Chapitre 4

Les Polynômes

4.1 Définitions et terminologie

Dans toute la suite, $\mathbb{k}$ désignera un corps commutatif

Définition 59 *On appelle polynôme à une indéterminée et coefficients dans* $\mathbb{k}$ *ou plus simplement polynôme, toute expression algébrique de la forme*
$a_pX^p + a_{p-1}X^{p-1} + \cdots + a_1X + a_0$, *avec* $a_i \in \mathbb{k}$ *pour tout* $i \in \{0, \cdots, p\}$.

• Les scalaires a_i sont appelés coefficients du polynôme.
• Le plus grand indice i tel que $a_i \neq 0$, s'il existe, s'appelle le degré de P et est noté $degP$.
• Si tous les coefficients a_i sont nuls, P est appelé polynôme nul et est noté 0. Par convention, deg $0 = -\infty$.
• Un polynôme de la forme $P = a_0$ avec $a_0 \in \mathbb{k}$ est appelé polynôme constant. Si $a_0 \neq 0$, son degré est 0.
• L'ensemble des polynôme à une indéterminée et à coefficients dans $\mathbb{k}$ est noté $\mathbb{k}[X]$.
• L'ensemble des polynôme à une indéterminée, à coefficients dans $\mathbb{k}$ et de degré $\leq n$ est noté $\mathbb{k}_n[X]$
Exemples :
• $X^3 - \frac{1}{4}X + \frac{3}{2}$ est un polynôme de degré 3.
• Si $n \in \mathbb{N}^*$, $X^n - 1$ est un polynôme de degré n
• 1 est un polynôme de degré 0.
Remarque : Nous serons amenés par la suite à additionner des degrés de polynômes. Comme l'application deg est à valeurs dans $\mathbb{N} \cup \{-\infty\}$, il faut étendre la définition de l'addition.
On adopte la convention suivante pour $n \in \mathbb{N} \cup \{-\infty\}$: $-\infty + n = -\infty$.

Définition 60 *Les polynômes ne comportant qu'un seul terme non nul (i.e du type* $P = a_pX^p$*) sont appelés monômes.*

Remarque : Tout polynôme d'après la definition est donc une somme finie de monômes.

Définition 61 *Soit $P = a_pX^p + \cdots + a_0$ avec $a_p \neq 0$ un polynôme. On appelle terme dominant de P le monôme a_pX^p. Si le coefficient a_p du terme dominant est 1, on dit que P est un polynôme unitaire.*

Remarque 12 *On adopte la convention que l'on ne change pas un polynôme P en lui ajoutant un ou plusieurs monômes à coefficients nuls. Par exemple, on ne fera pas la distinction entre $X^4 - X + 1$ et $0X^5 + X^4 + 0X^2 - X + 1$.*

4.2 Opérations sur $\mathbb{k}[X]$

Nous allons munir $\mathbb{k}[X]$ de deux lois internes "+" et "$*$", et d'une loi externe "$\cdot$".
a) Addition de deux polynômes :

Définition 62 *Soit $P = a_nX^n + \cdots + a_0$ et $Q = b_nX^n + \cdots + b_0$ avec $n \in \mathbb{N}$. On définit alors le polynôme $P + Q$ par*

$$P + Q \overset{déf}{=} (a_n + b_n)X^n + \cdots + (a_1 + b_1)X + (a_0 + b_0).$$

Remarque : Dans la définition ci-dessus, il n'est pas restrictif de faire commencer les expressions des polynômes P et Q par un monôme de même degré n (voir la remarque 12 ci-dessus)

Proposition 68 *Soit P et Q deux polynômes de $\mathbb{k}[X]$. Alors on a*

$$deg(P + Q) \leq \ max(degP, degQ).$$

De plus, si $degP \neq degQ$ alors $deg(P + Q) = max(degP, degQ)$.
Preuve : Notons $p = degP$ et $q = degQ$.
– Si $p > q$, le coefficient du terme dominant de $P + Q$ est a_p donc $deg(P + Q) = degP$.
– Si $p < q$, le coefficient du terme dominant de $P + Q$ est b_q donc $deg(P + Q) = degQ$.
– Si $p = q$, le monôme de plus haut degré dans l'expression de $P + Q$ est $(a_p + b_p)X^p$.
Donc $deg(P + Q) \leq \ p$. Si $b_p = -a_p$, ce monôme est nul et l'on a donc $deg(P + Q) < p$.
b) Multiplication de deux polynômes :
Considérons deux monômes $P = a_pX^p$ et $Q = b_qX^q$. Si l'on interprète ces deux monômes comme des fonctions de la variable réelle ou complexe X, il est naturel de définir le produit de P par Q comme étant le monôme $P * Q \overset{déf}{=} a_pb_qX^{p+q}$.
Plus généralement, on définit le produit de deux polynômes de la façon suivante :

Définition 63 *Etant donnés deux polynômes $P = a_pX^p + \cdots + a_0$ et $Q = b_qX^q + \cdots + b_0$,*
on définit le polynôme $P * Q$ par $P * Q = c_rX^r + \cdots + c_0$ avec $r = p + q$ et, pour $k \in \{0, \cdots, r\}$,

$$c_k = \sum_{i+j=k} a_ib_j = \sum_{i=0}^{k} a_ib_{k-i} = \sum_{j=0}^{k} a_{k-j}b_j.$$

Remarque : Si P ou Q est nul, on a donc $P * Q = 0$.

La proposition suivante est une conséquence immédiate de la définition de "$*$" :

Proposition 69 *Soit P et Q deux polynômes de $\mathbb{k}[X]$. Alors on a*

$$deg(P * Q) = degP + degQ.$$

Exemple : Soient $P = X^3 - 3X^2 + 2$ et $Q = X^2 - X + 2$. Il s'agit de calculer le polynôme $P * Q$.

On pourra décomposer un des deux polynômes, par exemple Q, en somme de monômes, donc X^2,$-X$ et 2, puis effectuer chacune des multiplications de P par ces monômes, et enfin tout regrouper. Une présentation claire, en alignant les monômes de mêmes degrés, est une condition nécessaire de calcul sans erreurs.

$$\begin{array}{lccccc} X^2 \times P = & X^5 & -3X^4 & +2X^2 & & \\ -X \times P = & & -X^4 & +3X^3 & -2X & \\ 2 \times P = & & & 2X^3 & -6X^2 & +4 \\ \hline Q * P = P * Q = & X^5 & -4X^4 & +5X^3 & -4X^2 & -2X+4 \end{array}$$

c) Multiplication d'un polynôme par un scalaire :

Définition 64 *Soit $P = a_pX^p + \cdots + a_0$ un polynôme de $\mathbb{k}[X]$, et $\lambda \in \mathbb{k}$. On définit alors le polynôme $\lambda \cdot P$ par*

$$\lambda \cdot P \overset{déf}{=} \sum_{i=0}^{p} \lambda a_i X^i$$

Proposition 70 *Soit P un polynôme et λ un scalaire non nul. Alors $deg(\lambda \cdot P) = \lambda degP$.*

Preuve : evidente

4.3 Propriétés algébriques de $\mathbb{k}[X]$

Proposition 71 *$(\mathbb{k}[X], +, *)$ est un anneau commutatif.*

Preuve : Montrons que $(\mathbb{k}[X], +)$ est un groupe commutatif.

– Le polynôme nul est clairement l'élément neutre pour l'addition.

– Si $P = a_pX^p + \cdots + a_0$, le polynôme $-P \overset{déf}{=} -a_pX^p - \cdots - a_0$ vérifie $P + (-P) = 0$.

– L'associativité et la commutativité résultent de celles de l'addition sur $\mathbb{k}$.

Reste à étudier les propriétés de la multiplication "$*$".

– De la définition de la multiplication sur $\mathbb{k}[X]$, on déduit facilement que le polynôme $P = 1$ est l'élément neutre pour "$*$".

– Commutativité : considérons $P = a_pX^p + \cdots + a_0$ et $Q = b_qX^q + \cdots + b_0$. Notons $r = p + q$, $P * Q = c_rX^r + \cdots + c_0$ et $Q * P = d_rX^r + \cdots + d_0$. Alors on a

$$\forall k \in \{0, \cdots, r\}, c_k = \sum_{i+j=k} a_ib_j = \sum_{i+j=k} b_ja_i = d_k$$

Donc $P * Q = Q * P$.

– Associativité : se verifie sans difficulté

– Distributivité de la multiplication par raport à l'addition : Définissons $P = a_pX^p+\cdots+a_0$, $Q = b_qX^q+\cdots+b_0$ et $R = c_rX^r+\cdots+c_0$

et posons $U \overset{déf}{=} (P+Q)*R$ et $V \overset{déf}{=} P*R+Q*R$. Notons d_l les coefficients de U, et e_m ceux de V . Alors on a

$$d_l = \sum_{i+j=l}(a_i+b_i)c_j = \sum_{i+j=l}(a_ic_j+b_ic_j) = \sum_{i+j=l}a_ic_j + \sum_{i+j=l}b_ic_j = e_l$$

Donc $U = V$.

Coclusion : $(\mathbb{k}[X], +, *)$ est bien un anneau commutatif.

Proposition 72 *$(\mathbb{k}[X], +, *)$ est un anneau intègre. c-à-d $P*Q = 0 \Longrightarrow P = 0$ ou $Q = 0$.*

Preuve : Soit donc (P, Q) tel que $P*Q = 0$. Alors on a $degP+degQ = deg(P*Q) = -\infty$.

Donc $degP$ ou $degQ$ vaut $-\infty$, ce qui est exactement la propriété demandée.

Notations : Dorénavant, on omettra les symboles"$*$" et "$\cdot$". Ainsi PQ désignera $P*Q$, et λP désignera $\lambda\cdot P$.

4.4 Arithmétique dans $\mathbb{k}[X]$

Division euclidienne (Ou division suivant les puissanes décroissantes).

Proposition 73 *Soit A et B deux polynômes tel que $B \neq 0$. Alors il existe un unique couple (Q, R) tels que :*

$$A = BQ + R \quad \text{avec } deg(R) < deg(B)$$

Q est le quotient, R est le reste.

Lorsque le reste est nul, on dit que B divise A.

On notera l'analogie dans l'énoncé avec la division euclidienne dans $\mathbb{Z}$.

Les démonstrations ; en ce qui concerne l'unicité, sont également analogues.

Preuve :

Montrons l'unicité :

Si $A = BQ + R = BQ' + R'$ avec $deg(R) < deg(B)$ et $deg(R') < deg(B)$,

on a $B(Q - Q') = R' - R$; avec $deg(B(Q - Q')) = deg(B) + deg(Q - Q')$ et

$deg(B) + deg(Q - Q') = deg(R - R') \leq Max(deg(R), deg(R')) < deg(B)$.

Ceci n'est possible que si $Q - Q\prime = 0$ et alors $R - R\prime = 0$.

Montrons l'existence :

Supposons que $deg(A) = n$ et $deg(B) = p$

1^{er} cas : si $n < p$ alors on prend $Q = 0$ et $R = A$.

$2^{ème}$cas : si n $\geq$ p.

On procède par récurrence sur le degré n de A .

Supposons que la propriété est vraie jusqu'à n - 1.

Soit $A = a_0 + a_1x + ...a_nx^n$ et $B = b_0 + b_1x + ...b_px^p$

On définit $A' = A - \dfrac{a_n}{b_p}\, x^{n-p}.B$

A' est degré $n-1$ et donc d'après l'hypothèse de récurrence on a :

$A' = BQ' + R'$ avec $deg(R') < deg(B)$

Or $A = A' + \dfrac{a_n}{b_p}x^{n-p}B = BQ' + R' + \dfrac{a_n}{b_p}x^{n-p}B = B\ (Q' + \dfrac{a_n}{b_p}x^{n-p}) + R' = B\ Q + R'$ avec $deg(R') < deg(B)$ C.Q.F.D.

Donnons un exemple :

$$\begin{array}{l|l} 2X^4 + X^3 - X^2 + X + 1 & 2X^2 - X - 2 \\ \underline{2X^4 - X^3 - 2X^2} & \\ \quad 2X^3 + X^2 + X + 1 & \underline{\qquad\qquad} \\ \quad \underline{2X^3 - X^2 - 2X} & X^2 + X + 1 \\ \qquad 2X^2 + 3X + 1 & \\ \qquad \underline{2X^2 - X - 2} & \\ \qquad 4X + 3 & \end{array}$$

Nous avons alors que :

$$\underbrace{2X^4 + X^3 - X^2 + X + 1}_{Dividende} = \underbrace{(2X^2 - X - 2\ )}_{diviseur}\ \underbrace{(X^2 + X + 1\ )}_{quotient} + \underbrace{(4X + 3)}_{Reste}$$

Division des polynômes

Définition 65 *On dit que le polynôme A est divisible par le polynôme B s'il existe un polynôme Q tel que $A = BQ$. Dans ce cas, on note $B \mid A$ et l'on dit que A est multiple de B (ou que B est diviseur de A). Le polynôme Q est parfois noté $\frac{A}{B}$ ou A/B.*

Remarques :

1. Le polynôme nul est divisible par tous les polynômes. En revanche seul le polynôme nul est divisible par le polynôme nul.

2. Dans le cas où A et B sont tous les deux non nuls, $B \mid A$ entraîne $degB \leq degA$.

Proposition 74 *Soit A et B, deux polynômes non nuls. Si $A \mid B$ et $B \mid A$ alors A et B sont proportionnels, c'est-à-dire qu'il existe $\lambda \in \mathbb{k}^*$ tel que $A = \lambda B$. On dit que A et B* ***sont associés.***

Preuve : D'après la remarque ci-dessus, on a à la fois $degA \leq degB$ et $degB \leq deg$A. Donc A et B sont de même degré. Comme $B \mid A$, on en déduit que $A = BQ$ avec $degQ = 0$. Autrement dit Q est un polynôme constant (et non nul car A n'est pas nul).

Remarque 13 *Deux polynômes unitaires associés sont forcément égaux.*

Proposition 75 *Soit B un polynôme non nul, et A un multiple de B de même degré que B. Alors A et B sont associés.*

Preuve : se fait de la même manière que la dernière partie de la proposition précédente.

Notation : Pour $A \in \mathbb{k}[X]$, on note $A\mathbb{k}[X]$ l'ensemble des multiples de A.

Proposition 76 *$A\mathbb{k}[X]$ est un idéal de $\mathbb{k}[X]$. En particulier, le singleton $\{0\}$ est un idéal.*

Preuve : facile

Proposition 77 *Soit A et B deux polynômes. Alors $A \mid B$ si et seulement si $B\mathbb{k}[X] \subset A\mathbb{k}[X]$.*

Preuve : si $P \in B\mathbb{k}[X]$ il existe $Q_1 \in \mathbb{k}[X]/\ P = BQ_1$ Comme $A \mid B$ alors il existe $Q_2 \in \mathbb{k}[X]\ /\ B = AQ_2$ et donc $P = AQ_1Q_2$ ce qui montre que $P \in A\mathbb{k}[X]$.Réciproquement si $B\mathbb{k}[X] \subset A\mathbb{k}[X]$ ceci veut dire que tout multiple de B est un multiple de A . Or B est multiple de lui même et donc multiple de A et donc $A \mid B$.

Proposition 78 *Soit I un idéal de $(\mathbb{k}[X], +, .)$ non réduit à $\{0\}$. Alors il existe un unique polynôme P unitaire tel que $I = P\mathbb{k}[X]$. Le polynôme P est appelé générateur unitaire de I. En d'autres termes $(\mathbb{k}[X]$,+, .) est un idéal principal .*

Preuve : Soit I un idéal de $(\mathbb{k}[X]$,+, .) non réduit à $\{0\}$. On note $E = \{degA \mid A \in I\backslash\{0\}\}$.

L'ensemble E est une partie non vide de $\mathbb{N}$, donc admet un plus petit élément. On en déduit que I contient un polynôme P non nul et de degré minimal. Comme pour tout $\lambda \in \mathbb{k}$, le polynôme λP appartient aussi à I, on peut toujours choisir P unitaire. La stabilité de I par multiplication par les éléments de $\mathbb{k}[X]$ assure que $P\mathbb{k}[X] \subset I$.

Reste à montrer que $I \subset P\mathbb{k}[X]$. Soit donc $A \in I$. Ecrivons la division euclidienne de A par P :

$A = PQ + R$ avec $degR < degP$.

Comme A et PQ appartiennent à I, on a aussi $R \in I$. Mais par ailleurs $degR < degP$.

Vu la définition de P, on conclut que $R = 0$. et donc $A \in P\mathbb{k}[X]$, soit $I \subset P\mathbb{k}[X]$.

4.5 Pgcd et Ppcm

La division euclidienne va nous permettre de définir les notions de PGCD et de PPCM dans l'ensemble des polynômes.

PGCD

Proposition 79 *Soit A et B deux polynômes non tous les deux nuls. L'ensemble $A\mathbb{k}[X] + B\mathbb{k}[X] \overset{déf}{=} \{AP + BQ \mid P \in \mathbb{k}[X], Q \in \mathbb{k}[X]\}$ est un idéal de $\mathbb{k}[X]$ non réduit à $\{0\}$. Son générateur unitaire D est appelé Plus Grand Commun Diviseur (ou plus simplement PGCD) de A et de B, et est noté $PGCD(A, B)$.*

Preuve : Notons $J \overset{déf}{=} A\mathbb{k}[X] + B\mathbb{k}[X]$. Remarquons que J n'est pas réduit à $\{0\}$ car contient A et B, et que l'un de ces deux polynômes n'est pas nul par hypothèse. Reste à montrer que J est un idéal.

1. Montrons que J est un sous-groupe de $(\mathbb{k}[X], +)$:

– Il est évident que $0 \in J$.

– Soit C et C_0 deux polynômes de J. Alors il existe quatre polynômes P, P_0, Q et Q_0 tels que

$$C = AP + BQ \text{ et } C_0 = AP_0 + BQ_0.$$

Donc $C + C_0 = A(P + P_0) + B(Q + Q_0) \in J$.

– Enfin, si $C = AP + BQ$, il est clair que $-C = A(-P) + B(-Q)$, donc $-C \in J$.

2. Stabilité de J par produit :

Soit $C = AP + BQ$ un élément de J, et R un polynôme quelconque. Alors $RC = A(PR) + B(QR)$ donc $RC \in J$.

On conclut que J est un idéal non réduit à $\{0\}$. La proposition 78 assure l'existence d'un unique polynôme unitaire D tel que $A\mathbb{k}[X] + B\mathbb{k}[X] = \mathrm{D}\mathbb{k}[X]$.

Remarque : On convient que $\mathrm{PGCD}(0, 0) = 0$. Pour tout couple de polynômes (A, B), on a donc $A\mathbb{k}[X] + B\mathbb{k}[X] = PGCD(A, B)\mathbb{k}[X]$.

La proposition suivante justifie l'appellation "PGCD" donnée au générateur unitaire de $A\mathbb{k}[X] + B\mathbb{k}[X]$.

Proposition 80 *Soit (A, B) un couple de polynômes distinct de $(0, 0)$. Alors $PGCD(A, B)$ est l'unique polynôme unitaire vérifiant*

$$(1)\ PGCD(A, B) \mid A,\ PGCD(A, B) \mid B \ \text{ et } \ (P \mid A \text{ et } P \mid B) \Longrightarrow P \mid PGCD(A, B).$$

Preuve : Notons $D = PGCD(A, B)$ et montrons que D vérifie (1).

Par définition, $D\mathbb{k}[X] = A\mathbb{k}[X] + B\mathbb{k}[X]$. Comme A et B appartiennent tous les deux à l'ensemble de droite, A et B sont bien des multiples de D. Enfin, si P divise A et B alors, d'après la proposition 77, $A\mathbb{k}[X] \subset P\mathbb{k}[X]$ et $B\mathbb{k}[X] \subset P\mathbb{k}[X]$. Donc $D\mathbb{k}[X] = A\mathbb{k}[X] + B\mathbb{k}[X] \subset P\mathbb{k}[X]$. Donc P divise D (cf prop 77)

Pour montrer l'unicité, considérons un polynôme D' unitaire vérifiant (1). On a donc en particulier $D \mid D'$. Mais bien sûr $D' \mid D$ donc D et D' sont associés (cf prop. 74).

Comme D et D' sont unitaires, on a $D = D'$.

Proposition 81 *Si A et B ne sont pas simultanément nuls et si C est unitaire alors on a*

$$PGCD(AC, BC) = C.PGCD(A, B).$$

Preuve : Notons $D = PGCD(A, B)$ et $\Delta = PGCD(AC, BC)$. On a :

$\Delta\mathbb{k}[X] = AC\mathbb{k}[X] + BC\mathbb{k}[X] = C(A\mathbb{k}[X] + B\mathbb{k}[X]) = CD\mathbb{k}[X]$.

$\Delta\mathbb{k}[X] \subset CD\mathbb{k}[X] \Longrightarrow CD \mid \Delta$

$CD\mathbb{k}[X] \subset \Delta\mathbb{k}[X] \Longrightarrow \Delta \mid CD$

$CD \mid \Delta$ et $\Delta \mid CD$ donc CD et Δ sont associés mais comme ils sont unitaires donc ils sont égaux.

Définition 66 *On dit que deux polynômes A et B sont premiers entre eux si leur PGCD vaut* 1.

Définition 67 *Soit $n \geq 1$ un entier. On dira que n polynômes de $\mathbb{k}[X]$ sont premiers entre eux lorsque leurs seuls diviseurs communs sont constants (en d'autres termes, quand leur pgcd est* 1*).*

On prendra garde à ne pas confondre « premiers entre eux » (on dit parfois « premiers entre eux dans leur ensemble ») et « deux à deux premiers entre eux » : dans $\mathbb{R}[X]$, les polynômes $(X-1)(X-2), (X-1)(X-3), (X-2)(X-3)$ sont premiers entre eux (dans leur ensemble) mais ils ne sont pas deux à deux premiers entre eux !.

Proposition 82 *(Théorème de Bezout). Deux polynômes A et B sont premiers entre eux si et seulement si il existe deux polynômes U et V tels que*

$$AU + BV = 1.$$

Preuve : Si $PGCD(A, B) = 1$ alors par définition du PGCD, on a $A\mathbb{k}[X] + B\mathbb{k}[X] = \mathbb{k}[X]$. Donc $1 \in A\mathbb{k}[X] + B\mathbb{k}[X]$, ce qui signifie qu'il existe U et V tels que $AU + BV = 1$.

Réciproquement Si $AU + BV = 1$ alors $1 \in A\mathbb{k}[X] + B\mathbb{k}[X]$. Le générateur unitaire de $A\mathbb{k}[X]+B\mathbb{k}[X]$ est donc un diviseur de 1, donc 1 lui-même. On a donc bien $PGCD(A, B) = 1$.

Proposition 83 *Pour que le polynôme unitaire D soit le PGCD de A et de B, il faut et il suffit que :*

$$(2)\ D \mid A,\ D \mid B \text{ et } PGCD(\frac{A}{D}, \frac{B}{D}) = 1$$

Preuve : Si $D = PGCD(A, B)$, on a bien sûr $D \mid A$ et $D \mid B$. Notons $P = \dfrac{A}{D}$ et $Q = \dfrac{B}{D}$. D'après la proposition 81, on a

$$D = PGCD(A, B) = PGCD(DP, DQ) = D.PGCD(P, Q).$$

Comme D n'est pas nul, on conclut que $PGCD(P, Q) = 1$.

Réciproquement, supposons que (2) soit satisfaite. Alors, la proposition 81 entraîne

$$PGCD(A, B) = PGCD(D\frac{A}{D}, D\frac{B}{D}) = DPGCD(\frac{A}{D}, \frac{B}{D}) = D.$$

Proposition 84 *(Théorème de Bezout généralisé) Supposons que D est unitaire et divise A et B avec A et B non tous les deux nuls. Alors on a*

$$D = PGCD(A, B) \Leftrightarrow \exists U \in \mathbb{k}[X], \exists V \in \mathbb{k}[X],\ AU + BV = D.$$

Preuve : En appliquant la proposition 83, on a

$$D = PGCD(A, B) \Leftrightarrow 1 = PGCD(\frac{A}{D}, \frac{B}{D})$$

Or d'après le théorème de Bezout, on a

$$PGCD(\frac{A}{D}, \frac{B}{D}) = 1 \Leftrightarrow \exists U \in \Bbbk[X], \exists V \in \Bbbk[X],\ \tfrac{A}{D}U + \tfrac{B}{D}V = 1$$

ce qui achève la preuve du théorème.

Proposition 85 *(Théorème de Gauss) Si P divise AB et si P est premier avec A alors P divise B.*

Preuve : Soit B' le polynôme unitaire associé à B. On a

$$PGCD(PB, AB) = B'PGCD(P, A) = B'.$$

Par hypothèse, P divise AB, et P divise aussi PB. Donc P divise B' et, donc divise, B.

Proposition 86 *Un polynôme P est premier avec un produit AB si et seulement si P est premier avec A et avec B.*

Preuve : Supposons P premier avec AB. Soit P' divisant P et A. Alors P' divise aussi AB. Donc $P' \mid PGCD(AB, P)$, i.e $P' \mid 1$. On en déduit que P' est un polynôme constant. Donc P est premier avec A. On établit de même que P est premier avec B.

On prouve la réciproque par contraposition. Supposons que P ne soit pas premier avec AB. Alors il existe P' divisant P et AB, et tel que $\deg P' \geq 1$. Si P est premier avec A alors P' l'est également. D'après le théorème de Gauss, P' divise donc B. On a donc montré que P' divise à la fois P et B. Comme $\deg P' \geq 1$, cela signifie que P et B ne sont pas premiers entre eux.

Remarque 14 *Une récurrence élémentaire permet de montrer plus généralement qu'un polynôme P est premier avec un produit de polynômes $A_1 \cdots A_k$ si et seulement si il est premier avec chacun des facteurs A_i.*

PPCM

Proposition 87 *Considérons deux polynômes non nuls A et B. Alors l'ensemble $AK[X] \cap BK[X]$ est un idéal non réduit à $\{0\}$. Son générateur unitaire est appelé Plus Petit Commun Multiple (ou plus simplement PPCM) de A et B. On le note $PPCM(A, B)$.*

Preuve : $AK[X]$ est un idéal, de même que $BK[X]$ et on sait déjà que l'intersection de deux idéaux est un idéal. L'existence du générateur unitaire est assurée par la proposition 78.

Remarque : Si A ou B est nul, on a $AK[X] \cap BK[X] = \{0\}$. On adopte alors la convention que $PPCM(A, B) = 0$. Ainsi, on aura toujours $AK[X] \cap BK[X] = PPCM(A, B)K[X]$.

En s'inspirant de la preuve de la proposition 80, on obtient le résultat suivant qui explique l'appellation "Plus Petit Commun Multiple" donnée au générateur unitaire de $AK[X] \cap BK[X]$.

Proposition 88 *Soit A et B deux polynômes non nuls. Le PPCM de A et de B est l'unique polynôme unitaire vérifiant la propriété suivante :*

$$A \mid PPCM(A,B),\ \ B \mid PPCM(A,B) \text{ et } (A \mid M \text{ et } B \mid M) \Longrightarrow PPCM(A,B) \mid M.$$

A certains égards, le PPCM et le PGCD ont des propriétés très similaires. On a par exemple :

Proposition 89 *Soit C un polynôme unitaire et A, B deux polynômes. Alors on a*

$$PPCM(AC,BC) = C.PPCM(A,B).$$

Preuve : Il suffit de remarquer que $ACK[X] \cap BCK[X] = C(AK[X] \cap BK[X])$.

Proposition 90 *Soit A et B deux polynômes non nuls. Pour que M unitaire soit le PPCM de A et de B, il faut et il suffit que :*

$$A \mid M, B \mid M \ \text{ et } \ PGCD(\frac{M}{A}, \frac{M}{B}) = 1$$

Preuve : Notons M le PPCM de A et de B. Alors $MK[X]$ est inclus dans $AK[X]$ et dans $BK[X]$. Donc M divise bien A et B. Soit D unitaire divisant $\frac{M}{A}$ et $\frac{M}{B}$.

Alors $AD \mid M$ et $BD \mid M$. Donc $PPCM(AD,BD) \mid M$. Mais d'après la proposition 89, $PPCM(AD,BD) = D.PPCM(A,B) = DM$. Donc $D = 1$.

Réciproquement, soit M un multiple commun unitaire de A et de B vérifiant de plus $PGCD(\frac{M}{A}, \frac{M}{B}) = 1$

D'après le théorème de Bezout, il existe deux polynômes U et V tels que

$$\frac{M}{A}U + \frac{M}{B}V = 1$$

Multiplions les deux membres de cette égalité par $PPCM(A,B)$. On trouve

$$M(\frac{PPCM(A,B)}{A}U + \frac{PPCM(A,B)}{B}V) = PPCM(A,B)$$

Donc M divise $PPCM(A,B)$. Comme M est unitaire et est multiple de A et de B, on conclut que $M = PPCM(A,B)$.

Proposition 91 *Soient A et B deux polynômes. Il existe une constante λ non nulle telle que :*

$$(3) \quad \lambda AB = PGCD(A,B)PPCM(A,B).$$

– Si de plus A et B sont unitaires, alors $\lambda = 1$.

– Si A et B sont premiers entre eux alors AB et $PPCM(A,B)$ sont associés.

Preuve : écartons le cas évident où l'un des deux polynômes A et B est nul. On peut alors appliquer la proposition 90. On en déduit que

$$PGCD(\frac{PPCM(A,B)}{A}, \frac{PPCM(A,B)}{B}) = 1$$

Notons λ l'inverse du coefficient du terme dominant de AB. Alors λAB est unitaire, et la proposition 89 combinée avec (3) montre que

$$PGCD(\lambda AB(\frac{PPCM(A,B)}{A}), \lambda AB(\frac{PPCM(A,B)}{B})) = \lambda AB$$

En appliquant la proposition 81, on constate que le membre de gauche de cette égalité vaut $PPCM(A,B).PGCD(A,B)$.

4.6 L'Algorithme d'Euclide

L'algorithme d'Euclide est un moyen systématique permettant de calculer le PGCD de deux polynômes. L'outil de base est la division euclidienne. L'algorithme repose sur le lemme suivant :

Lemme 92 *Soit B un polynôme non nul, et A un polynôme quelconque. Notons Q et R le quotient et le reste de la division euclidienne de A par B. Alors on a :*

$$PGCD(A,B) = PGCD(B,R).$$

Preuve : Soit D divisant A et B. Comme $R = A - BQ$, le polynôme D divise aussi R. Donc D divise $PGCD(B,R)$. En choisissant $D = PGCD(A,B)$, on conclut que $PGCD(A,B) \mid PGCD(B,R)$.

Soit maintenant D un polynôme divisant B et R. Comme $A = BQ + R$, on a aussi $D \mid A$.

Donc $D \mid PGCD(A,B)$. On a donc finalement $PGCD(B,R) \mid PGCD(A,B)$.

Les deux polynômes $PGCD(B,R)$ et $PGCD(A,B)$ sont unitaires et associés. Ils sont donc égaux.

Remarque : Les divseurs communs à A et 0 sont les diviseurs de A.

Algorithme d'Euclide

Le lemme précédent indique clairement la stratégie à suivre pour calculer $PGCD(A,B)$. Quitte à permuter A et B, on peut toujours supposer que $degA \geq degB$. On procède alors comme suit :

• Si $B = 0$, il n'y a rien à faire : $PGCD(A,B)$ est égal au polynôme unitaire associé à A.

• Si B n'est pas nul, on effectue la division euclidienne de A par B, ce qui donne deux polynômes Q_0 et R_1 tels que $A = BQ_0 + R_1$ et $degR1 < degB$.

Le lemme 92 montre que $PGCD(A,B) = PGCD(B,R_1)$. On reprend le calcul ci-dessus en remplaçant A par B, et B par R_1. En itérant le procédé, on construit deux suites $R_1, R_2, \cdots$ et $Q_0, Q_1, \cdots$ telles que :

$A = BQ_0 + R_1$ avec $degR_1 < degB$,
$B = R_1Q_1 + R_2$ avec $degR_2 < degR_1$,
$R_1 = R_2Q_2 + R_3$ avec $degR_3 < degR_2$,
. . . . . .

$R_{k-1} = R_kQ_k + R_{k+1}$ avec $degR_{k+1} < degR_k$,
. . . . . .
$R_{n-1} = R_nQ_n + 0$.

Le procédé s'arrête nécessairement au bout d'au plus $degB$ étapes car chaque itération diminue d'au moins 1 le degré du reste de la division euclidienne. On a donc finalement

$$PGCD(A,B) = PGCD(B,R_1) =\cdot\cdot = PGCD(R_k,R_{k+1}) =\cdot\cdot = PGCD(R_n,0) = R_n'.$$

où R_n' est le polynôme unitaire associé à R_n.

Exemple1 : Calculer le PGCD de $x^3 + 2x^2 - \ x - \ 2$ et de $x^2 + 4x + 3$
On a :
$x^3 + 2x^2 - \ x - \ 2 = (x^2 + 4x + 3)(x - \ 2) + 4x + 4$
$x^2 + 4x + 3 = (4x + 4)(\frac{x}{4} + \frac{3}{4}) + 0$
Le PGCD est $x + 1$
Exemple2 : Calculer PGCD$(X^4 - 1, X^3 - 1)$.
Posons la division euclidienne de $X^4 - 1$ par $X^3 - 1$.
$X^4 - 1 = (X^3 - 1)X + (X - 1)$
$(X^3 - 1) = (X - 1)(X^2 + X + 1) + 0$
Donc PGCD$(X^4 - 1, X^3 - 1) = X - 1$.

4.7 Polynôme et fonction polynomiale associée

Jusqu'à présent, nous avons traité les polynômes comme des objets algébriques "abstraits". Ce point de vue permet de manipuler de façon unifiée des objets mathématiques très différents dès lors qu'ils peuvent être interprétés comme des polynômes. Dans cette section, nous allons nous borner à remplacer la variable muette X par des nombres réels ou complexes. Mais la notion de polynôme est beaucoup plus large et que l'on peut fort bien remplacer X par une matrice...

Définition 68 *Soit $P = a_nX^n+\cdots+a_1X + a_0$ un polynôme de $\Bbbk[X]$, et $t \in \Bbbk$. On définit alors l'élément $P(t)$ de $\Bbbk$ par*

$$P(t) = a_nt^n+\cdots+a_1t + a_0.$$

On dit que $P(t)$ est obtenu par substitution de t à X.

Définition 69 *Soit $P \in \Bbbk[X]$. L'application*
$P : \Bbbk \longrightarrow \Bbbk$
$\quad t \longrightarrow a_nt^n + \cdots + a_1t + a_0 = P(t)$
est appelée fonction polynôme associée à P sur K.

Remarque : le polynôme $P(X)$ est, par construction nul si et seulement si tous ses coefficients sont nuls $(*)$
alors que la fonction polynômiale associée :
$P : \Bbbk \longrightarrow \Bbbk \quad x \longrightarrow a_0+a_1x+...a_nx^n = P(x)$ est nulle si et seulement si : $\forall x \in \Bbbk; P(x) = 0$
On a bien évidemment l'implication :

$$P(X) = 0 \Longrightarrow \forall x \in \Bbbk; P(x) = 0 :$$

Mais la réciproque est loin d'être évidente. Nous allons montrer que, lorsque $\Bbbk$ est égal à $\mathbb{R}$ ou $\mathbb{C}$, il y a équivalence, ce qui permet de confondre polynôme et fonction polynômiale. La phrase $P = 0$ gardera cependant de préférence le sens $(*)$.

Proposition 93 *i) Soit P un polynôme à coefficients dans $\mathbb{R}$ ou $\mathbb{C}$. Alors si la fonction polynômiale associée à P est identiquement nulle. P a tous ses coefficients nuls.*

ii) Soient P et Q deux polynômes dans $\mathbb{R}$ ou C. Alors, si les fonctions polynomiales associées sont égales (prennent les mêmes valeurs), les deux polynômes sont égaux (leurs coefficients sont égaux).

Preuve :

i) $\Bbbk$ contenant $\mathbb{R}$, nous supposons que la variable x ne prend que des valeurs dans $\mathbb{R}$. Soit $P = \sum_{k\geq 0} a_k X^k$ tel que $\forall\ x \in \Bbbk\,;\ P(x) = 0$

Alors, pour $x = 0$, on obtient $a_0 = 0$. Donc : $\forall x \in \mathbb{R}, a_1 x + ...a_n x_n = 0$

Donc $\forall\ x \neq 0$, $a_1 + ...a_n x^{n-1} = 0$

On ne peut plus prendre $x = 0$, cependant, on peut prendre la limite lorsque x tend vers 0, ce qui donne $a_1 = 0$, etc...

ii) se prouve en appliquant i) à $P - Q$.

Remarque : Dans la suite du cours, on ne fera plus la distinction entre le polynôme P qui est un objet algébrique et la fonction polynôme qui lui est associée.

4.8 Racines d'un polynôme

Définition 70 *On dit que a, élément de $\Bbbk$, est un zéro ou une racine du polynôme P si a annule la fonction polynômiale associée à P, c'est à dire $P(a) = 0$.*

Remarque : En toute précision il faudrait dire que a est racine du polynôme P ou que a est un zéro de la fonction polynôme associée à P, mais par abus on dit que a est un zéro du polynome P.

On a alors le résultat suivant :

Proposition 94 *a est un zéro de P si et seulement si P est divisible par $X - a$.*

Preuve :

Si P est divisible par $X - a$, alors il existe Q tel que $P(X) = (X - a)Q(X)$. On a alors $P(a) = 0$.

Réciproquement, si $P(a) = 0$, considérons la division euclidienne de P par $X - a$. On a :

$P(X) = (X - a)Q(X) + R$ avec $deg(R) < deg(X - a) = 1$, donc R est une constante. On obtient alors $0 = P(a) = R$ donc $R = 0$ et P est divisible par $X - a$.

Définition 71 *Soit $P \in \mathbb{k}[X]$, $a \in \mathbb{k}$ et $k \in \mathbb{N}^*$. On dit que a est racine de P de multiplicité k si $(X-a)^k \mid P$ et $(X-a)^{k+1} \nmid P$*

– *Si $k = 1$, on parle de racine simple,*

– *Si $k = 2$, on dit que a est racine double,*

– *Si $k = 3$, on dit que a est racine triple, etc.*

Proposition 95 *Soit P un polynôme non nul admettant les racines $a_1, ...a_k$ avec multiplicités respectives $\alpha_1, \cdots, \alpha_k$ Alors $\prod_{i=1}^{k}(X-a_i)^{\alpha_i}$ divise P.*

Preuve : Par récurrence sur le produit

· On sait déjà que $(X-a_1)^{\alpha_1}$ divise P.

· Supposons que $\prod_{i=1}^{j-1}(X-a_i)^{\alpha_i}$ divise P (avec $j \leq k$). Comme les a_i sont deux à deux distincts, les polynômes $(X-a_i)^{\alpha_i}$ sont premiers entre eux deux à deux. La remarque 14 permet donc d'affirmer que $(X-a_j)^{\alpha_j}$ est premier avec $\prod_{i=1}^{j-1}(X-a_i)^{\alpha_i}$. Comme P est multiple de $(X-a_j)^{\alpha_j}$ par hypothèse, et de $\prod_{i=1}^{j-1}(X-a_i)^{\alpha_i}$, P est également multiple du PPCM de ces deux polynômes qui, d'après la proposition 91, vaut $\prod_{i=1}^{j}(X-a_i)^{\alpha_i}$.

Nous venons donc de montrer par récurrence sur j que $\prod_{i=1}^{k}(X-a_i)^{\alpha_i}$ divise P

Remarque : En particulier, si $P \neq 0$, toutes les racines de P sont de multiplicité inférieure ou égale à deg P.

Proposition 96 *Un polynôme de degré $n \in \mathbb{N}$ admet au plus n racines comptées avec leur ordre de multiplicité : Si $\{a_1, \cdots, a_k\}$ est l'ensemble des racines de P, et α_i est la multiplicité de a_i, alors on a $\alpha_1 + \cdots + \alpha_k \leq n$.*

Preuve : D'après la proposition 95, on a $\prod_{i=1}^{k}(X-a_i)^{\alpha_i}$ divise P. Donc $\sum_{i=1}^{k}\deg(X-a_i)^{\alpha_i} \leq$ deg P.

Le membre de gauche vaut $\sum_{i=1}^{k}\alpha_i$, d'où le résultat.

Remarque : Le seul polynôme ayant une infinité de racines est le polynôme nul.

4.9 Polynôme Dérivé

On définit le polynôme dérivé de $P = \sum_{k\geq 0} a_k X^k$ comme étant égal à $P' = \sum_{k\geq 1} k a_k X^{k-1}$.

On peut définir de la même façon les dérivées successives.

Proposition 97 *Soient P et Q deux polynômes, et $\lambda \in \mathbb{k}$.*

1. Si *deg* $P > 0$ alors $degP' = degP - 1$,
2. Si P est constant alors $P' = 0$,
3. $(P+Q)' = P' + Q'$,
4. $(\lambda P)' = \lambda P'$,
5. $(PQ)' = P'Q + PQ'$.

Preuve : Les quatre premiers points sont évidents. le cinquième est laissé en exercice.

Proposition 98 *On a* $(X^k)^{(n)} = A_k^n X^{k-n}$ *avec* $A_k^n = n!C_k^n$

où $(X^k)^{(n)}$ est la dérivée n^{ème} de X^k
La démonstration se fait facilement par récurrence sur n.

4.10 Formules de Mac-Laurin et de Taylor pour un polynôme

Proposition 99 *(Formule de Mac-Laurin)*
Soit $P \in \mathbb{k}_n[X]$, *alors*

$$P(X) = \sum_{k=0}^{n} \frac{P^k(0)}{k!} X^k$$

Démonstration :

Soit $P = \sum_{k=0}^{n} a_k X^k$

Pour tout entier j, $P^{(j)} = \sum_{k=0}^{n} a_k (X^k)^{(j)} = \sum_{k=j}^{n} a_k A_k^j X^{k-j}$

Par suite, pour tout $j = 0, 1, ..., n$, on a $P^{(j)}(0) = a_j A_j^j = a_j j!$

et donc $a_j = \frac{P^{(j)}(0)}{j!}$

Par conséquent $P = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!} X^k$.

Proposition 100 *(Formule de Taylor)*
Soit $P \in K_n[X]$ *et* $a \in \mathbb{k}$, *alors* $P = \sum_{k=o}^{n} \frac{P^{(k)}(a)}{k!} (X-a)^k$

Démonstration :

Il suffit d'appliquer la formule de Mac-Laurin au polynôme $P(X+a)$, on trouve :

$$P(X+a) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} X^k$$

On obtient la formule souhaitée en substituant $X - a$ à X.

Proposition 101 *Les propositions suivantes sont équivalentes :*
i) P est divisible par $(X-a)^k$ *et pas par* $(X-a)^{k+1}$ *(a est une racine de multiplicité k de P)*
ii) il existe Q tel que $Q(a) \neq 0$ *et* $P = (X-a)^k Q$
iii) $P(a) = P'(a) = ... = P^{k-1}(a) = 0$ *et* $P^{(k)}(a) \neq 0$

Démonstration :

i) $\Longrightarrow$ii)

Si P est divisible par $(X-a)^k$, il existe Q tel que $P=(X-a)^kQ$. Si on avait $Q(a)=0$, alors Q pourrait se factoriser par $X-a$ et P serait divisible par $(X-a)^{k+1}$.

ii) $\Longrightarrow$iii)

Si $P=(X-a)^kQ$ avec $Q(a)\neq 0$, alors, on a, pour i compris entre 0 et k

$$P^{(i)}(X)=(X-a)^{k-i}Q_i(X) \text{ avec } Q_i(a)\neq 0$$

Ce résultat se montre aisément par récurrence. Il est vrai pour $i=0$,

Suposons qu'il est vrai pour $i<k$, alors :

$$\begin{aligned} P^{(i+1)}(X) &= (k-i)(X-a)^{k-i-1}Q_i(X)+(X-a)^{k-i}Q_i'(X) \\ &= (X-a)^{k-i-1}Q_{i+1}(X) \quad \text{avec } Q_{i+1}(X)=(k-i)Q_i(X)+(X-a)Q_i'(X) \end{aligned}$$

On a bien $P^{(i)}(a)=0$ pour $0\leq i\leq k-1$, et $P^{(k)}(a)=Q_k(a)\neq 0$.

iii) $\Longrightarrow$i)

On applique la formule de Taylor et on factorise par $(X-a)^k$. Comme $P(a)=P'(a)=$

$...=P^{k-1}(a)=0$ et $P^{(k)}(a)\neq 0$ on a :

$$P(X)=\sum_{i=k}^{n}\frac{P^{(i)}(a)}{i!}(X-a)^i=(X-a)^k\left[\sum_{i=k}^{n}\frac{P^{(i)}(a)}{i!}(X-a)^{i-k}\right]$$

Donc P est divisible par $(X-a)^k$ et pas par $(X-a)^{k+1}$(le terme entre crochet n'est pas divisible par $(X-a)$)

4.11 Polynômes irréductibles

Au cours des sections qui précédent, on a pu constater que l'ensemble $\mathbb{k}[X]$ avait beaucoup de similarités avec l'ensemble $\mathbb{Z}$ des entiers relatifs : les deux ensembles sont des anneaux principaux intègres sur lesquels on peut définir la division euclidienne, le PGCD et le PPCM. Dans cette section, nous allons introduire une classe de polynômes qui jouent dans $\mathbb{k}[X]$ le même rôle que les nombres premiers dans $\mathbb{Z}$: les polynômes irréductibles.

Définition 72 *On dit qu'un polynôme P est irréductible si ses seuls diviseurs sont les constantes et les polynômes qui lui sont associés.*

Remarques :

1. A la différence des nombres premiers, les polynômes irréductibles ont une infinité de diviseurs. Mais on notera que ces diviseurs sont triviaux !

2. Tout polynôme de degré 1 est irréductible. En effet, soit P de degré 1, et Q un diviseur de P. Alors $degQ\in\{0,1\}$. Si $degQ=0$ alors Q est une constante, si $degQ=1$ alors $degQ=degP$ donc P et Q sont associés.

La proposition suivante constitue une "loi du tout ou rien" pour la division par les polynômes

irréductibles.

Proposition 102 *Soit A un polynôme et P un polynôme irréductible ne divisant pas A. Alors P est premier avec A.*

Preuve : Soit B un diviseur commun de A et de P. Comme P est irréductible, B doit être constant, ou associé à P. Le deuxième cas est exclus car on a supposé que P ne divisait pas A. Donc B est constant. On a donc bien $PGCD(A, P) = 1$.

De même que tout entier possède une décomposition en facteurs premiers, tout polynôme a une décomposition en facteurs irréductibles.

Proposition 103 *(Théorème de décomposition en facteurs irréductibles) Soit P un polynôme non constant. Alors il existe un entier $k \geq 1$, k entiers $\alpha_1, \cdots, \alpha_k$ non nuls, k polynômes irréductibles unitaires $P_1, \cdots, P_k$ deux à deux distincts, et $\lambda \in \mathbb{k}\backslash\{0\}$ tels que :*

$$P = \lambda \prod_{i=1}^{k} P_i^{\alpha_i}$$

Cette décomposition, appelée décomposition en facteurs irréductibles, est unique à l'ordre des facteurs près.

Preuve : On prouve d'abord l'existence puis l'unicité à l'ordre des facteurs près.

Existence : Elle se fait par récurrence sur le degré de P.

– Si deg $P = 1$ alors P est irréductible. On pose $k = 1$, $\alpha_1 = 1$ et l'on prend pour P_1 le polynôme unitaire associé à P. Il est de degré 1 donc irréductible.

– Supposons maintenant que le théorème de décomposition soit vrai pour tout polynôme de degré compris entre 1 et n.

Soit P de degré $n + 1$ et $P' \overset{déf}{=} P/\lambda$ avec λ coefficient du terme dominant de P. Le polynôme P' est unitaire et de degré $n + 1$. S'il est irréductible, $P = \lambda P'$ constitue une décomposition de P en facteurs premiers. Sinon, il existe un polynôme A unitaire de degré compris entre 1 et n et divisant P'. On a donc $P' = AB$ avec A et B unitaires et de degré compris entre 1 et n. D'après l'hypothèse de récurrence, A et B admettent chacun une décomposition en facteurs premiers : $A = \prod_{i=1}^{k} A_i^{\alpha_i}$ et $B = \prod_{i=1}^{l} B_i^{\beta_i}$

$$\text{Donc } P = \lambda(\prod_{i=1}^{k} A_i^{\alpha_i})(\prod_{i=1}^{l} B_i^{\beta_i})$$

Il ne reste plus qu'à renuméroter les facteurs de la décomposition pour obtenir le résultat voulu.

Unicité : Supposons que P admette deux décompositions en facteurs irréductibles :

$$P = \lambda \prod_{i=1}^{k} P_i^{\alpha_i} = \eta \prod_{i=1}^{l} Q_i^{\beta_i}$$

Comme tous les facteurs irréductibles sont unitaires, λ et η sont égaux au coefficient du terme dominant de P. Donc $\lambda = \eta$. De ce fait, on a

$$(4) \prod_{i=1}^{k} P_i^{\alpha_i} = \prod_{i=1}^{l} Q_i^{\beta_i}$$

Par ailleurs, P_1 divise le produit de droite. De la remarque 14, on déduit que P_1 n'est pas premier avec au moins un des Q_j : il existe j_1 tel que Qj_1 et P_1 ne soient pas premiers entre eux. Comme par ailleurs Qj_1 et P_1 sont irréductibles et unitaires, cela signifie que $P_1 = Qj_1$. En vertu du caractère intègre de $\mathbb{k}[X]$, on peut donc simplifier l'expression (4) par P_1. On itère ce procédé et en $\alpha_1+\cdots+\alpha_k$ étapes, on parvient à une expression du type $1 = \prod_{j=1}^{l} Q_j^{\beta_j'}$ avec $\beta_j' = \beta_j - \alpha_j$. Cela permet de conclure que tous les β_j' sont nuls. Donc les deux décompositions sont identiques à l'ordre près des facteurs.

4.12 Le théorème fondamental de l'algèbre

Définition 73 *On dit qu'un polynôme non constant est scindé si la somme des ordres de multiplicité de ses racines est égal à son degré.*

Remarque : Autrement dit, P de degré n est scindé si et seulement si il existe un n-uplet $(\lambda_1,\cdots,\lambda_n)$ de $\mathbb{k}^n$ tel que P soit associé à $(X-\lambda_1)\cdots(X-\lambda_n)$. c-à-d $P(X) = \lambda\prod_{i=1}^{n}(X-\lambda_i)$ ou encore que P admet exactement n racines comptées avec leur degré de multiplicité.

Proposition 104 *Soit P un polynôme scindé unitaire d'expression $X^n + a_{n-1}X^{n-1}+\cdots+a_0$.*

Notons λ_i ses racines comptées avec leur ordre de multiplicité. Alors on a les relations suivantes entre les racines et les coefficients :

$$a_0 = (-1)^n \prod_{i=1}^{n} \lambda_i \text{ et } a_{n-1} = -\sum_{i=1}^{n} \lambda_i$$

Preuve : On développe l'expression $(X-\lambda_1)\cdots(X-\lambda_n)$ et on identifie les termes du développement avec ceux de l'expression $X^n + a_{n-1}X^{n-1}+\cdots+a_0$

Remarque : Dans le cas où $P = X^2 + a_1X + a_0$ a pour racines λ_1 et λ_2, on retrouve les relations $a_0 = \lambda_1\lambda_2$ et $a_1 = -(\lambda_1+\lambda_2)$.

Le très important résultat suivant est connu sous le nom de théorème fondamental de l'algèbre ou théorème de d'Alembert-Gauss. Il en existe de nombreuses preuves, mais toutes dépassent le cadre du programme.

Theorem 105 *Théorème fondamental de l'algèbre (Théorème de D'Alembert) Tout polynôme de $\mathbb{C}[X]$ est scindé.*

Remarque : On a vu que toutes les équations de degré 2 avaient deux solutions (éventuellement confondues) dans $\mathbb{C}$. Le théorème fondamental exprime que toute équation de degré n admet n solutions (éventuellement confondues) dans $\mathbb{C}$. Dans le cas $n = 3$ ou 4, il existe des formules (assez compliquées) donnant les solutions en fonction des coefficients. Pour une équation de degré supérieur ou égal à 5, il a été prouvé par un jeune mathématicien du XIX ^{ème} siècle, E. Galois, que de telles formules n'existent pas !.

Polynômes irréductibles de $\mathbb{C}[X]$

Proposition 106 *Un polynôme P est irréductible dans $\mathbb{C}$ si et seulement si $degP = 1$.*

Preuve : On a déjà vu que tout polynôme de degré 1 était irréductible (que ce soit dans $\mathbb{C}$ ou dans $\mathbb{R}$).

Pour montrer la réciproque, donnons-nous un polynôme P de degré au moins 2. Le théorème fondamental de l'algèbre nous dit que P admet au moins une racine λ_1. Donc P est divisible par $X - \lambda_1$. Clairement $X - \lambda_1$ n'est pas constant et n'est pas associé à P car de degré strictement inférieur à 2. Donc P n'est pas irréductible.

En appliquant le théorème général de décomposition en facteurs irréductibles, on en déduit :

Corollaire 107 *Tout polynôme P non nul de $\mathbb{C}[X]$ admet une décomposition en facteurs irréductibles du type suivant :*

$P = \lambda\prod_{i=1}^{k}(X - \lambda_i)^{\alpha_i}$ où $\{\lambda_1,\cdots,\lambda_k\}$ est l'ensemble des racines de P, α_i est la multiplicité de λ_i, et λ est le coefficient du terme dominant de P.

Polynômes irréductibles de $\mathbb{R}[X]$

Dans $\mathbb{R}[X]$, la situation est un peu plus compliquée. On sait d'ores et déjà que tous les polynômes irréductibles ne sont pas de degré 1. Par exemple, X^2+1 ne saurait être réductible dans $\mathbb{R}[X]$ car n'a pas de racine réelle (la fonction polynôme associée est minorée par 1, donc ne s'annule jamais).

On peut cependant dresser une liste de tous les polynômes irréductibles de $\mathbb{R}[X]$:

Proposition 108 *Les polynômes irréductibles de $\mathbb{R}[X]$ sont :*

- *Les polynômes de degré 1,*
- *Les polynômes de degré 2 à discriminant strictement négatif : $P = aX^2 + bX + c$ avec $a \neq 0$ et $\Delta \overset{déf}{=} b^2 - 4ac < 0$.*

La preuve de ce théorème repose sur le lemme suivant :

Lemme 109 *Soit $P = \sum_{i=1}^{k} a_k X^k$ un polynôme de $\mathbb{C}[X]$. Notons $\overline{P} = \sum_{i=1}^{k} \overline{a_k} X^k$ le polynôme conjugué. Alors :*

$$\lambda \text{ est racine de } P \text{ de multiplicité } \alpha \Leftrightarrow \overline{\lambda} \text{ est racine de } \overline{P} \text{ de multiplicité } \alpha.$$

Preuve : Soit λ une racine de P de multiplicité α. Alors il existe un polynôme Q tel que $P = Q(X - \lambda)^\alpha$. En prenant le conjugué de cette expression, on obtient $\overline{P} = \overline{Q}(X - \overline{\lambda})^\alpha$. Donc $\overline{\lambda}$ est racine de $\overline{P}$ de multiplicité $\overline{\alpha} \geq \alpha$.

En échangeant les rôles de P et $\overline{P}$, λ et $\overline{\lambda}$, α et $\overline{\alpha}$, on obtient $\overline{\alpha} \leq \alpha$, d'où le résultat.

Preuve de la proposition 108 :

On sait déjà que les polynômes de degré 1 sont irréductibles.

Soit maintenant $P = aX^2 + bX + c$ à discriminant strictement négatif.

La fonction $t \longrightarrow P(t)$ associée ne s'annule pas sur $\mathbb{R}$ (elle est du signe de a), et donc aucun polynôme de degré 1 ne saurait diviser P.

Par ailleurs, on sait que toute équation de degré 2 à coefficients réels et discriminant positif ou nul admet au moins une solution réelle. Donc les polynômes de degré 2 à discriminant positif ne sont pas irréductibles dans $\mathbb{R}[X]$.

Soit maintenant $P \in \mathbb{R}[X]$ un polynôme de degré ≥ 3. Supposons que P n'ait pas de racine réelle (sinon P n'est pas irréductible dans $\mathbb{R}[X]$). D'après le lemme 109, les racines complexes non réelles de P sont deux à deux conjuguées (avec ordres de multiplicité égaux deux à deux). Le corollaire 107 assure donc l'existence de nombres complexes (non réels) $\mu_1,\cdots,\mu_p$, d'entiers $\alpha_1, \cdots, \alpha_p$, et d'un réel α, tels que

$$P = \alpha \prod_{i=1}^{p} [(X-\mu_i)^{\alpha_i}(X-\overline{\mu_i})^{\alpha_i}]$$

Mais un calcul facile montre que

$$(X-\mu_i)^{\alpha_i}(X-\overline{\mu_i})^{\alpha_i} = (X^2 - 2Re\mu_i X + |\mu_i|^2)^{\alpha i}$$

Donc P est divisible par le polynôme réel $X^2 - 2Re\mu_i X + \mu_i^2$ (de degré 2) et n'est donc pas irréductible.

En reprenant la preuve ci-dessus, on déduit facilement le résultat suivant.

Corollaire 110 *Tout polynôme à coefficients réels admet dans* $\mathbb{R}[X]$ *une décomposition en facteurs irréductibles du type suivant :*

$$P = \lambda \left(\prod_{i=1}^{k} (X-\lambda_i)^{\alpha_i} \right) \left(\prod_{j=1}^{l} (X^2 - 2Re\mu_j X + |\mu_j|^2)^{\beta j} \right)$$

où λ est le coefficient du terme dominant de P, $\{\lambda_1,\cdots,\lambda_k\}$ est l'ensemble des racines réelles de P, α_i, multiplicité de λ_i, et $\{\mu_1,\cdots,\mu_l\}$ est l'ensemble des racines complexes et non réelles de P et β_j , la multiplicité de μ_j.

Exemple : $X^6 - 2X^5 + X^4 + X^2 - 2X + 1$ se factorise sur $\mathbb{R}$ sous la forme :

$$(X-1)^2(X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$$