CHAPITRE 28

POLYNÔMES

Dans tout le chapitre, $(\mathbb{K}, +, .)$ désignera un corps. Le programme se limite au cas où ce corps est $\mathbb{R}$ ou $\mathbb{C}$ (on utilisera éventuellement $\mathbb{Q}$ pour quelques exemples).

28.1 POLYNÔMES À COEFFICIENT DANS $\mathbb{K}$

§1 Construction et axiomes

Définition 1

- Un **polynôme** à coefficients dans $\mathbb{K}$ est une suite $P = (a_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang

$$P = (a_0, a_1, \dots, a_n, 0, 0, \dots, 0, \dots) \in \mathbb{K}^{\mathbb{N}}.$$

  On dit qu'une telle suite est de **support fini** ou qu'elle est **presque nulle**.

- a_k est un élément de $\mathbb{K}$ et s'appelle le **coefficient d'indice** k du polynôme P.

- On note $\mathbf{0} = (0, 0, 0, \dots, 0, \dots)$ le polynôme dont tous les coefficients sont nuls, on dit que $\mathbf{0}$ est le **polynôme nul**.

De la définition de l'égalité de deux applications (ici de $\mathbb{N}$ dans $\mathbb{K}$), il résulte que deux polynômes sont égaux si et seulement si ils ont mêmes coefficients.

Les sous-ensemble de $\mathbb{K}^{\mathbb{N}}$ formé des suites à support fini est noté $\mathbb{K}^{(\mathbb{N})}$. Toutefois, la définition formelle que nous venons de donner permet de définir rigoureusement la notion de polynômes mais elle est très lourde à manipuler. Nous allons donc adopter une notation plus pratique.

Notation

- Le polynôme $P = (a_0, a_1, \dots, a_n, 0, 0, \dots, 0, \dots)$ est noté
$$P(X) = \sum_{n\geq 0} a_n X^n.$$
On appellera respectivement **terme de degré n** et **coefficient de degré n** du polynôme P le **monôme** $a_n X^n \in \mathbb{K}[X]$ et le **coefficient** $a_n \in \mathbb{K}$.
- Un polynôme $\sum_{n\geq 0} a_n X^n$ tel que $a_n = 0$ pour $n \geq 1$ est appelé **polynôme constant** et identifié à l'élément a_0 de $\mathbb{K}$.
- On appelle **indéterminée** le polynôme
$$X = (0, 1, 0, 0, \dots) = (\delta_{1,n})_{n\in\mathbb{N}}.$$

L'ensemble des polynôme à coefficients dans $\mathbb{K}$ se note $\mathbb{K}[X]$.

Il peut arriver que l'on choisisse une autre lettre (généralement majuscule) telle que Y, Z, T... pour désigner l'indéterminée. La notation de l'ensemble des polynômes à coefficients dans $\mathbb{K}$ est alors adaptée en conséquence et devient $\mathbb{K}[Y]$, $\mathbb{K}[Z]$, $\mathbb{K}[T]$...

Exemples 2

La suite $(1, 0, 3, 0, \dots, 0, \dots)$ correspond à $1 + 3X^2$.

La notion d'égalité entre polynômes se déduit de l'égalité entre suites.

Proposition 3

Deux polynômes sont égaux si et seulement si leurs coefficients sont égaux.

$$\sum_{n\geq 0} a_n X^n = \sum_{n\geq 0} b_n X^n \iff \forall n \in \mathbb{N}, a_n = b_n$$
$$\sum_{n\geq 0} a_n X^n = 0 \iff \forall n \in \mathbb{N}, a_n = 0.$$

X est une notation pour un objet particulier (un polynôme), *il ne s'agit ni d'une variable, ni d'une inconnue d'une équation*. L'avantage de cette notation est sa commodité d'emploi pour les opérations mais ne doit pas faire confondre une écriture telle que $aX + b = 0$ avec une équation en X. D'ailleurs,

$$aX + b = 0 \iff (a, b, 0, 0, \dots) = (0, 0, 0, 0, \dots) \iff a = 0 \text{ et } b = 0.$$

De même, dans aucun cas on pourra écrire une égalité $X = \lambda$ avec $\lambda \in \mathbb{K}$.

Définition 4

Soit $\lambda \in \mathbb{K}$ et soient P et Q deux polynômes à coefficients dans $\mathbb{K}$
$$P = \sum_{n\geq 0} a_n X^n \quad \text{et} \quad Q = \sum_{n\geq 0} b_n X^n.$$

- On appelle **somme des polynômes P et Q** le polynôme
$$P + Q = \sum_{n\geq 0} (a_n + b_n) X^n$$

- On appelle **produit des polynômes P et Q** le polynôme

$$P \times Q = \sum_{n\geq 0} c_n X^n \quad \text{avec} \quad c_n = \sum_{k=0}^{n} a_{n-k} b_k.$$

- On appelle **produit externe du polynôme P par le scalaire λ** le polynôme

$$\lambda \cdot P = \sum_{n\geq 0} \lambda a_n X^n.$$

Remarques

1. On remarquera que si l'addition des polynômes et la multiplication externe sont bien les opérations habituelles définies sur $\mathbb{K}^{\mathbb{N}}$, il n'en est pas de même de la multiplication — la multiplication de deux suites $(a_n), (b_n)$ étant définie par $(a_n)(b_n) = (a_n b_n)$, formule très différente de la formule ci dessus.
2. La définition de c_n peut aussi s'écrire

$$c_n = a_n b_0 + a_{n-1} b_1 + \cdots + a_1 b_{n-1} + a_0 b_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{\substack{i+j=n \\ i,j\in\mathbb{N}}} a_i b_j.$$

   Cette dernière formule montrant directement que $P \times Q = Q \times P$.
3. Si les termes a_n sont nuls si $n > d$ et les termes b_n sont nuls si $n > d'$, alors
   - Si $n > \max(d, d')$, alors $a_n + b_n = 0$;
   - Si $n > d$, alors $\lambda a_n = 0$;
   - Si $n > d + d'$, alors $c_n = 0$. En effet, l'inégalité $i + j > d + d'$ exige $i > d$ ou $j > d'$, et donc $a_i b_j = 0$. Cela justifie que le produit de deux polynômes est bien définit.

Théorème 5

L'addition et la multiplications des polynômes sont des lois associatives, commutatives. De plus, la multiplication est distributive par rapport à l'addition.

1. $\mathbb{K}[X]$ *muni de l'addition et de la multiplication des polynôme est un anneau commutatif.*
2. $\mathbb{K}[X]$ *muni de l'addition des polynôme et de la multiplication externe est un* $\mathbb{K}$*-espace vectoriel.*
3. $\mathbb{K}[X]$ *muni de ces trois opérations est une* $\mathbb{K}$*-algèbre.*

Remarques

1. Lorsqu'aucune confusion est possible, on pourra omettre les symboles de multiplication: $PQ = P \times Q$, $\lambda P = \lambda \cdot P$.
2. La multiplication des polynômes admet pour élément neutre le polynôme $1 = 1X^0 + 0X^1 + \ldots$.
3. Nous utiliserons la convention usuelle d'exponentiation: pour tout polynôme P, P^0 sera par convention le polynôme 1 ; pour tout $n \geq 1$, P^n désignera le polynôme $P \times \cdots \times P$ (n fois).
4. La formule du binôme de Newton, reste valide

$$(P + Q)^n = \sum_{k=0}^{n} \binom{n}{k} P^{n-k} Q^k;$$

   ainsi que les autres identités remarquables comme

$$P^{n+1} - Q^{n+1} = (P - Q) \times \left(\sum_{k=0}^{n} P^{n-k} Q^k \right).$$

§2 Degré d'un polynôme

Théorème 6 *Tout polynôme non nul de $\mathbb{K}[X]$ admet une unique écriture*

$$P(X) = \sum_{n=0}^{d} a_n X^n = a_0 + a_1 X + \cdots + a_d X^d, \quad \text{avec} \quad a_d \neq 0.$$

Cela justifie, a posteriori, la notation $P = \sum_{n\geq 0} a_n X^n$.

Définition 7 Soit $P = \sum_{n\geq 0} a_n X^n \in \mathbb{K}[X]$.

- Lorsque $P \neq \mathbf{0}$, on appelle **degré** de P, et l'on note $\deg P$, le plus grand des entiers d tel que $a_d \neq 0$.
- Le **terme dominant** de P est $a_d X^d$ et son **coefficient dominant** est a_d. Ils ne sont définis que pour des polynômes non nuls.
- Le polynôme P est dit **unitaire** ou **normalisé** si son coefficient dominant est 1.
- Lorsque $P = \mathbf{0}$, le degré de P est égal par convention à $-\infty$.

Lorsqu'il sera question de degré de polynômes, nous conviendrons de prolonger à $\mathbb{N} \cup \{ -\infty \}$ la relation d'ordre et l'addition de $\mathbb{N}$ par les conventions suivantes, où $n \in \mathbb{N}$,

$$-\infty < n, \quad (-\infty) + n = n + (-\infty) = -\infty, \quad (-\infty) + (-\infty) = -\infty.$$

Proposition 8

1. *Pour tous $P, Q \in \mathbb{K}[X]$,*

$$P \times Q = \mathbf{0} \implies P = \mathbf{0} \text{ ou } Q = \mathbf{0}.$$

*On dit que $\mathbb{K}[X]$ est **intègre**.*

2. *L'ensemble des polynômes inversibles pour la multiplication est l'ensemble des polynômes constants non nuls.*

3. *On a les règles suivantes pour des polynômes P et Q non nuls:*

$$\text{terme dominant}(PQ) = \text{terme dominant}(P) \times \text{terme dominant}(Q)$$
$$\text{coefficient dominant}(PQ) = \text{coefficient dominant}(P) \times \text{coefficient dominant}(Q).$$

Démonstration. Soit P, Q deux polynômes non nuls. Écrivons $P(X) = a_0 + \cdots + a_d X^d$ et $Q(X) = b_0 + \cdots + b_e X^e$ avec $a_d \neq 0$ et $b_e \neq 0$. Alors, de la définition de la multiplication dans $\mathbb{K}[X]$, on tire

$$PQ(X) = a_0 b_0 + \cdots + a_d b_e X^{d+e} \quad \text{et} \quad a_d b_e \neq 0.$$

Le fait que $PQ \neq 0$ et les deux règles de s'en déduisent immédiatement.

Il est clair que si $P \in \mathbb{K}\setminus\{ 0 \}$, P est inversible dans $\mathbb{K}$ donc dans $\mathbb{K}[X]$. Réciproquement, si $PQ = 1$, alors P et Q sont non nuls, et le polynôme $PQ = 1$ a pour terme dominant $1 = a_d b_e X^{d+e}$, d'où $a_d b_e = 1$ et $d + e = 0$, d'où $d = e = 0$. ∎

Corollaire 9 *Tout polynôme non nul est simplifiable, c'est-à-dire, pour $P, A, B \in \mathbb{K}[X]$,*

$$(P \times A = P \times B \text{ et } P \neq \mathbf{0}) \implies A = B.$$

Théorème 10 *Pour tous $P, Q \in \mathbb{K}[X]$,*

1. $\deg(PQ) = \deg(P) + \deg(Q)$,
2. $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$,
3. $\deg(P+Q) < \max(\deg(P), \deg(Q))$ *si, et seulement si*

$$\deg P = \deg Q \geq 0 \text{ et } cd(P) + cd(Q) = 0.$$

Démonstration. En reprenant les notations de la démonstration précédente.

Si $\deg P < \deg Q$ (l'autre cas est symétrique), alors

$$(P+Q)(X) = (a_0 + b_0) + \cdots + (a_d + b_d)X^d + \cdots + b_e X^e \quad \text{et} \quad b_e \neq 0.$$

donc $\deg(P+Q) = \deg(Q)$.

Si $\deg P = \deg Q$, alors

$$(P+Q)(X) = (a_0 + b_0) + \cdots + (a_d + b_d)X^d,$$

donc $\deg(P+Q) \leq d$ et l'on a $\deg(P+Q) < d$ si, et seulement si $a_d + b_d = 0$. ∎

Notation Pour $n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré *inférieur ou égal* à n. Ainsi

$$\mathbb{K}_n[X] = \left\{ \sum_{k=0}^{n} a_k X^k \;\middle|\; (a_0, \ldots, a_n) \in \mathbb{K}^{n+1} \right\}.$$

§3 Fonctions polynômiales

Définition 11 Soit $P = \sum_{n \geq 0} a_n X^n \in \mathbb{K}[X]$ et $x \in \mathbb{K}$.

- On note

$$\widetilde{P}(x) = \sum_{n=0}^{\deg P} a_n x^n \in \mathbb{K}.$$

$\widetilde{P}(x)$ s'appelle l'**élément de $\mathbb{K}$ déduit par substitution de x à X dans P**, ou encore la **valeur de P en x**. Plus simplement, on peut noter

$$\widetilde{P}(x) = P(x) = \sum_{n \geq 0} a_n x^n.$$

- L'application

$$\begin{array}{rccc} \widetilde{P} : & \mathbb{K} & \to & \mathbb{K} \\ & x & \mapsto & \widetilde{P}(x) \end{array}$$

s'appelle la **fonction polynômiale** définie par P.

Proposition 12

Quels que soient les polynômes P et Q de $\mathbb{K}[X]$, et le scalaire $\lambda \in \mathbb{K}$, on a

$$\widetilde{P+Q} = \widetilde{P} + \widetilde{Q}, \quad \widetilde{\lambda \cdot P} = \lambda \cdot \widetilde{P} \quad \text{et} \quad \widetilde{P \times Q} = \widetilde{P} \times \widetilde{Q}.$$

On peut, plus généralement, *substituer à X dans P un polynôme $Q \in \mathbb{K}[X]$*, ou alors une matrice carré $A \in \mathscr{M}_n(\mathbb{K})$ ou un endomorphisme $f \in \mathbf{L}(E)$ d'un $\mathbb{K}$-espace vectoriel E...

§4 Méthode de Horner pour l'évaluation polynomiale

Au temps jadis, les physiciens et les astronomes devaient faire tous leurs calculs à la main, et ces calculs pouvaient être très compliqués. Il fallait souvent évaluer des quantités polynomiales, par exemple $5x^4 - 4x^3 + 3x^2 - 2x + 1$ pour $x = 8$. La façon naïve d'arriver au résultat est de calculer x, x^2, x^3 et x^4 pour la valeur choisie $x = 8$, ce qui représente 3 multiplications, puis $5x^4$, $4x^3$, $3x^2$ et $2x$, ce qui représente 4 multiplications supplémentaires. En ajoutant les sommes à la liste des opérations nécessaires, on obtient en tout 7 multiplications et 4 additions. La tradition attribue au mathématicien anglais William George Horner (1786-1837) la description en 1819 d'une méthode efficace pour économiser des opérations, méthode encore utilisée de nos jours par les ordinateurs. Remplaçons en effet $5x^4 - 4x^3 + 3x^2 - 2x + 1$ par l'expression équivalente

$$x(x(x(x \times 5 - 4) + 3) - 2) + 1,$$

On économise donc des multiplications, qui sont des opérations longues à réaliser. De plus, on n'a été obligé de stocker en mémoire (ou dans son cerveau, si on n'est pas en silicium) que deux valeurs. La tradition a retenu cette méthode sous le nom d'algorithme de Horner à cause de l'article de 1819 cité plus haut. Il se trouve que cet article ne contient pas ladite méthode! Horner la décrit bien, mais dans un autre article, publié en 1830 seulement. Et entre temps, en 1820, un fabricant de montres londonien nommé Theophilus Holdred avait, lui, effectivement publié la méthode.

Proposition 13

$$\sum_{n=0}^{d} a_n x^n = x\left(\ldots\left(x\left(x\left(x \times a_d + a_{d-1}\right) + a_{d-2}\right) + a_{d-3}\right)\cdots + a_1\right) + a_0.$$

§5 Composée

Définition 14

Soit $(P, Q) \in \mathbb{K}[X]^2$, avec $P = \sum_{n\geq 0} a_n X^n$. On appelle polynôme composé des deux polynômes P et Q, et on note $P \circ Q$ ou encore $P(Q)$ le polynôme défini par

$$P \circ Q = P(Q) = \sum_{n=0}^{\deg P} a_n Q^n$$

que l'on écrit plus simplement

$$P \circ Q = \sum_{n\geq 0} a_n Q^n.$$

On a bien sûr $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$.

Définition 15

- Un polynôme P est **pair** si $P(-X) = P(X)$.
- Un polynôme P est **impair** si $P(-X) = -P(X)$.

Proposition 16

Soit $P = \sum_{n \geq 0} a_n X^n \in \mathbb{K}[X]$.

- *P est impair si et seulement si P ne contient que des termes non nuls de degré impairs, c'est-à-dire*
$$\forall n \in \mathbb{N}, n \in 2\mathbb{N} \implies a_n = 0.$$
- *P est pair si et seulement si P ne contient que des termes non nuls de degré pairs, c'est-à-dire*
$$\forall n \in \mathbb{N}, n \notin 2\mathbb{N} \implies a_n = 0.$$

28.2 Division dans $\mathbb{K}[X]$

§1 Multiples et diviseurs

Définition 17

Soient $A, B \in \mathbb{K}[X]$. On dit que A **divise** B lorsqu'il existe un polynôme Q vérifiant $B = AQ$. On note cette relation $A \mid B$. On dit aussi que B est un **multiple** de A.

Lorsque $A \neq 0$, le polynôme Q est unique car $\mathbb{K}[X]$ est intègre et s'appelle **quotient exact** de la division de B par A. Dans ce cas, on a

$$\deg A \leq \deg B \quad \text{et} \quad \deg Q = \deg B - \deg A.$$

Exemples 18

1. $X - 1 \mid X^5 - 1$ car $X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1)$.
2. On a $X \mid 3X$, mais aussi $3X \mid X$ car $X = \frac{1}{3} 3X$. Plus généralement, $\lambda P \mid P$ pour tout $\lambda \in \mathbb{K}^\star$.
3. Le polynôme nul $\mathbf{0}$ est multiple de tout polynôme (car $\mathbf{0} = A \times \mathbf{0}$) mais il ne divise que lui-même (car $B = Q \times \mathbf{0}$ implique $B = \mathbf{0}$).
4. Un polynôme de degré 0 divise tous les polynômes et n'est multiple que des polynômes de degré 0.
5. On a bien $3 \mid 2$ dans $\mathbb{K}[X]$ bien que cette relation soit fausse dans $\mathbb{N}$.

Test 19

Soient $A, B, C, D \in \mathbb{K}[X]$.

1. Si $A \mid B$ et $A \mid C$, alors pour tous polynômes $U, V \in \mathbb{K}[X]$,
$$A \mid UB + VC.$$
2. Si $A \mid B$ et $C \mid D$, alors $AC \mid BD$.

Test 20

La relation $\mid$ sur $\mathbb{K}[X]$ est

1. réflexive : $\forall A \in \mathbb{K}[X], A \mid A$;
2. transitive : $\forall (A, B, C) \in \mathbb{K}[X]^3, \left(A \mid B \text{ et } B \mid C\right) \implies A \mid C$.
3. n'est pas antisymétrique, mais
$$\forall (A, B) \in \mathbb{K}[X]^2, \left(B \mid A \text{ et } A \mid B\right) \implies \exists \lambda \in \mathbb{K} \setminus \{0\}\ A = \lambda B.$$
Rappelons que les éléments inversibles pour la multiplication dans $\mathbb{Z}$ sont -1 et 1, les éléments inversibles dans $\mathbb{K}[X]$ sont les éléments de $\mathbb{K} \setminus \{0\}$. On remarquera alors l'analogie entre ce résultat et les propriétés de la divisibilité dans l'anneau $\mathbb{Z}$ des entiers…

§2 Polynômes associés

Proposition 21 **Caractérisation des polynômes associés**

Soit A, B deux polynômes non nuls de $\mathbb{K}[X]$. Les assertions suivantes sont équivalentes

1. $A \mid B$ *et* $B \mid A$;
2. $A \mid B$ *et* $\deg A = \deg B$;
3. $\exists \lambda \in \mathbb{K} \setminus \{0\}, A = \lambda B$.

Définition 22

On dit que deux polynômes A et B sont **associés** lorsqu'il existe un scalaire non nul $\lambda \in \mathbb{K} \setminus \{0\}$ tel que $A = \lambda B$.

On note alors $A \sim B$. La relation $\sim$ est clairement une relation d'équivalence sur $\mathbb{K}[X]$.

§3 Division euclidienne dans $\mathbb{K}[X]$

Théorème 23 *Soit $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Il existe un unique couple de polynômes $(Q, R) \in \mathbb{K}[X]^2$ tels que*

$$A = BQ + R \quad \text{et} \quad \deg R < \deg B.$$

*On appelle Q le **quotient** de la division euclidienne de A par B.*
*Le polynôme $R = A - BQ$ est le **reste** de la division euclidienne de A par B.*

Exemple 24 En suivant l'algorithme décrit dans la démonstration :

$$\begin{array}{rrrrr|l}
2X^4 & +5X^3 & -X^2 & +2X & +1 & 2X^2-3X+1 \\
\cline{6-6}
+2X^4 & -3X^3 & +X^2 & & & X^2 \\
\cline{1-5}
 & 8X^3 & -2X^2 & +2X & +1 & \\
 & 8X^3 & -12X^2 & +4X & & +4X \\
\cline{2-5}
 & & 10X^2 & -2X & +1 & \\
 & & 10X^2 & -15X & +5 & +5 \\
\cline{3-5}
 & & & 13X & -4 &
\end{array}$$

Ici $A = 2X^4 + 5X^3 - X^2 + 2X + 1, B = 2X^2 - 3X + 1, Q = X^2 + 4X + 5, R = 13X - 4$.

Test 25 Effectuer la division euclidienne de $A = X^7 + X + 1$ par $B = X^3 + X + 1$.

Théorème 26 *Soit $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Alors $B \mid A$ si et seulement si le reste de la division euclidienne de A par B est nul.*

Remarque Soit $A, B \in \mathbb{R}[X]$. Le quotient et le reste de la division euclidienne de B par A sont identique dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$.

Ainsi, si $A \mid B$ dans $\mathbb{C}[X]$, c'est-à-dire $B = AQ$ avec $Q \in \mathbb{C}[X]$, alors $A \mid B$ dans $\mathbb{R}[X]$, c'est-à-dire que $Q \in \mathbb{R}[X]$.

§4 Idéaux de $\mathbb{K}[X]$

Théorème 27 *Tout idéal de $\mathbb{K}[X]$ est de la forme*

$$A\mathbb{K}[X] = \{\, AQ \mid Q \in \mathbb{K}[X] \,\},$$

où A est un polynôme, que l'on peut choisir unitaire (il est alors unique).

28.3 RACINES

Proposition 28 *Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.*
Le reste de la division euclidienne de $P(X)$ par $X - a$ est $\tilde{P}(a)$. On a donc l'équivalence

$$(X-a) \mid P \iff \widetilde{P}(a) = 0.$$

Définition 29 Lorsque $\widetilde{P}(a) = 0$, on dit que a est **une racine** ou **un zéro** de P.

§1 Racines d'un polynôme

Définition 30 Soit $P \in \mathbb{K}[X]$ un polynôme non nul et soit $a \in \mathbb{K}$.

- On dit que a est **une racine** ou **un zéro** de P si $\widetilde{P}(a) = 0$.

  Pour que a soit un zéro de P, il faut, et il suffit, que $X - a$ divise P.

- On suppose que a est un zéro de P. Il existe alors un unique entier m tel que P est divisible par $(X-a)^m$ mais pas par $(X-a)^{m+1}$. On a $1 \leq m \leq \deg P$.

  L'entier m est appelé l'**ordre** ou la **multiplicité** de la racine a. La racine a est dite **simple** si $m = 1$, et **multiple** sinon.

Théorème 31 *Soit $P \in \mathbb{K}[X]$ un polynôme non nul et soit $a \in \mathbb{K}$.*
a est une racine de multiplicité m si, et seulement si il existe un polynôme $Q \in \mathbb{K}[X]$ tel que

$$P = (X-a)^m Q \quad \text{et} \quad \widetilde{Q}(a) \neq 0.$$

Exemple 32 Déterminons la multiplicité de 1 relativement aux polynômes $P = X^3 - 3X^2 + 2$ et $Q = X^3 - 4X^2 + 5X - 2$.

Lemme 33 *Soient $a_1, a_2, \ldots, a_k$ des racines deux à deux distinctes du polynôme non nul P et soient $m_1, m_2, \ldots, m_k$ leurs multiplicités. Alors*

$$P(X) = \left(X - a_1\right)^{m_1} \left(X - a_2\right)^{m_2} \ldots \left(X - a_k\right)^{m_k} Q(X) \quad \text{où} \quad Q(a_1) \neq 0, \ldots, Q(a_k) \neq 0.$$

Soient $a_1, a_2, \ldots, a_k$ toutes les racines de P et soient $m_1, m_2, \ldots, m_k$ leurs multiplicités. L'expression **le nombre de racines de P comptées avec leurs multiplicités** désigne alors la somme $m_1 + m_2 + \cdots + m_k$ de ces multiplicités.

Théorème 34 *Le nombre de racines d'un polynôme non nul P, comptées avec leurs multiplicités, est inférieur ou égal à* $\deg(P)$.

Corollaire 35 *Soit $n \in \mathbb{N}$. Si $\deg P \leq n$ et si P admet au moins $n+1$ racines distinctes alors $P = 0$.*

Corollaire 36 *Soient $P, Q \in \mathbb{K}[X]$ de degré $\leq n$. S'il existe $n+1$ éléments $x_1, \cdots, x_{n+1}$ de $\mathbb{K}$, deux à deux distincts, tels que $P(x_i) = Q(x_i)$ pour $1 \leq i \leq n+1$, on a $P = Q$.*

Corollaire 37 *Soient $P, Q \in \mathbb{K}[X]$ tels qu'il existe une partie infinie de $\mathbb{K}$ sur laquelle $\widetilde{P}$ et $\widetilde{Q}$ coïncident. Alors $P = Q$.*

En particulier, l'application $P \in \mathbb{K}[X] \mapsto \widetilde{P} \in \mathscr{F}(\mathbb{K}, \mathbb{K})$ est injective.

§2 Polynôme d'interpolation de Lagrange

Donnons nous n scalaires distincts $x_1, x_2, \dots, x_n$ et n autres scalaires $y_1, y_2, \dots, y_n$. On cherche un polynôme P tel que,

$$\forall j \in [\![1, n]\!], P(x_j) = y_j.$$

On dira alors que l'on a résolu le **problème d'interpolation** du système $(x_1, x_2, \dots, x_n)$ pour les valeurs $y_1, y_2, \dots, y_n$. En pratique, le plus souvent, les y_j sont les valeurs prises par une certaine fonction f en les x_j: on dit que P interpole f selon les x_j.

Théorème 38 *Soient $(x_1, x_2, \dots, x_n)$ des éléments deux à deux distincts de $\mathbb{K}$. Pour $j \in [\![1, n]\!]$, on pose*

$$L_j = \prod_{k \in [\![1,n]\!] \setminus \{j\}} \left(\frac{X - x_k}{x_j - x_k} \right).$$

Ces polynômes sont de degré $n-1$ et

$$\forall (j, k) \in [\![1, n]\!], L_j(x_k) = \delta_{j,k}.$$

Théorème 39 **Polynôme d'interpolation de Lagrange**
Soient $(x_1, x_2, \dots, x_n)$ des éléments deux à deux distincts de $\mathbb{K}$ et $(y_1, y_2, \dots, y_n) \in \mathbb{K}^n$. L'unique polynôme P tel que

$$\deg(P) \leq n-1 \text{ et } P(x_1) = y_1 \text{ et } P(x_2) = y_2 \text{ et } \dots \text{ et } P(x_n) = y_n$$

est le polynôme

$$P = \sum_{j=1}^{n} y_j L_j.$$

§3 Relations entre coefficients et racines

Définition 40 Un polynôme non nul P est dit **scindé** s'il est produit de polynômes du premier degré (ou, de manière équivalente, s'il admet $\deg(P)$ racines comptées avec leurs multiplicités).

Soit P un polynôme scindé de $\mathbb{K}[X]$ de degré $n \geq 1$, $x_1, \dots, x_n$ ses zéros comptés avec leur ordre de multiplicité. Les éléments $x_1, \dots, x_n$ sont éléments de $\mathbb{K}$ distincts ou non. On a deux écritures possibles

$$P = a_0 + a_1 X + \cdots + a_n X^n = a_n (X - x_1)(X - x_2) \cdots (X - x_n)$$

Quelles relations y-a-t-il entre $x_1, x_2, \dots, x_n$ et $a_0, \dots, a_n$?

Exemples élémentaires

Proposition 41

Cas $n = 2$
Soit

$$P = a_0 + a_1X + a_2X^2 = a_2(X - x_1)(X - x_2)$$

un polynôme scindé de degré 2. Alors

$$x_1x_2 = \frac{a_0}{a_2} \quad \text{et} \quad x_1 + x_2 = -\frac{a_1}{a_2}.$$

Proposition 42

Cas $n = 3$
Soit

$$P = a_0 + a_1X + a_2X^2 + a_3X^3 = a_3(X - x_1)(X - x_2)(X - x_3)$$

un polynôme scindé de degré 3. Alors

$$x_1x_2x_3 = -\frac{a_0}{a_3} \quad x_1x_2 + x_1x_3 + x_2x_3 = \frac{a_1}{a_3} \quad x_1 + x_2 + x_3 = -\frac{a_2}{a_3}.$$

Généralisation : fonctions symétriques élémentaires

Définition 43

Soient $n \in \mathbb{N}^\star$, et $x_1, \dots, x_n$ dans $\mathbb{K}$. On note pour tout entier k compris entre 1 et n, [a]

$$\sigma_k(x_1, \dots, x_n) = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} x_{i_1}x_{i_2} \cdots x_{i_k} = \sum_{\substack{H \subset [\![1,n]\!] \\ \text{card } H = k}} \prod_{i \in H} x_i.$$

La fonction $\sigma_k : \mathbb{K}^n \to \mathbb{K}$, s'appelle **fonction symétrique élémentaire de degré k**.

[a] 43. Cette somme contient $\binom{n}{k}$ termes.

On écrira souvent σ_k au lieu de $\sigma_k(x_1, \dots, x_n)$ afin d'alléger les notations. On a par exemple

$$\begin{aligned}
\sigma_1 &= x_1 + x_2 + \cdots x_n \\
\sigma_2 &= \sum_{1 \leq i < j \leq n} x_ix_j = x_1x_2 + x_1x_3 + x_2x_3 + \cdots + x_{n-1}x_n \\
&\vdots \\
\sigma_n &= x_1x_2 \cdots x_n.
\end{aligned}$$

Lorsqu'il convient de préciser l'entier n, on écrit $\sigma_{k,n}$ pour σ_k.

Le terme symétrique signifie que si l'on permute x_i et x_j, cela ne change pas la valeur de σ_k. L'intérêt des fonctions symétriques élémentaires provient de la propriété suivante, qui dépasse le cadre du programme

> *Toute expression rationnelle symétrique en $x_1, \dots, x_n$ peut s'exprimer en fonction des fonctions symétriques élémentaires.*

Théorème 44

Relations coefficient-racines (Formules de Viète)
Soit $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ un polynôme scindé de $\mathbb{K}[X]$ de degré $n \geq 1$; on

note $x_1, \dots, x_n$ ses zéros comptés avec leur ordre de multiplicité.
Alors, pour $k = 1, \dots, n$,

$$\sigma_{k,n} = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} x_{i_1} x_{i_2} \cdots x_{i_k} = (-1)^k \frac{a_{n-k}}{a_n}.$$

On peut donc écrire

$$P = a_n \left(X^n - \sigma_1 X^{n-1} + \cdots + (-1)^{n-1} \sigma_{n-1} X + (-1)^n \sigma_n \right).$$

Exemple 45

- $n = 4, k = 2$: on a $\dfrac{a_2}{a_4} = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$.
- $k = 1 : -\dfrac{a_{n-1}}{a_n} = \displaystyle\sum_{i=1}^{n} x_i$.
- $k = n : (-1)^n \dfrac{a_0}{a_n} = x_1x_2 \cdots x_n$.

Corollaire 46 **Somme et produit des racines**
Soit

$$P = a_0 + a_1X + a_2X^2 + \cdots + a_{n-1}X^{n-1} + a_nX^n = a_n(X - x_1)(X - x_2) \dots (X - x_n)$$

un polynôme scindé de $\mathbb{K}[X]$ de degré $n \ge 1$; avec $x_1, \dots, x_n$ ses zéros comptés avec leur ordre de multiplicité. Alors

$$x_1x_2 \dots x_n = (-1)^n \frac{a_0}{a_n} \quad \text{et} \quad x_1 + x_2 + \cdots + x_n = -\frac{a_{n-1}}{a_n}.$$

Exemple 47

Soit $P = X^4 + 4X^3 + 2X^2 + 7X + 12 \in \mathbb{C}[X]$, x_1, x_2, x_3, x_4 ses zéros.
Calculer $x_1^3 + x_2^3 + x_3^3 + x_4^3$.
Il existe des formules permettant de résoudre une équation algébrique du 4-ième degré (c'est même la plus grande valeur des degrés pour lesquels des formules sont possibles). On se doute que ces formules sont d'une utilisation extrêmement malaisée, voire même impossible dans la pratique. Mais dans le cas présent, on peut écrire

$$\begin{aligned}
\sigma_1^3 = \left(\sum_{i=1}^{4} x_i \right)^3 &= \sum_{i=1}^{4} x_i^3 + 3 \sum_{1 \le i < j \le 4} x_i^2 x_j + 3 \sum_{1 \le i < j \le 4} x_i x_j^2 + 6 \sum_{1 \le i < j < k \le 4} x_i x_j x_k \\
&= \sum_{i=1}^{4} x_i^3 + 3 \left(\sum_{1 \le i < j \le 4} x_i x_j (x_i + x_j) \right) + 6\sigma_3 \\
&= \sum_{i=1}^{4} x_i^3 + 3 \left(\sum_{1 \le i < j \le 4} x_i x_j \sigma_1 \right) - 3 \times 3 \left(\sum_{1 \le i < j < k \le 4} x_i x_j x_k \right) + 6\sigma_3 \\
&= \sum_{i=1}^{4} x_i^3 + 3\sigma_2\sigma_1 - 3\sigma_3.
\end{aligned}$$

Or on a $\sigma_1 = -4$, $\sigma_2 = 2$, $\sigma_3 = -7$, $\sigma_4 = 12$, d'où

$$\sum_{i=1}^{4} x_i^3 = \sigma_1^3 - 3\sigma_2\sigma_1 + 3\sigma_3 = -61.$$

28.4 Polynômes dérivés

§1 Dérivée formelle

Définition 48

Soit $P = \sum_{n\geq 0} a_n X^n \in \mathbb{K}[X]$. On appelle **dérivée formelle de P** ou **polynôme dérivé de P**, le polynôme

$$P' = \sum_{n\geq 0} (n+1)a_{n+1}X^n.$$

Si $P = a_0 + a_1 X + a_2 X^2 + \cdots + a_d X^d$, alors

$$P' = a_1 + 2a_2 X + \cdots + d a_d X^{d-1} = \sum_{n=0}^{d-1} (n+1)a_{n+1}X^n = \sum_{n=1}^{d} n a_n X^{n-1}.$$

On utilise donc également la notation

$$P' = \sum_{n\geq 1} n a_n X^{n-1}.$$

Remarque

Il s'agit d'une dérivation formelle définie algébriquement. Bien sûr, dans le cas réel, on a pour $x \in \mathbb{R}$,

$$\widetilde{(P')}(x) = \left(\widetilde{P}\right)'(x).$$

Théorème 49

La dérivation $\mathrm{D} : \mathbb{K}[X] \to \mathbb{K}[X]$ *est une application linéaire, c'est-à-dire,*

$$\forall (\alpha,\beta) \in \mathbb{K}^2, \forall (P,Q) \in \mathbb{K}[X]^2, (\alpha P + \beta Q)' = \alpha P' + \beta Q'.$$

De plus, la dérivation satisfait la règle de Leibniz:

$$\forall (P,Q) \in \mathbb{K}[X]^2, (PQ)' = P'Q + PQ'.$$

Démonstration. La linéarité de $P \mapsto P'$ est évidente.

Supposons $P = X^p$ et $Q = X^q$ avec $p, q \geq 1$. On a alors

$$(PQ)' = (p+q)X^{p+q-1} = pX^{p-1}X^q + X^p(qX^{q-1}) = P'Q + PQ'.$$

Supposons $P = X^p$ et $Q = \sum_{q\geq 0} b_q X^q$, alors

$$\begin{aligned}(PQ)' &= \left(\sum_{q\geq 0} b_q P X^q\right)' = \sum_{q\geq 0} b_q (PX^q)' \\ &= \sum_{q\geq 0} b_q \left(P'X^q + P(X^q)'\right) = P' \sum_{q\geq 0} b_q X^q + P \sum_{q\geq 0} b_q (X^q)' = P'Q + PQ'.\end{aligned}$$

Supposons $P = \sum_{p\geq 0} a_p X^p$ et $Q = \sum_{q\geq 0} b_q X^q$, alors

$$(PQ)' = \sum_{p\geq 0} a_p (X^p Q)' = \sum_{p\geq 0} a_p (X^p)' Q + \sum_{p\geq 0} a_p X^p Q' = P'Q + PQ'.$$

∎

Théorème 50

Soient $P, Q \in \mathbb{K}[X]$.

$$(P\circ Q)' = \left(P'\circ Q\right) \times Q'.$$

En particulier, pour $m \geq 1$, $(P^m)' = mP^{m-1}P'$.

§2 Dérivées successives

Définition 51

On définit par récurrence le **polynôme dérivé d'ordre k** de P, notée $P^{(k)}$ ou $\mathrm{D}^k(P)$, comme suit

- On pose $P^{(0)} = P$,
- pour $k \in \mathbb{N}$, on pose $P^{(k+1)} = \left(P^{(k)}\right)'$.

Test 52

Quelles sont les dérivées successives de $P = X^m$? De $Q = (X-a)^m$?

Théorème 53

Formule de Leibniz pour les polynômes
Soient $(P, Q) \in \mathbb{K}[X]^2$ et $k \in \mathbb{N}$. Alors

$$(PQ)^{(k)} = \sum_{j=0}^{k} \binom{k}{j} P^{(k-j)} \times Q^{(j)}.$$

§3 Formules de Taylor pour les polynômes

Théorème 54

Formules de Taylor pour les polynômes
Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors

$$P(X) = \sum_{n\geq 0} \frac{P^{(n)}(a)}{n!}(X-a)^n = P(a) + P'(a)(X-a) + \cdots + \frac{P^{(d)}(a)}{d!}(X-a)^d,$$

où $d = \deg(P)$.

On a donc en particulier

$$P(X) = \sum_{n\geq 0} \frac{P^{(n)}(0)}{n!} X^n = P(0) + P'(0)X + \cdots + \frac{P^{(d)}(0)}{d!} X^d$$

et aussi

$$P(X+a) = \sum_{n\geq 0} \frac{P^{(n)}(a)}{n!} X^n = P(a) + P'(a)X + \cdots + \frac{P^{(d)}(a)}{d!} X^d.$$

§4 Critère différentiel pour la multiplicité d'une racine

Lemme 55 *Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Supposons que a soit d'ordre $m \geq 1$ relativement à P. Alors a est d'ordre $m-1$ relativement à P'.*

Théorème 56 *Soit P un polynôme non nul sur le corps $\mathbb{K}$.*

1. *Pour que $a \in \mathbb{K}$ soit racine multiple de P, il faut, et il suffit, que a soit racine de P et de P'.*
2. *Soit m un entier non nul. Pour que $a \in \mathbb{K}$ soit racine de P d'ordre m, il faut, et il suffit que*

$$P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0 \quad \text{et} \quad P^{(m)}(a) \neq 0.$$

Corollaire 57 *$a \in \mathbb{K}$ est racine simple de P si et seulement si $P(a) = 0$ et $P'(a) \neq 0$.*

Exemple 58 Déterminons la multiplicité de 1 relativement aux polynômes $P = X^3 - 3X^2 + 2$ et $Q = X^3 - 4X^2 + 5X - 2$.

1. On a $P(1) = 0$, $P' = 3X^2 - 6X$, $P'(1) = -3 \neq 0$: 1 est donc racine simple de P.
2. On a $Q(1) = 0$, $Q' = 3X^2 - 8X + 5$, $Q'(1) = 0$, $Q'' = 6X - 8$, $Q''(1) = -2 \neq 0$: 1 est racine double de Q.

28.5 Arithmétique dans $\mathbb{K}[X]$

§1 Polynômes irréductibles

Définition 59 Un polynôme P non constant est dit **irréductible** ou **premier** si les seuls diviseurs de P sont les polynômes associés à P et les polynômes inversibles.
Dans le cas contraire, on dit que P est **réductible**.

Ainsi, le polynôme P de degré supérieur ou égal à 1 est irréductible si, et seulement si l'on a l'implication

$$\forall (A, B) \in \mathbb{K}[X]^2, P = AB \implies \deg A = 0 \text{ ou } \deg B = 0.$$

Exemples 60 **Cas importants**

1. Un polynôme constant n'est ni réductible ni irréductible.
2. Tout polynôme de degré 1 est irréductible.
3. Le polynôme $X^2 + 1$ de $\mathbb{R}[X]$ est irréductible. Mais le même polynôme $X^2 + 1$, considéré comme élément de $\mathbb{C}[X]$, se factorise en $(X + i)(X - i)$. La notion de polynôme irréductible est donc relative au corps de base $\mathbb{K}$.

4. Un polynôme de degré 2 est irréductible dans $\mathbb{K}[X]$ si, et seulement s'il n'a pas de racine dans $\mathbb{K}$.

Exemple 61

Soit P un polynôme de degré ≥ 3.
Si P admet une racine, c'est-à-dire s'il existe $a \in \mathbb{K}$ tel que $\widetilde{P}(a) = 0$, alors P n'est pas un polynôme irréductible.
La réciproque est fausse comme le montre l'exemple du polynôme $P = (X^2+1)(X^2+2) \in \mathbb{R}[X]$.

Théorème 62

Tout polynôme non constant est produit de polynômes irréductibles.

§2 Diviseurs communs à deux polynômes

Définition 63

Soit A et B deux polynômes. On dit qu'un polynôme D est un **plus grand commun diviseur** de A et B, ou **pgcd** de A et B, lorsque

$$A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X].$$

Définition 64

Tous les pgcd de A et B sont associés. On appellera celui qui est unitaire **le pgcd** de A et B et on le notera $\text{pgcd}(A, B)$ ou $A \wedge B$.

On conviendra que $\text{pgcd}(0, 0) = 0$ (qui n'est pas unitaire!).

Exemple 65

Si $A \mid B$, alors A est un pgcd de A et B.

Théorème 66

Soit A et B deux polynômes.

1. *Le pgcd de A et B est l'unique polynôme unitaire D tel que*
   - *D divise A et B,*
   - *tout diviseur commun à A et B divise D.*
2. *On a la **relation de Bézout***
$$\exists (U, V) \in \mathbb{K}[X]^2, UA + VB = D.$$
3. *L'ensemble des diviseur communs à A et B est l'ensemble des diviseurs de D:*
$$\text{Div}(A, B) = \text{Div}(D).$$

Remarque

Un polynôme D est un pgcd de A et B si, et seulement si

$$D \mid A \text{ et } D \mid B \text{ et } \exists (U, V) \in \mathbb{K}[X]^2, UA + VB = D.$$

§3 Polynômes premiers entre eux

Définition 67

Soit A et B deux polynômes. On dit que A et B sont **premiers entre eux** si leur pgcd est égal à 1. Cela revient à dire que les seuls diviseurs communs à A et B sont inversibles.

$$\forall D \in \mathbb{K}[X], \left(D \mid A \text{ et } D \mid B \implies D \in \mathbb{K}^\star\right).$$

Théorème 68

Théorème de Bézout
Deux polynômes A et B sont premiers entre eux si, et seulement si il existe des polynômes U et V tels que

$$UA + VB = 1.$$

§4 Lemme de Gauß, lemme d'Euclide

Théorème 69

Lemme de Gauß pour les polynômes
Soient A, B, C des polynômes non nuls.

$$A \wedge B = 1 \text{ et } A \mid BC \implies A \mid C.$$

Théorème 70

Lemme d'Euclide pour les polynômes
Soit P un polynôme irréductible.

$$\forall (A, B) \in \mathbb{K}[X]^2, P \mid AB \implies P \mid A \text{ ou } P \mid B.$$

Théorème 71

Si A est premier avec B et C, alors A est premier avec BC.

§5 Algorithme d'Euclide

Dans cette partie, on note $\mathrm{Div}(A)$ l'ensemble des polynômes divisant A et $\mathrm{Div}(A, B)$ l'ensemble des polynômes divisant à la fois A et B, c'est-à-dire

$$\mathrm{Div}(A, B) = \mathrm{Div}(A) \cap \mathrm{Div}(B).$$

Proposition 72

Soient A, B, P, Q, U, V des polynômes.

1. *Si $P \in \mathrm{Div}(A, B)$ et $Q \mid P$, alors $Q \in \mathrm{Div}(A, B)$.*
2. *Si P et Q sont associés :* $(P \in \mathrm{Div}(A, B)) \iff (Q \in \mathrm{Div}(A, B))$.
3. *Si $P \in \mathrm{Div}(A, B)$, alors $P \mid UA + VB$.*
4. $\mathrm{Div}(A, B - UA) = \mathrm{Div}(A, B)$.

Théorème 73

Soient A et B des polynômes non nuls. Un pgcd de A et B est un polynômes $D = A_{m-1}$ où $(A_k)_{k\in\mathbb{N}}$ est la suite de polynômes telle que

- $A_0 = A$,
- $A_1 = B$,
- *Pour $k \geq 2$, A_k est le reste de la division euclidienne de A_{k-2} par A_{k-1}.*
- $A_m = 0$ *et si $k < m$, alors $A_k \neq 0$.*

Démonstration. Supposons que $A_0, A_1, \dots, A_n$ soient non nuls, alors

$$\deg A_1 > \deg A_2 > \dots \deg A_n.$$

Ceci n'est pas possible indéfiniment, donc $n \leq \deg(A_1)$. Il existe donc $m \geq 2$ tel que $A_m = 0$. Cela signifie que A_{m-1} divise A_{m-2}.

Or, pour $k = 1, 2, \dots m-2$, on a $\mathrm{Div}(A_{k+1}, A_k) = \mathrm{Div}(A_k, A_{k-1})$. Donc $\mathrm{Div}(A, B) = \mathrm{Div}(A_{m-2}, A_{m-1})$. Finalement, A_{m-1} est un pgcd de A et B. ∎

§6 PPCM de deux polynômes

Définition 74

Soient A et B des polynômes. On dit qu'un polynôme M est un **plus petit commun multiple** de A et B, ou **ppcm** de A et B, lorsque

$$A\mathbb{K}[X] \bigcap B\mathbb{K}[X] = M\mathbb{K}[X].$$

Théorème 75

Soient A et B des polynômes non nuls. Soit M un ppcm de A et B.

1. *Les autres ppcm de A et B sont les polynômes associés à M. En particulier, il existe un et un seul ppcm unitaire de A et B. On le note* $\mathrm{ppcm}(A, B)$ *ou $A \vee B$.*
2. *Soit D un pgcd de A et B, alors MD et AB sont associés.*

§7 PGCD d'une famille finie de polynômes

Définition 76

Soient $A_1, A_2, \dots, A_r \in \mathbb{K}[X]$.

- On appelle **plus grand commun diviseur** de $A_1, A_2, \dots, A_r$ tout polynôme D tel que

$$A_1\mathbb{K}[X] + A_2\mathbb{K}[X] + \dots + A_r\mathbb{K}[X] = D\mathbb{K}[X].$$

- Les pgcd de $A_1, A_2, \dots, A_r$ sont associés. Un seul d'entre eux est unitaire, on l'appelle **le pgcd** de $A_1, A_2, \dots, A_r$ et on le note

$$A_1 \wedge A_2 \wedge \dots \wedge A_r \quad \text{ou} \quad \mathrm{pgcd}(A_1, A_2, \dots, A_r).$$

On pose par convention $\mathrm{pgcd}(0, 0, \dots, 0) = 0$.

Proposition 77

Soient $A_1, A_2, \dots, A_r \in \mathbb{K}[X]$.

1. *Les diviseurs communs de $A_1, A_2, \dots, A_r$ sont exactement les diviseur de $\operatorname{pgcd}(A_1, A_2, \dots, A_r)$.*
2. *Il existe des polynômes $U_1, U_2, \dots, U_r \in \mathbb{K}[X]$ pour lesquels*

$$U_1A_1 + U_2A_2 + \cdots + U_rA_r = \operatorname{pgcd}(A_1, A_2, \dots, A_r).$$

*Une telle relation est appelée **une relation de Bézout** pour $A_1, A_2, \dots, A_r$.*

Définition 78

- On dit que $A_1, A_2, \dots, A_r$ sont **premiers entre eux dans leur ensemble** si 1 est leur seul diviseur commun unitaire, c'est-à-dire lorsque $\operatorname{pgcd}(A_1, A_2, \dots, A_r) = 1$.
- On dit que $A_1, A_2, \dots, A_r$ sont **premiers entre eux deux à deux** si pour tous $i, j \in [\![1, r]\!]$ distincts, les polynômes A_i et A_j sont premiers entre eux.

Si les polynômes $A_1, A_2, \dots, A_r$ sont premiers entre eux deux à deux, alors ils sont premiers entre eux dans leur ensemble. La réciproque est fausse.

28.6 Décomposition en facteurs irréductibles

§1 Théorème fondamental de l'arithmétique des polynômes

Théorème 79

Tout polynôme non nul P admet une factorisation

$$P = CP_1 \dots P_r,$$

où $C \in \mathbb{K}^\star$ et où $P_1, \dots, P_r$ sont irréductibles unitaires. Cette décomposition est unique à l'ordre près des facteurs irréductibles.

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

Théorème 80

Théorème de d'Alembert-Gauß ou T.F.A
Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine.

Démonstration. Théorème admis. ∎

Théorème 81

Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Corollaire 82

Deux polynômes de $\mathbb{C}[X]$ sont premiers entre eux si, et seulement si ils n'ont pas de racine commune.

Théorème 83

Soit $P \in \mathbb{C}[X]$ un polynôme non nul alors P se décompose en facteurs irréductibles

$$P = C(X - a_1)^{m_1}(X - a_2)^{m_2} \cdots (X - a_k)^{m_k}$$

où $a_1, a_2, \ldots, a_k$ sont des scalaires distincts qui sont les zéros de P, et pour tout j, m_j est l'ordre de multiplicité de x_j comme zéro de P, et C est le coefficient directeur de P.

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

Exemple 84

Soit $P = X^3 - 2$. Ses racines sont $\sqrt[3]{2}$, $j\sqrt[3]{2}$, $j^2\sqrt[3]{2}$ et

$$X^3 - 2 = 1\left(X - \sqrt[3]{2}\right)\left(X - j\sqrt[3]{2}\right)\left(X - j^2\sqrt[3]{2}\right).$$

Exemple 85

Décomposons $P = X^n - 1$ dans $\mathbb{C}[X]$.
Pour tout $k \in [\![0, n-1]\!]$, $\omega_k = \mathrm{e}^{2ik\pi/n}$ est une racine de P. Puisque les ω_k sont distincts deux à deux, P possède $n = \deg P$ racines distinctes. De plus, le coefficient dominant de P est 1, on a donc

$$P = X^n - 1 = \prod_{k=0}^{n-1}\left(X - \mathrm{e}^{2ik\pi/n}\right).$$

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

Lemme 86

Soit P un polynôme réel et a un zéro complexe de P. Alors $\overline{a}$ est un zéro de P et les ordres de multiplicité de a et $\overline{a}$ sont égaux.

Théorème 87

Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 dont le discriminant est strictement négatif.

Un polynôme réel de degré > 2 n'est *jamais* irréductible dans $\mathbb{R}[X]$, même s'il n'a aucune racine réelle. Par exemple, $X^4 + 3X^2 + 2 = (X^2 + 1)(X^2 + 2)$.

Méthode

Décomposition en produit de polynômes irréductibles

Soit $P \in \mathbb{R}[X]$. On note $a_1, a_2, \ldots, a_k$ les racines réelles de P, d'ordre de multiplicité $m_1, m_2, \ldots, m_k$. Il existe donc $Q \in \mathbb{R}[X]$ n'ayant aucun zéro réel tel que

$$P(X) = \prod_{k=1}^{s}(X - a_k)^{m_k} \times Q(X).$$

Le polynôme Q est forcément de degré pair puisque tout polynôme de $\mathbb{R}[X]$ de degré impair admet au moins un zéro réel (pourquoi?). Soit $c_1, \ldots, c_r$ les zéros complexes de Q de partie imaginaire > 0. Notons v_i l'ordre de multiplicité de c_i. Les autres zéros de Q sont les conjugués des c_i ; on sait que $\bar{c}_i$ a pour ordre de multiplicité v_i. Donc

$$Q = \lambda(X - c_1)^{v_1}(X - c_2)^{v_2} \cdots (X - c_r)^{v_r}(X - \bar{c}_1)^{v_1}(X - \bar{c}_2)^{v_2} \cdots (X - \bar{c}_r)^{v_r}$$

On regroupe $(X - c_i)(X - \bar{c}_i) = X^2 - 2\,\mathfrak{Re}(c_i) + |c_i|^2 = X^2 + p_iX + q_i$ où p_i et q_i sont des réels tels que $p_i^2 - 4q_i < 0$.

Théorème 88

Tout polynôme $P \in \mathbb{R}[X]$ non nul s'écrit

$$C \prod_{k=1}^{s} (X - a_k)^{m_k} \prod_{i=1}^{r} (X^2 + p_i X + q_i)^{v_i}$$

où C est le coefficient directeur de P, les $a_k \in \mathbb{R}$ sont des réels distincts, les $(p_i, q_i) \in \mathbb{R}^2$ sont des couples distincts de réels tels que $p_i^2 - 4q_i < 0$. Cette décomposition est unique, à l'ordre des facteurs près.

Exemple 89

Soit $P = X^4 + 1$. Les racines de P sont les racines quatrièmes de $-1 = \mathrm{e}^{i\pi}$, c'est-à-dire les $\mathrm{e}^{i(2k+1)\pi/4}$, $k \in [\![0, 3]\!]$. Le coefficient dominant de P est 1, donc

$$\begin{aligned} P &= \left(X - \mathrm{e}^{i\pi/4}\right)\left(X - \mathrm{e}^{7i\pi/4}\right)\left(X - \mathrm{e}^{3i\pi/4}\right)\left(X - \mathrm{e}^{5i\pi/4}\right) \\ &= \left(X^2 - 2\,\mathfrak{Re}\left(\mathrm{e}^{i\pi/4}\right)X + 1\right)\left(X^2 - 2\,\mathfrak{Re}\left(\mathrm{e}^{3i\pi/4}\right)X + 1\right) \\ &= \left(X^2 - \sqrt{2}X + 1\right)\left(X^2 + \sqrt{2}X + 1\right). \end{aligned}$$

Exemple 90

On veut décomposer le polynôme $P = X^n - 1$ dans $\mathbb{R}[X]$. La décomposition de P dans $\mathbb{C}[X]$ est

$$P = X^n - 1 = \prod_{k=0}^{n-1} \left(X - \mathrm{e}^{2ik\pi/n}\right).$$

Le conjugué de $\omega_k = e^{2ik\pi/n}$ est $\mathrm{e}^{-2ik\pi/n} = \mathrm{e}^{2i(n-k)\pi/n} = \omega_{n-k}$. On calcule

$$(X - \omega_k)(X - \omega_{n-k}) = X^2 - 2X\cos\left(\frac{2k\pi}{n}\right) + 1. \tag{28.1}$$

Si n est impair, donc $n = 2m + 1$ où m est entier,

- $\omega_0 = 1$ est la seule racine réelles ;
- Les racines non réelles de P sont les ω_k avec $1 \leq k \leq m$ et leurs conjuguées.

On obtient donc

$$X^{2m+1} - 1 = (X - 1)\prod_{k=1}^{m}\left(X^2 - 2\cos\left(\frac{2k\pi}{2m+1}\right)X + 1\right). \tag{28.2}$$

Si n est pair, donc $n = 2m$ où m est entier,

- Les racines réelles de P sont $\omega_0 = 1$ et $\omega_m = -1$;
- les racines non réelles de P sont les ω_k avec $1 \leq k \leq m - 1$, et leurs conjuguées.

On a donc

$$X^{2m} - 1 = (X - 1)(X + 1)\prod_{k=1}^{m-1}\left(X^2 - 2\cos\left(\frac{k\pi}{m}\right)X + 1\right). \tag{28.3}$$