'écrire comme un barycentre à coefficients positifs des racines de P.
Soit n le degré de P. Tout polynôme à coefficients complexes étant scindé sur $\mathbf{C}$, il existe n complexes (pas forcément distincts) $\omega_1 \ldots \omega_n$ tels que $P(X) = a_n \prod_{i=1}^{n} (X - \omega_i)$, où a_n est le coefficient de degré n de P.
Si r est une racine de P, il est clair qu'elle se trouve dans l'enveloppe convexe (puisque par définition toutes les racines de P appartiennent à cette enveloppe convexe).
Supposons maintenant que r ne soit pas une racine de P. Exprimons la dérivée $P'(X)$:

$$P'(X) = a_n \sum_{i=1}^{n} \prod_{\left\{ \begin{array}{l} j = 1 \ldots n \\ j \neq i \end{array} \right.} (X - \omega_j)$$

Comme r n'est pas l'une des racines :

$$P'(r) = \sum_{i=1}^{n} \frac{P(r)}{r - \omega_i}$$

Ensuite, on trafique un peu en se servant des hypothèses :

$$\begin{array}{rcll} 0 & = & \sum_{i=1}^{n} \frac{P(r)}{r-\omega_i} & \text{car } P'(r)=0 \\ 0 & = & \sum_{i=1}^{n} \frac{1}{r-\omega_i} & \text{en divisant par } P(r)\neq 0 \\ 0 & = & \sum_{i=1}^{n} \frac{\overline{r-\omega_i}}{|r-\omega_i|^2} & \text{en multipliant par } \overline{r-\omega_i} \\ 0 & = & \sum_{i=1}^{n} \frac{1}{|r-\omega_i|^2}(r-\omega_i) & \text{en conjuguant} \end{array}$$

Or pour tout $i \in \{1..n\}$, $\frac{1}{|r-\omega_i|^2} > 0$, donc on a bien exprimé r comme un barycentre à coefficients positifs des racines $\omega_1 \dots \omega_n$ du polynôme P. CQFD. ∎

Lemme 1.3 (regroupement des racines dans un polynôme à racines simples) *Soit* $\mathbf{K}$ *un sous-corps de* $\mathbf{C}$*, et soient* k *nombres algébriques* $\alpha_1 \dots \alpha_k$*, racines de polynômes* $P_1 \dots P_k$ *à coefficients dans* $\mathbf{K}[X]$*.*
Alors il existe un polynôme à coefficients dans $\mathbf{K}$*, dont toutes les racines (dans* $\mathbf{C}$*) sont simples, et dont les* k *nombres* $\alpha_1 \dots \alpha_k$ *sont racines.*

Preuve : Posons $Q(X) = P_1(X) \dots P_k(X)$. Soit A le pgcd de Q et de sa dérivée Q'. Alors il existe $B \in \mathbf{K}[X]$ tel que $Q = AB$.
Soit α une racine de B. Supposons un instant que sa multiplicité m soit supérieure ou égale à 2. Alors ce serait une racine d'ordre m de Q, et donc une racine d'ordre $m-1$ de Q'. Donc $(X-\alpha)^{m-1}$ diviserait le pgcd de Q et Q', qui est A. Comme $Q = AB$, α serait alors racine simple de B, ce qui serait exactement le contraire de notre hypothèse. Donc B est à racines simples.
Soit à présent une racine α de Q, de multiplicité m. C'est alors une racine de multiplicité $m-1$ de A. Or $Q = AB$, donc α est racine d'ordre 1 de B.
Finalement, toutes les racines de Q sont racines de B, de multiplicité 1 dans B. En particulier, $\alpha_1 \dots \alpha_k$ sont racines de B. Comme de plus B est à racines simples, c'est bien le polynôme recherché. CQFD. ∎

Proposition 1.4 (Majoration du module des racines) *Soit un polynôme unitaire* $P \in \mathbf{C}[X]$*, tel que* $P = \sum_{k=0}^{n} p_k X^k$*. Alors pour toute racine* x *de* P*,* $|x| \leq \max\left\{1, \sum_{k=0}^{n-1} |p_k|\right\}$

Preuve : Si $|x| \leq 1$ c'est vrai. Sinon on a $x^n = -\sum_{k=0}^{n-1} p_k x^k$ donc, en divisant par x^{n-1} et en utilisant l'inégalité triangulaire, on obtient $|x| \leq \sum_{k=0}^{n-1} \left|\frac{p_k}{x^{n-1-k}}\right|$.
Or pour $0 \leq k \leq n-1$, $|x|^{n-1-} \geq 1$ donc $\left|\frac{p_k}{x^{n-1-k}}\right| \leq |p_k|$, d'où le résultat recherché. CQFD. ∎

Théorème 1.5 (Racines rationnelles d'un polynôme) *Soit* $A \in \mathbf{Z}[X]$*, de degré* ≥ 1*. Si* $A(p/q) = 0$*, (avec* $(p,q) \in \mathbf{Z} \times \mathbf{N}^*$ *et* $p \wedge q = 1$*) alors* q *divise le coefficient dominant de* A*, et* p *divise son coefficient constant.*

Preuve : Notons $A(X) = \sum_{k=0}^{n} a_k X^k$. Comme $A(p/q) = 0$, on a $a_0 q^n = -\sum_{k=1}^{n} a_k p^k q^{n-k}$. Donc $a_0 q^n = -p \sum_{k=1}^{n} a_k p^{k-1} q^{n-k}$ est multiple de p, et comme $p \wedge q = 1$, le théorème de Gauss dit que a_0 est multiple de p.
De même, $a_n p^n = -q \sum_{k=0}^{n-1} a_k p^k q^{n-1-k}$ est multiple de q donc a_n l'est. CQFD. ∎

Corollaire 1.6 *Les racines rationnelles d'un polynôme unitaire de degré* ≥ 1 *à coefficients entiers sont entières.*

Théorème 1.7 (Combinaison polynomiale de racines) *Soit* $P \in \mathbf{Z}[X_1, \dots, X_n]$*. Si* $x_1, \dots, x_n$ *sont racines de polynômes unitaires de* $\mathbf{Z}[X]$*, alors* $P(x_1, \dots, x_n)$ *est racine d'un tel polynôme.*

Preuve : Il suffit de montrer que c'est vrai pour $x_1 + x_2$, $x_1 x_2$ et pour ax_1, où $a \in \mathbf{Z}$ est quelconque. Le reste suit immédiatement, par récurrence sur le nombre de termes de P. Remarquons d'abord que, quitte à faire des produits de polynômes, on peut considérer que x_1, x_2 (distincts ou non) sont racines d'un certain polynôme unitaire $A \in \mathbf{Z}[X]$. Soit $m \geq 2$ son degré et notons $x_1, \dots, x_m$ les racines (distinctes ou non) de A.
Considérons le polynôme $B(X) = \prod_{i<j} (X - x_i x_j)$. Il est unitaire, et tous ses coefficients sont les valeurs prises en $(x_1, \dots, x_m)$ par des polynômes symétriques de $\mathbf{Z}[X_1, \dots, X_m]$. Ils sont donc entiers d'après le

théorème de Waring, et par conséquent, pour tout (i,j), le produit x_ix_j est racine d'un certain polynôme unitaire de $\mathbf{Z}[X]$.
De même, considérer le polynôme $C(X) = \prod_{i<j}(X-(x_i+x_j))$ nous fait conclure que x_i+x_j est aussi racine d'un polynôme unitaire de $\mathbf{Z}[X]$.
Enfin, tout $a \in \mathbf{Z}$ est racine de $X-a$ qui est unitaire, donc ax_1 est racine d'un polynôme unitaire de $\mathbf{Z}[X]$ d'après la remarque sur les produits. ∎

2 Arithmétique sur les polynômes

Lemme 2.1 (Lemme de Gauss sur le pgcd des coefficients) *Notons c la fonction qui à un polynôme de $\mathbf{Z}[X]$ associe le pgcd de ses coefficients. Alors pour tout couple (A,B) de polynômes de $\mathbf{Z}[X]$, $c(AB) = c(A)c(B)$.*

Preuve : Commençons par le cas particulier où $c(A) = c(B) = 1$. Supposons que $c(AB)$ soit multiple d'un nombre premier q. Alors, en notant $\tilde{A}$, $\tilde{B}$ et $\widetilde{AB}$ les polynômes de $(\mathbf{Z}/q\mathbf{Z})[X]$ obtenus en associant aux coefficients de A, B et AB leurs classes d'équivalence modulo q, on obtient $\widetilde{AB} = 0$.
Alors [1] $\tilde{A} = 0$ ou $\tilde{B} = 0$, donc tous les coefficients de A ou de B sont multiples de q, ce qui contredit $c(A) = c(B) = 1$. Donc $c(AB) = 1$.

Passons maintenant au cas général. En posant $\alpha = c(A)$ et $\beta = c(B)$ on obtient $A = \alpha A_1$ et $B = \beta B_1$ avec $c(A_1) = c(B_1) = 1$. Alors $AB = \alpha\beta A_1B_1$, donc $c(AB) = \alpha\beta c(A_1B_1)$. Or par définition $c(A_1) = c(B_1) = 1$ donc d'après le premier cas $c(A_1B_1) = 1$ et finalement $c(AB) = \alpha\beta$. CQFD. ∎

Lemme 2.2 (Réductibilité dans Z) *Si un polynôme à coefficients dans $\mathbf{Z}$ est réductible dans $\mathbf{Q}[X]$, alors il l'est dans $\mathbf{Z}[X]$.*

Preuve : Soit P un polynôme de $\mathbf{Z}[X]$ tel qu'il existe deux polynômes A et B de $\mathbf{Q}[X]$ vérifiant $P = AB$. Soient α et β deux entiers tels que $A_1 = \alpha A$ et $B_1 = \beta B$ soient dans $\mathbf{Z}[X]$. Avec les notations du lemme 2.1, posons $A_2 = \frac{1}{c(A_1)}A_1$ et $B_2 = \frac{1}{c(B_1)}B_1$: ils sont à coefficients entiers et on a $\alpha\beta P = c(A_1)c(B_1)A_2B_2$.
Or $\alpha\beta P = A_1B_1$ donc le lemme de Gauss 2.1 donne $\alpha\beta c(P) = c(A_1)c(B_1)$ donc $\alpha\beta P = \alpha\beta c(P)A_2B_2$.
Donc $P = c(P)A_2B_2$ qui est bien un produit de polynômes à coefficients entiers. CQFD. ∎

Exercice 2.3 (Critère d'Eisenstein) *Soit P un polynôme de $\mathbf{Z}[X]$ et de degré $n \geq 2$. S'il existe un entier premier p tel que :*

$$\forall k \in \{0 \dots n-1\} \quad p \mid P_k, \quad p \not| P_n, \quad p^2 \not| P_0$$

où $P(X) = \sum_{k=0}^{n} P_kX^k$, alors P est irréductible dans $\mathbf{Q}[X]$.

Solution : Supposons P réductible dans $\mathbf{Q}[X]$. Alors d'après le lemme 2.2 il est réductible dans $\mathbf{Z}[Z]$ et il existe A et B à coefficients entiers tels que $P = AB$.
Comme d'habitude, associons à P, A et B les polynôme $\tilde{P}$, $\tilde{A}$, $\tilde{B}$ dont les coefficients sont les classes d'équivalence modulo p de ceux de P, A et B.
Or par hypothèse $\tilde{P} = \tilde{P}_nX^n$. En appelant a et b les degrés respectifs de A et B on obtient $\tilde{A}(X) = \tilde{A}_aX^a$ et $\tilde{B}(X) = \tilde{B}_bX^b$ (si on avait $\tilde{A} = 0$ ou $\tilde{B} = 0$ alors $\tilde{P}_n = 0$: absurde). En particulier $\tilde{A}_0 = \tilde{B}_0 = 0$ donc $p \mid A_0$ et $p \mid B_0$. Mais alors p^2 diviserait $A_0B_0 = P_0$ ce qui contredirait les hypothèses. CQFD ∎

Exercice 2.4 (Pas de polynôme à valeurs premières) *Il n'existe aucun polynôme non-constant à coefficients dans $\mathbf{Z}$ qui, pour tout entier n, prenne une valeur première.* [2]

Solution : Supposons qu'il existe un tel polynôme P. Soit n un entier quelconque. Alors pour tout $k \in \mathbf{N}$, $P(n+kP(n))$ est multiple de $P(n)$. En effet, en notant $P(X) = \sum_{i=0}^{N} a_iX^i$, on obtient :

$$\begin{aligned} P(n+kP(n)) &= \sum_{i=0}^{N} a_i(n+kP(n))^i \\ &= \sum_{i=0}^{N} a_iS_i \end{aligned}$$

[1] en effet, puisque q est premier, $\mathbf{Z}/q\mathbf{Z}$ est un corps donc $(\mathbf{Z}/q\mathbf{Z})[X]$ est un anneau intègre.
[2] Par contre il existe des polynômes (à plusieurs variables) qui *s'ils prennent une valeur positive* pour des valeurs entières de leurs variables, prennent alors une valeur première, et donnent ainsi tous les nombres premiers. Ce résultat s'étend non seulement aux nombres premiers, mais à tout sous-ensemble de $\mathbf{N}$ calculable par ordinateur. Dans le cas des nombres premiers, on a même pu exhiber de tels polynômes, malheureusement sans utilité pratique pour le calcul.

Où, d'après la formule du binôme, $S_i = \sum_{j=0}^{i} \mathcal{C}_i^j n^{i-j}(kP(n))^j$. En remarquant que $\sum_{j=1}^{i} \mathcal{C}_i^j n^{i-j}(kP(n))^j$ est multiple de $P(n)$, il reste :

$$\begin{array}{lll} P(n+kP(n)) & \equiv \sum_{i=0}^{N} a_i \mathcal{C}_i^0 n^i (kP(n))^0 & \pmod{P(n)} \\ & \equiv \sum_{i=0}^{N} a_i n^i & \pmod{P(n)} \\ & \equiv P(n) & \pmod{P(n)} \\ & \equiv 0 & \pmod{P(n)} \end{array}$$

Donc $P(n+kP(n))$ est bien multiple de $P(n)$.

Comme P n'est pas constant, sa dérivée est de signe constant non nul à partir d'un certain rang n. Cela impose que P soit strictement monotone à partir de ce rang. Or P, étant censé ne donner que des nombres premiers, doit rester positif, donc il est strictement croisssant à partir du rang n. Donc $P(n+P(n)) > P(n)$. Or $P(n+P(n))$ est multiple de $P(n)$, donc il n'est pas premier : cela contredit la définition de P. ∎

Exercice 2.5 (Polynôme à valeurs entières) *Soit un polynôme $Q \in \mathbf{Q}[X]$ tel que $\forall n \in \mathbf{N}, Q(n) \in \mathbf{Z}$. Montrer que Q est à coefficients entiers.*

Solution : Supposons que Q ne soit pas à coefficients entiers. Soit m le plus petit entier ≥ 1 tel que $mQ \in \mathbf{Z}[X]$ et posons $P = mQ$.
Alors m admet un facteur premier de $q \geq 2$. Soit $\tilde{P}$ le polynôme de $K[X]$, où K est le corps $\mathbf{Z}/q\mathbf{Z}$, dont chaque coefficient est la classe d'équivalence modulo q du coefficient de P de même degré.
Pour tout $n \in \mathbf{N}$, $Q(n)$ est entier donc $P(n) = mQ(n)$ est multiple de m, donc de q. En notant $\tilde{n}$ la classe d'équivalence de n on en déduit : $\forall \tilde{n} \in K, \tilde{P}(\tilde{n}) = 0$. D'où $\tilde{P} = 0$.
Donc tous les coefficients de P sont multiples de q.
C'est absurde puisque par définition de m les coefficients de P sont premiers entre eux ! Donc Q est bien à coefficients entiers. CQFD. ∎

Exercice 2.6 (Polynômes entiers multiples l'un de l'autre) *Soient A et B deux polynômes (non-nuls) de $\mathbf{Z}[X]$. Montrer que A est multiple de B si et seulement si pour tout entier $n \geq 0$, $A(n)$ est multiple de $B(n)$.*

Remarque : Cela devient faux si $A(n)$ n'est multiple de $B(n)$ que sur un ensemble infini d'entiers. Par exemple l'équation de Fermat $x^2 = Dy^2 + 1$ possède (pour D non-carré) une infinité de couples (x, y) entiers solutions, mais $DX^2 + 1$ est premier avec X^2.
Solution : Supposons A multiple de B. Alors il existe $C \in \mathbf{Z}[X]$ tel que $A = BC$. Comme pour tout $n \in \mathbf{N}$, $A(n) = B(n)C(n)$ donc $A(n)$ est multiple de $B(n)$.
C'était évident ! Dans l'autre sens ça l'est moins. Procédons à la division euclidienne de A par B. Il existe alors $(Q, R) \in \mathbf{Q}[X] \times \mathbf{Q}[X]$ tels que $A(X) = B(X)Q(X) + R(X)$ et que $\text{degre}(R) < \text{degre}(B)$.
Soit α la partie fractionnaire du coefficient constant (i.e. celui de degré 0) de Q. Soit m le plus petit multiple commun des dénominateurs des autres coefficients Q. Alors, en notant f la fonction partie fractionnaire, on a : $\forall n \in \mathbf{N}, f(Q(nm)) = \alpha$. Comme B n'est pas nul, ses racines sont bornées, donc il existe $N_0 \in \mathbf{N}$ tel que, pour tout $n \geq N_0$, $B(nm) \neq 0$.
Alors $\forall n \geq N_0$, $\frac{A(nm)}{B(nm)} = Q(nm) + \frac{R(nm)}{B(nm)}$.
Par hypothèse : $\forall n \geq N_0, f\left(Q(nm) + \frac{R(nm)}{B(nm)}\right) = 0$ Or $f(Q(nm)) = \alpha$ donc :

$$\forall n \geq N_0, \quad f\left(\alpha + \frac{R(nm)}{B(nm)}\right) = 0 \quad (*)$$

Par définition de α, $\alpha \in [0 \quad 1[$.
Supposons $\alpha \in]0 \quad 1[$. Comme R est de degré strictement inférieur à celui de B, le quotient $\frac{R(nm)}{B(nm)}$ tend vers 0 quand n tend vers $+\infty$. En particulier, il existerait $N_1 \in \mathbf{N}$ tel que : $\forall n \geq N_1, \left|\frac{R(nm)}{B(nm)}\right| < \min\{\alpha, 1-\alpha\}$.
Alors $\forall n \geq N_1, \alpha + \frac{R(nm)}{B(nm)} \in]0 \quad 1[$, ce qui contredit clairement $(*)$.
Donc $\alpha = 0$ et $(*)$ devient :

$$\forall n \geq N_0, \quad f\left(\frac{R(nm)}{B(nm)}\right) = 0$$

Comme le quotient $\frac{R}{B}$ tend vers 0, l'égalité ci-dessus implique l'existence d'un $N_2 \in \mathbf{N}$ tel que :

$$\forall n \geq N_2, \quad \frac{R(nm)}{B(nm)} = 0$$

d'où : $\forall n \geq N_2, R(nm) = 0$. R a donc une infinité de racines, donc il est nul et $A(X) = B(X)Q(X)$. Alors par hypothèse $\forall n \geq 0, Q(n) \in \mathbf{Z}$. Or $Q(X)$ est à coefficients rationnels, donc d'après l'exo 2.5, il est à coefficients entiers. CQFD ∎

3 L'essentiel des polynômes symétriques

Définition 3.1 (Degré, degré partiel, poids d'un monôme) *Soit un monôme $M = \beta X_1^{\alpha_1} \dots X_n^{\alpha_n}$, avec $\beta \neq 0$*

- *Pour tout $k \in \{1 \dots n\}$, α_k est appelé degré partiel du monôme par rapport à l'indéterminée X_k. On le note $\mathrm{dp}_{X_k}(M)$.*
- *La somme $\alpha_1 + \dots + \alpha_n$ est le degré du monôme.*
- *La somme $\alpha_1 + 2\alpha_2 + \dots + n\alpha_n$ est le poids du monôme.*
- *Par convention (commode), si $\beta = 0$, alors degré et degré partiel valent $-\infty$, avec : pour tout entier α, $\alpha > -\infty$ et $-\infty + \alpha = -\infty$.*

Soit un polynôme P à n indéterminées.

- *Pour tout $k \in \{1 \dots n\}$, on appelle degré partiel de P par rapport à X_k le plus grand des degrés partiels, par rapport à X_k, de ses monômes. On le note $\mathrm{dp}_{X_k}(P)$*
- *On appelle degré de P le plus grand des degrés de ses monômes.*
- *On appelle poids de P le plus grand des poids de ses monômes.*

Définition 3.2 (Polynôme symétrique) *Soit un polynôme P à n indéterminées $X_1, \dots, X_n$. Ce polynôme est dit symétrique si et seulement si, pour toute permutation φ des entiers $1, \dots, n$, $P(X_1, \dots, X_n) = P(X_{\varphi(1)}, \dots, X_{\varphi(n)})$.*

Remarque : Pour les polynômes symétriques, le degré partiel par rapport à chacune des indéterminées est identique, donc on parle du degré partiel, tout court, et on se contente de le noter $\mathrm{dp}(P)$.

Définition 3.3 (Polynômes symétriques élémentaires) *Soit un entier $n \geq 1$. Pour tout entier $i \in \{1 \dots n\}$, on appelle i-ème fonction symétrique élémentaire à n indéterminées et on note Σ_i^n le polynôme formé par la somme de tous les produits possibles de i indéterminées sur n :*

$$\Sigma_i^n = \sum_{1 \leq k_1 < k_2 < \dots < k_i \leq n} X_{k_1} X_{k_2} \dots X_{k_i}$$

Exemple : Pour $n = 3$: $\Sigma_1^3 = X_1 + X_2 + X_3$, $\Sigma_2^3 = X_1X_2 + X_1X_3 + X_2X_3$, $\Sigma_3^3 = X_1X_2X_3$

Lemme 3.4 (Degré d'une somme ou d'un produit de polynômes) *Soient deux polynômes P et Q, à n indéterminées, et à coefficients dans un anneau $\mathbf{A}$ commutatif intègre.*

Alors : $\begin{cases} \mathrm{degre}(P+Q) & \leq & \max\{\mathrm{degre}(P), \mathrm{degre}(Q)\} \\ \mathrm{degre}(PQ) & = & \mathrm{degre}(P) + \mathrm{degre}(Q) \end{cases}$

Preuve : Si un coefficient de $P + Q$ est non-nul, alors l'un au moins des coefficients correspondants de P ou de Q est non-nul, ce qui démontre le lemme pour la somme.
Si P ou Q est nul, alors $PQ = 0$ donc $\mathrm{degre}(PQ) = -\infty$ donc le lemme est vrai.
Pour le produit c'est moins évident : soient P et Q sont non-nuls et de degrés respectifs p et q. Prenons, parmi les coefficients non-nuls de degré p de P, celui qui a le plus grand indice $\alpha = (\alpha_1, \dots, \alpha_n)$ pour l'ordre lexicographique [3] . On procède de même pour extraire de Q le coefficient d'indice $\beta = (\beta_1, \dots, \beta_n)$ et de degré q.
L'ordre lexicographique est compatible avec l'addition, donc le coefficient d'indice $\gamma = \alpha + \beta$ du produit

[3] Pour deux n-uplets d'entiers $x = (x_1, \dots, x_n)$ et $y = (y_1, \dots, y_n)$, on dit que $x \leq y$ pour l'ordre lexicographique si et seulement si $x = y$ ou si, pour le plus petit indice i tel que $x_i \neq y_i$, on a $x_i < y_i$. On vérifie alors facilement qu'il s'agit d'une relation d'ordre (Pour tout x, $x \leq x$; Si $x \leq y$ et $y \leq x$ alors $x = y$; Si $x \leq y$ et $y \leq z$ alors $x \leq z$), qu'elle est totale (on a toujours $x \leq y$ ou $y \leq x$) et qu'elle est compatible avec l'addition (Si $x \leq y$ et $x' \leq y'$ alors $x + x' \leq y + y'$).

$R = PQ$ est le produit de P_α et Q_β [4] . Or **A** est intègre, donc ce produit est non-nul. Or il est de degré $p+q$, donc $R = PQ$ est au moins de degré $p+q$. Enfin, il est clair que PQ est de degré inférieur ou égal à $p+q$, donc le lemme est démontré.CQFD. ∎

Lemme 3.5 *Soit un polynôme P à n indéterminées, et soient n polynômes $Q_1, \ldots, Q_n$, tels que pour $k = 1, \ldots, n$,* $\text{degre}(Q_k) = k$. *Alors le degré de $P(Q_1, Q_2, \ldots, Q_n)$ est inférieur ou égal au poids de P.*

Preuve : Le degré d'un produit $Q_1^{\alpha_1} \ldots Q_n^{\alpha_n}$ est inférieur ou égal au poids du monôme $X_1^{\alpha_1} \ldots X_n^{\alpha_n}$. On applique ça à chaque monôme de P et c'est gagné. ∎

Théorème 3.6 (Polynôme symétrique et symétriques élémentaires) *Soit un anneau commutatif* **A**, *et soit un polynôme symétrique à n indéterminées $P \in \mathbf{A}[X_1, \ldots, X_n]$. Alors il existe un polynôme $Q \in \mathbf{A}[X_1, \ldots, X_n]$, de poids inférieur ou égal au degré de P, tel que $P = Q(\Sigma_1^n, \ldots, \Sigma_n^n)$.*

Remarque : On peut de plus montrer que Q est unique, et que $\text{degre}(Q) \leq \text{dp}(P)$, mais on n'en a pas besoin ici.

Preuve : On peut procéder par récurrence sur le nombre d'indéterminées n.

Soit $H(n)$ la proposition : "Le théorème est vrai pour tous les polynômes à n indéterminées ou moins".

- $H(1)$ est vraie : il suffit de prendre $Q = P$.
- Soit $n \geq 1$ et supposons $H(n)$ vraie. Soit P un polynôme symétrique à $n+1$ indéterminées. On va montrer par récurrence sur le degré de P que $H(n+1)$ est vraie.

Soit $G(d)$ la proposition : "H(n+1) est vraie pour les polynômes de degré inférieur ou égal à d".

- Si $d = 0$, alors P est constant et $Q = P$ suffit.
- Prenons $d \geq 0$ et supposons $G(d)$ vraie.

Supposons P de degré $d+1$. Posons $P_1 = P(X_1, \ldots, X_n, 0)$. C'est un polynôme symétrique à n indéterminées, dont le degré est inférieur ou égal à celui de P. Comme $H(n)$ est vraie, il existe un polynômes Q_1, tel que $P_1 = Q_1(\Sigma_1^n, \ldots, \Sigma_n^n)$, avec $\text{poids}(Q_1) \leq \text{degre}(P_1) \leq \text{degre}(P)$. Posons $P_2 = P_1 - Q_1(\Sigma_1^{n+1}, \ldots, \Sigma_n^{n+1})$. P_2 est symétrique, et $\text{degre}(P_2) \leq \text{Max}\{\text{degre}(P_1), \text{poids}(Q_1)\} \leq \text{degre}(P)$. Par construction, on a $P_2(X_1, \ldots, X_n, 0) = 0$, et comme il est symétrique, on a pour tout entier j tel que $1 \leq j \leq n$,

$$P_2(X_1, \ldots, X_{j-1}, 0, X_{j+1}, \ldots, X_{n+1}) = 0$$

et est donc multiple de X_j. Donc P_2 est multiple de $X_1 \ldots X_{n+1}$, qui n'est autre que Σ_{n+1}^{n+1}. Il existe donc un polynôme P_3 tel que $P_2 = \Sigma_{n+1}^{n+1} P_3$. P_2 est symétrique donc P_3 aussi.

On a alors : $\text{degre}(P_3) = \text{degre}(P_2) - (n+1)$ donc $\text{degre}(P_3) \leq (d+1) - (n+1)$. On peut alors appliquer $G(d)$: il existe un polynôme Q_2 à $n+1$ indéterminées, tel que $\text{poids}(Q_2) \leq \text{degre}(P_3) \leq (d+1) - (n+1)$, avec $P_3(X_1, \ldots, X_{n+1}) = Q_2(\Sigma_1^{n+1}, \ldots, \Sigma_{n+1}^{n+1})$.Alors :

$$P = Q_1(\Sigma_1^n, \ldots, \Sigma_n^n) + \Sigma_{n+1}^{n+1} Q_2(\Sigma_1^{n+1}, \ldots, \Sigma_{n+1}^{n+1})$$

En conclusion, $Q(X_1, \ldots, X_{n+1}) = Q_1(X_1, \ldots, X_n) + X_{n+1} Q_2(X_1, \ldots, X_{n+1})$ convient, et avec les remarques faites sur les poids de Q_1 et Q_2, on conclut que $\text{poids}(Q) \leq \text{degre}(P)$. Donc $G(d+1)$ est vraie.

- Par récurrence sur d, $G(d)$ est donc vraie pour tout entier d. Du coup, on a montré la véracité de $H(n+1)$, ce qui achève la première récurrence. CQFD. ∎

Théorème 3.7 (Relation coefficients-racines d'un polynôme) *Soit un corps commutatif* **K** *et soit P un polynôme scindé sur K, de degré n, dont le coefficient de degré i est noté p_i. Alors, si l'on note $\omega_1, \ldots, \omega_n$ les racines de P dans* **K**, *on a la relation :*

$$\forall i \in \{0 \ldots n-1\}, \frac{p_i}{p_n} = (-1)^{n-i} \Sigma_{n-i}^n(\omega_1, \ldots, \omega_n)$$

Preuve : On peut écrire P sous la forme : $P(X) = p_n(X - \omega_1) \ldots (X - \omega_n)$. En développant, on constate que, pour $i = 0 \ldots n-1$, le terme de degré i est la somme de tous les produits possibles de $n-i$ racines, multipliée par $(-1)^i$ et par p_n. On reconnaît la définition de $\Sigma_{n-i}^n(\omega_1, \ldots, \omega_n)$et on en conclut le résultat annoncé. ∎

[4] On peut expliciter ce "donc": Soient deux indices ρ et φ tels que $P_\rho Q_\varphi$ apparaisse dans l'expression de R_γ. Ces indices correspondent obligatoirement à des termes de degrés p et q. Par définition de α et β, on a alors $\rho \leq \alpha$ et $\varphi \leq \beta$. Donc, si $\rho < \alpha$ ou $\varphi < \beta$, alors $\rho + \varphi < \alpha + \beta$, ce qui serait absurde puisque l'on doit avoir $\rho + \varphi = \gamma = \alpha + \beta$. Donc $\rho \geq \alpha$ et $\varphi \geq \beta$, et comme on a déjà les inégalités $\rho \leq \alpha$ et $\varphi \leq \beta$, on conclut $\rho = \alpha$ et $\varphi = \beta$.

Théorème 3.8 (Waring) *Soient un corps commutatif* $\mathbf{K}$*,* $\mathbf{A}$ *un sous-anneau de* $\mathbf{K}$*, et* P *un polynôme unitaire de degré* n *à coefficients dans* $\mathbf{A}$*, possédant* n *racines* $\omega_1, \ldots, \omega_n$ *dans* $\mathbf{K}$*.*
Soit Q *un polynôme symétrique à* n *indéterminées et à coefficients dans* $\mathbf{A}$*.*
Alors $Q(\omega_1, \ldots, \omega_n) \in \mathbf{A}$*.*

Preuve : Q est symétrique, donc il existe un polynôme R à coefficients dans $\mathbf{A}$ tel que :

$$Q = R(\Sigma_1^n, \ldots, \Sigma_n^n)$$

Notons $p_0, \ldots, p_n$ les coefficients de P. D'après les relations entre coefficients et racines, on a pour tout $i \in \{1, \ldots, n\}$:

$$\Sigma_i^n(\omega_1, \ldots, \omega_n) = (-1)^i p_{n-i} \text{ car } p_n = 1$$

Donc $Q(\omega_1, \ldots, \omega_n) = R((-1)^1 p_{n-1}, \ldots, (-1)^n p_0)$. Or les coeficients $p_0, \ldots, p_{n-1}$ appartiennent à l'anneau $\mathbf{A}$, et les coefficients de R aussi, donc $Q(\omega_1, \ldots, \omega_n) \in \mathbf{A}$. CQFD. ∎
Remarque : Si $\mathbf{A}$ est un sous-corps de $\mathbf{K}$, il n'est plus nécessaire que P soit unitaire car, en divisant tous ses coefficients par p_n, on obtient un polynôme Q unitaire dont les coefficients sont encore dans $\mathbf{A}$ et qui a les mêmes racines que P. On peut alors appliquer le théorème à Q.

4 Autour des Polynômes de Tchebytchev

Définition 4.1 (Polynômes de Tchebytchev) *Pour tout* $n \in \mathbf{N}$*, il existe un unique polynôme* P_n *de* $\mathbf{Z}[X]$ *tel que pour tout* $\theta \in \mathbf{R}$*,* $\cos(n\theta) = P_n(\cos(\theta))$
Ces polynômes sont définis par récurrence :

$$P_0(X) = 1, \quad P_1(X) = X, \quad \forall n \geq 0, P_{n+2}(X) = 2XP_{n+1}(X) - P_n(X)$$

Pour tout $n \geq 1$*,* P_n *est de degré* n*, de coefficient dominant* 2^{n-1}

Preuve : L'unicité est évidente : s'il existe un autre polynôme Q_n tel que $\cos(n\alpha) = P_n(\cos(\alpha)) = Q_n(\cos(\alpha))$, alors pour une infinité de réels, $P_n(x) = Q_n(x)$ ce qui implique $P_n(x) = Q_n(x)$.
Montrons maintenant l'existence :

- Il est clair que P_0 et P_1 existent.
- Soit $n \geq 0$, et supposons que P_n et P_{n+1} existent. Alors :

$$\cos((n+1)\alpha) = \cos(n\alpha)\cos(\alpha) - \sin(n\alpha)\sin(\alpha) \quad (1)$$

De même, $\cos((n+2)\alpha) = \cos(n\alpha)\cos(2\alpha) - \sin(n\alpha)\sin(2\alpha)$. Or $\sin(2\alpha) = 2\sin(\alpha)\cos(\alpha)$ donc :

$$\cos((n+2)\alpha) = \cos(n\alpha)\cos(2\alpha) - 2\sin(n\alpha)\sin(\alpha)\cos(\alpha) \quad (2)$$

En calculant $(2) - 2\cos(\alpha)(1)$ et en se rappelant que $\cos(2\alpha) = 2\cos^2(\alpha) - 1$, on se débarasse des sinus :

$$\cos((n+2)\alpha) - 2\cos(\alpha)\cos((n+1)\alpha) = \cos(n\alpha)(2\cos^2(\alpha) - 1) - 2\cos^2(\alpha)\cos(n\alpha)$$

ce qui donne $P_{n+2}(X) - 2XP_{n+1}(X) = P_n(X)(2X^2 - 1) - 2X^2P_n(X) = -P_n(X)$, i.e.

$$P_{n+2}(X) = 2XP_{n+1}(X) - P_n(X)$$

qui est bien un polynôme de $\mathbf{Z}[X]$. Déterminer le coefficient dominant et le degré est alors évident par récurrence. ∎

Exercice 4.2 (Points à distances rationnelles) *Trouver, dans le plan,* N *points dont les distances deux à deux sont rationnelles. On peut chercher des points cocycliques.*

Remarque : On ignore s'il existe des solutions avec des points non-cocycliques.
Solution : Commen cons par remarquer que, pour $\alpha \in \left]0 \quad \frac{\pi}{2}\right[$ tel que $\cos(\alpha)$ et $\sin(\alpha)$ soient rationnels, les points $M_i(\cos(2i\alpha), \sin(2i\alpha))$ où $i \in \mathbf{N}^*$, ont deux à deux ont des distances rationnelles.
En effet les points M_i et M_j sont tous deux sur le cercle unité, et

$$d(M_i, M_j) = 2\sin\left(\frac{2(i-j)\alpha}{2}\right)$$

Il nous suffit donc de montrer que pour tout entier $n \in \mathbf{N}^*$, $\cos(n\alpha)$ et $\sin(n\alpha)$ sont rationnels. En effet :
- Par hypothèse c'est vrai pour $n = 1$.
- Si c'est vrai pour $n \geq 1$, alors $\cos((n+1)\alpha) = \cos(n\alpha)cos(\alpha) + \sin(n\alpha)\sin(\alpha)$ et $\sin((n+1)\alpha) = \sin(n\alpha)\cos(\alpha) + \cos(n\alpha)\sin(\alpha)$ sont tous deux rationnels en tant que somme de produits de rationnels.

Trouvons maintenant une condition suffisante sur α pour que les points M_i soient distincts deux-à-deux. S'il existe deux entiers $1 \leq i < j$ tels que $M_i = M_j$, alors en particulier :

$$\begin{cases} \cos(j\alpha) &= \cos(i\alpha) \\ \sin(j\alpha) &= \sin(i\alpha) \end{cases}$$

ce qui implique $j\alpha \equiv i\alpha \pmod{2\pi}$. Il existe donc un entier $n \geq 1$ tel que $n\alpha \equiv 0 \pmod{2\pi}$, et en particulier :

$$\cos(n\alpha) = 1$$

Posons $A = \cos(\alpha)$; alors $P_n(A) = 1$ où P_n est le n-ième polynôme de Tchebytchev. A est donc racine de $P_n - 1$, et il est rationnel par hypothèse. Or $P_n \in \mathbf{Z}[X]$ a pour coefficient dominant 2^{n-1}, donc $P_n - 1$ aussi et A peut s'écrire sous la forme $\frac{p}{2^k}$ où $p \wedge 2^k = 1$.
Il nous suffit donc de choisir α tel que $\cos(\alpha)$ ne puisse pas s'écrire sous cette forme et que, par conséquent, les points $(M_i)_{i\in\mathbf{N}^*}$ soient tous distincts.
Un tel α existe bien : il suffit de s'inspirer du triangle rectangle $3, 4, 5$ et de poser $\alpha = \arccos(\frac{3}{5})$. Alors $\cos(\alpha) = \frac{3}{5}$ et $\sin(\alpha) = \frac{4}{5}$ sont bien deux fractions irréductibles dont le dénominateur n'est pas une puissance de 2. CQFD. ∎