Table des matières

I Polynômes à coefficients dans $\mathbb{K}$ . . . 2
I.1 Suites de $\mathbb{K}$ à support fini . . . 2
I.2 L'anneau $\mathbb{K}[X]$ . . . 3
I.3 Degré et valuation . . . 4
I.4 Evaluation des polynômes . . . 6
I.5 Dérivation des polynômes . . . 8
II Division dans $\mathbb{K}[X]$, Pgcd et Ppcm . . . 10
II.1 Divisibilité dans $\mathbb{K}[X]$ . . . 10
II.2 Division euclidienne . . . 11
II.3 Algorithme d'Euclide, Pgcd . . . 12
II.4 Polynômes premiers entre eux . . . 16
II.5 Equation $AU + BV = C$ . . . 17
II.6 Ppcm de deux polynômes . . . 18
II.7 Brève extension au cas de plusieurs polynômes . . . 18
III Racines des polynômes, factorisations . . . 19
III.1 Racines d'un polynôme . . . 19
III.2 Racines distinctes, polynômes scindés . . . 20
III.3 Identification entre polynômes et fonctions polynomiales . . . 21
III.4 Relations coefficients-racines pour un polynôme scindé . . . 22
IV Polynômes irréductibles et factorisations . . . 24
IV.1 Polynômes irréductibles . . . 24
IV.2 Factorisation dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$ . . . 25
V Fractions rationnelles . . . 27
V.1 Le corps des fractions rationnelles . . . 27
V.2 Opérations diverses sur fractions rationnelles . . . 28
V.3 Degré, partie entière . . . 29
V.4 Pôles et partie polaires . . . 30
V.5 Décomposition en éléments simples . . . 32
V.6 Pratique de la décomposition en éléments simples . . . 34
V.7 Exemples de référence . . . 35

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 37 pages.

I Polynômes à coefficients dans $\mathbb{K}$

Dans tout ce chapitre $\mathbb{K}$ désigne un corps commutatif (le plus souvent $\mathbb{R}$ ou $\mathbb{C}$).

I.1 Suites de $\mathbb{K}$ à support fini

Définition

Soit $a=(a_k)_{k\geq 0}$ un élément de $\mathbb{K}^{\mathbb{N}}$, c'est-à-dire une suite à valeurs dans $\mathbb{K}$.
On appelle *support* de a l'ensemble (éventuellement vide) des indices k tels que $a_k\neq 0$.
On note $\mathbb{K}^{(\mathbb{N})}$ l'ensemble des suites de $\mathbb{K}$ qui sont à support fini.

Remarques

- La suite $a=(a_k)_{k\geq 0}$ est à support fini$\Leftrightarrow$il existe un n dans $\mathbb{N}$ tel que : $\forall\, k>n, a_k=0$.
  On peut alors noter symboliquement $a=(a_0,a_1,\dots,a_n,0,0,\dots)$.
- Soient $a=(a_k)_{k\geq 0}$ et $b=(b_k)_{k\geq 0}$ deux éléments de $\mathbb{K}^{(\mathbb{N})}$.
  $a+b=(a_k+b_k)_{k\geq 0}$ est encore un élément de $\mathbb{K}^{(\mathbb{N})}$.
  Pour cette loi, $\mathbb{K}^{(\mathbb{N})}$ a une structure de groupe commutatif :
  - ◇ L'élément neutre est la suite nulle.
  - ◇ L'opposé de la suite $(a_k)_{k\geq 0}$ est la suite $(-a_k)_{k\geq 0}$.
- Si $a=(a_k)_{k\geq 0}$ est dans $\mathbb{K}^{(\mathbb{N})}$, et si λ est dans $\mathbb{K}$ on pose $\lambda a=(\lambda a_k)_{k\geq 0}$.
  La suite λa est encore un élément de $\mathbb{K}^{(\mathbb{N})}$.
  Pour désigner cette opération $(\lambda,a)\mapsto\lambda a$, on parle de la *loi externe* sur $\mathbb{K}^{(\mathbb{N})}$.
- On peut définir ce qu'on appelle des *combinaisons linéaires* dans $\mathbb{K}^{(\mathbb{N})}$.
  Par exemple si $a=(a_k)_{k\geq 0}$, $b=(b_k)_{k\geq 0}$ et $c=(c_k)_{k\geq 0}$ sont trois éléments de $\mathbb{K}^{(\mathbb{N})}$, et si α,β,γ sont trois scalaires (c'est-à-dire trois éléments de $\mathbb{K}$), alors $d=\alpha a+\beta b+\gamma c$ désigne la suite à support fini dont le terme général est $d_k=\alpha a_k+\beta b_k+\gamma c_k$.
  On dit que d est une combinaison linéaire de a,b,c, avec les coefficients α,β,γ.
- Pour tout n dans $\mathbb{N}$, notons $e_n=(a_k)_{k\geq 0}$ l'élément de $\mathbb{K}^{(\mathbb{N})}$ défini par $\begin{cases} a_n=1\\ a_k=0 \text{ si } k\neq n\end{cases}$
  Ainsi $e_0=(1,0,0\dots)$, $e_1=(0,1,0,0,\dots)$, $e_2=(0,0,1,0,0,\dots)$.
- On remarque par exemple que $a=(3,0,1,-2,0,0,4,0,0,\dots)$ s'écrit $a=3e_0+e_2-2e_3+4e_6$.
  Plus généralement, soit $a=(a_0,a_1,\dots,a_n,0,0,\dots)$ un élément de $\mathbb{K}^{(\mathbb{N})}$.
  Alors a s'écrit $a=a_0e_0+a_1e_1+\cdots+a_ne_n=\sum_{k=0}^{n}a_ke_k$.
  On notera aussi $a=\sum_{k\geq 0}a_ke_k$ ou $a=\sum_{k=0}^{+\infty}a_ke_k$, en se souvenant que cette somme est finie.
  L'écriture de a comme *combinaison linéaire* des e_n est unique, à l'ordre près.

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 37 pages.

I.2 L'anneau $\mathbb{K}[X]$

Définition *(un produit sur $\mathbb{K}^{(\mathbb{N})}$)*

Soient $a=(a_k)_{k\geq 0}$ et $b=(b_k)_{k\geq 0}$ deux éléments de $\mathbb{K}^{(\mathbb{N})}$.
On définit une suite à support fini $c=ab$ en posant : $\forall\, n\in\mathbb{N}, c_n=\sum\limits_{j+k=n} a_j\, b_k$.

Remarques et propriétés

– La définition précédente peut aussi s'écrire : $\forall\, n\in\mathbb{N}, c_n=\sum\limits_{k=0}^{n} a_{n-k}b_k=\sum\limits_{k=0}^{n} a_k b_{n-k}$.
En particulier $c_0=a_0b_0$, $c_1=a_0b_1+a_1b_0$, $c_2=a_0b_2+a_1b_1+a_2b_0$, etc.

– On sait qu'il existe $m\in\mathbb{N}$ tel que $j\geq m\Rightarrow a_j=0$ et $p\in\mathbb{N}$ tel que $k\geq p\Rightarrow b_k=0$.
On en déduit que si $n=j+k\geq m+p-1$, alors :
◇ Ou bien $j\geq m$ et alors $a_j=0$.
◇ Ou bien $j\leq m-1$ et alors $k\geq m+p-1-j\geq p$, donc $b_k=0$.
Ainsi $n\geq m+p-1\Rightarrow c_n=0$, ce qui prouve que la suite c est à support fini.

– La loi produit sur $\mathbb{K}^{(\mathbb{N})}$ est commutative, associative, distributive par rapport à l'addition.
La suite $e_0=(1,0,0,\ldots)$ est élément neutre pour ce produit.

– Pour tous indices j et k, on remarque que $e_je_k=e_{j+k}$.
On en déduit que pour tout n de $\mathbb{N}$, on a $e_n=e_1^n$ (en posant $e_1^0=e_0$).

Définition

Muni de la loi + "naturelle" et de la loi $\times$ précédente, $\mathbb{K}^{(\mathbb{N})}$ est donc un anneau commutatif.
Les éléments de cet anneau sont appelés *polynômes à coefficients dans* $\mathbb{K}$.

Notation définitive des polynômes

– L'application $\varphi:\mathbb{K}\to\mathbb{K}^{(\mathbb{N})}$ définie par $\varphi(\lambda)=\lambda e_0$ est un morphisme injectif d'anneaux.
φ est donc un isomorphisme de $\mathbb{K}$ sur son image $\{P=\lambda e_0,\lambda\in\mathbb{K}\}$.
On peut ainsi identifier λe_0 et λ. On posera donc $e_0=1$ et on écrira $P=\lambda e_0=\lambda$.

– On pose $\mathrm{X}=e_1=(0,1,0,0,\ldots)$.
Avec cette notation, $\mathrm{X}^n=e_n=(0,\ldots,0,1,0,0,\ldots)$, et en particulier $\mathrm{X}^0=e_0=1$.
$P=(a_k)_{k\geq 0}$ s'écrit donc $P=\sum\limits_{k\geq 0} a_k\mathrm{X}^k=\sum\limits_{k=0}^{+\infty} a_k\mathrm{X}^k=a_0+a_1\mathrm{X}+\cdots+a_n\mathrm{X}^n+\cdots$
Une telle somme, toujours finie, représente P de façon unique (à l'ordre près).
On dit que les a_k sont les *coefficients* de P.
Si n est un entier tel que $k>n\Rightarrow a_k=0$, on notera aussi $P=\sum\limits_{k=0}^{n} a_k\mathrm{X}^k$.

– L'unicité de l'écriture $P=\sum\limits_{k\geq 0} a_k\mathrm{X}^k$ permet de procéder à des identifications.
En particulier, P est le polynôme nul si et seulement si tous ses coefficients sont nuls.
De même, on a l'équivalence : $\sum\limits_{k\geq 0} a_k\mathrm{X}^k=\sum\limits_{k\geq 0} b_k\mathrm{X}^k\Leftrightarrow\forall\, k\in\mathbb{N}, a_k=b_k$.

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 37 pages.

- On notera maintenant $\mathbb{K}[X]$ l'anneau des polynômes à coefficients dans $\mathbb{K}$.
- Les lois sur $\mathbb{K}[X]$ sont donc définies par :
  - ◇ Produit d'un polynôme par un scalaire : $\lambda \sum_{k\geq 0} a_k X^k = \sum_{k\geq 0} (\lambda a_k) X^k$
  - ◇ Somme de deux polynômes : $\sum_{k\geq 0} a_k X^k + \sum_{k\geq 0} b_k X^k = \sum_{k\geq 0} (a_k + b_k) X^k$
  - ◇ Produit de deux polynômes : $\left(\sum_{k\geq 0} a_k X^k\right)\left(\sum_{k\geq 0} b_k X^k\right) = \sum_{k\geq 0} \left(\sum_{i+j=k} a_i\, b_j\right) X^k$
- Soit P un élément de $\mathbb{K}[X]$.
  On dit que P est un *monôme* s'il s'écrit $P = \lambda X^n$, avec $\lambda \in \mathbb{K}$ et $n \in \mathbb{N}$.
  On dit que P est un *polynôme constant* si $P = \lambda$, avec $\lambda \in \mathbb{K}$.
- Dans la notation $\mathbb{K}[X]$, on dit que le polynôme X est l'*indéterminée*. Il est évident que le choix de la lettre X est assez arbitraire (quoique classique) et qu'on peut très bien travailler sur des polynômes de l'indéterminée Y par exemple.
  On peut même définir l'anneau $\mathbb{K}[X, Y]$ des polynômes aux indéterminées X, Y (c'est-à-dire des sommes de monômes $\lambda_{m,n} X^m Y^n$, comme $P = 1 - X + X^4Y + 2XY^2 + Y^3$) mais cette notion est hors-programme.

I.3 Degré et valuation

Définition

Soit $P = \sum_{k\geq 0} a_k X^k$ un polynôme non nul de $\mathbb{K}[X]$.
On appelle *degré* de P et on note $\deg(P)$ l'entier k maximum tel que $a_k \neq 0$.
On appelle *valuation* de P et on note $\mathrm{val}\,(P)$ l'entier k minimum tel que $a_k \neq 0$.
Par convention, on pose $\deg(0) = -\infty$ et $\mathrm{val}\,(0) = +\infty$.

Exemples et remarques

- Le polynôme $P = 3X^2 + X^3 - 2X^5 + X^7$ est de valuation 2 et de degré 7.
- Si $P = \sum_{k\geq 0} a_k X^k$, on dit que a_k est le coefficient du terme ou du monôme de degré k dans P.
  On dit que a_0 est le coefficient *constant* de P.
- Les polynômes sont en général écrits suivant les degrés croissants ($P = 3X^2 + X^3 - 2X^5 + X^7$) ou suivant les degrés décroissants ($P = X^7 - 2X^5 + X^3 + 3X^2$). Ce choix n'est souvent qu'une question de "confort" (identification de coefficients, division de deux polynômes, etc.)
- On a $\mathrm{val}\,(P) = 0$ si et seulement si le coefficient constant de P est non nul.
  écrire que $\deg(P)$ appartient à $\mathbb{N}$, c'est écrire que P est non nul.
  écrire que $\deg(P) \geq 1$, c'est écrire que P n'est pas un polynôme constant.
- Soit $P = \sum_{k\geq 0} a_k X^k$ un polynôme non nul, et soit $n = \deg(P) \geq 0$.
  On dit que a_n est le coefficient *dominant* de P.
  On dit que le polynôme P est *normalisé* (ou encore *unitaire*) si $a_n = 1$.

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 37 pages.

Proposition *(degré et valuation d'une somme ou d'un produit)*

Soient A et B deux éléments de $\mathbb{K}[X]$. On a les résultats suivants :

- $\deg(A+B) \leq \max(\deg(A), \deg(B))$, avec égalité si $\deg(A) \neq \deg(B)$.
- $\text{val}\,(A+B) \geq \min(\text{val}\,(A), \text{val}\,(B))$, avec égalité si $\text{val}\,(A) \neq \text{val}\,(B)$.
- $\deg(AB) = \deg(A) + \deg(B)$.
- $\text{val}\,(AB) = \text{val}\,(A) + \text{val}\,(B)$.

Proposition *(intégrité de l'anneau $\mathbb{K}[X]$)*

L'égalité $\deg(AB) = \deg(A) + \deg(B)$ montre que si $A \neq 0$ et $B \neq 0$ alors $AB \neq 0$.
Autrement dit $AB = 0 \Rightarrow (A = 0 \text{ ou } B = 0)$.
Plus généralement, si $A_1 A_2 \dots A_n = 0$, alors l'un au moins des A_k est nul.
Autre interprétation : tout polynôme non nul est simplifiable pour le produit.
Conclusion : $\mathbb{K}[X]$ est un anneau intègre.

Proposition *(éléments inversibles de $\mathbb{K}[X]$)*

Soient A et B deux éléments de $\mathbb{K}[X]$.
On a $AB = 1$ si et seulement si A et B sont des constantes inverses l'une de l'autre.
Les seuls éléments inversibles pour le produit dans l'anneau $\mathbb{K}[X]$ sont donc les polynômes de degré 0, c'est-à-dire les polynômes constants non nuls.

Remarques

- Les résultats de la proposition précédente sont valables y compris si A ou B est nul, avec les conventions $\deg(0) = -\infty$, $\text{val}\,(0) = +\infty$ et les règles de calculs habituelles avec $\pm\infty$.
- Si $\deg(A) = \deg(B) = n$, on peut avoir $\deg(A+B) < n$.
  Il suffit pour cela que les termes de plus haut degré de A et B se "neutralisent".
  Par exemple, si $\begin{cases} A = X^3 + X \\ B = -X^3 + 1 \end{cases}$, alors $A + B = X + 1$ et $\deg(A+B) = 1 < 3$.
  On peut aussi prendre l'exemple extrême $B = -A$, car alors $\deg(A+B) = -\infty$.
- De la même manière, on peut avoir $\text{val}\,(A+B) > n$ si $\text{val}\,(A) = \text{val}\,(B) = n$.
  Par exemple, si $\begin{cases} A = X^3 + X \\ B = X^2 - X \end{cases}$, on a $A + B = X^3 + X^2$ et $\text{val}\,(A+B) = 2 > 1$.
  De même, si on choisit $B = -A$, alors $\text{val}\,(A+B) = +\infty$.
- Pour tout A dans $\mathbb{K}[X]$ et pour tout λ dans $\mathbb{K}$, on a $\begin{cases} \deg(\lambda A) = \deg(A) & \text{si } \lambda \neq 0 \\ \deg(\lambda A) = -\infty & \text{si } \lambda = 0 \end{cases}$
- On a $\deg(A_1 A_2 \cdots A_n) = \sum_{k=1}^{n} \deg(A_k)$. En particulier $\deg(A^n) = n \deg(A)$.
  Pour tous scalaires λ_k, on a $\deg\left(\sum_{k=1}^{n} \lambda_k A_k\right) \leq \max_{k=1,..,n} (\deg(A_k))$.
  Dans ce dernier résultat, si l'un des A_k est de degré supérieur aux autres et si le coefficient λ_k correspondant est non nul, alors il y a égalité.

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 37 pages.

I.4 Evaluation des polynômes

Définition *(Composition de deux polynômes)*

Soit $A = \sum_{k\geq 0} a_k X^k$ un élément de $\mathbb{K}[X]$.

Pour tout polynôme B, on pose $A(B) = \sum_{k\geq 0} a_k B^k$.

On dit que $A(B)$ est le composé du polynôme B par le polynôme A.

Remarques et propriétés

- Un exemple : posons $A = X^3 + X + 1$ et $B = X^2 - 1$.
  Alors $A(B) = B^3 + B + 1 = (X^2-1)^3 + (X^2-1) + 1 = X^6 - 3X^4 + 4X^2 - 1$.
- Si $B = X$, alors $A(B) = A$. Ceci justifie qu'on note souvent $A(X)$ un polynôme de $\mathbb{K}[X]$.
- Un cas classique est le calcul des polynômes $A(X+h)$, appelés *translatés* du polynôme A.
  Par exemple : $A = aX^2 + bX + 1 \Rightarrow A(X+1) = aX^2 + (2a+b)X + a + b + 1$.
- Pour tous polynômes non nuls A et B, on a $\deg(A(B)) = \deg(A)\deg(B)$.
- Pour tous polynômes A, B, C, on a $(AB)(C) = A(C)B(C)$

Définition *(Fonction polynomiale associée)*

Soit $A = \sum_{k\geq 0} a_k X^k$ un élément de $\mathbb{K}[X]$. Pour tout λ de $\mathbb{K}$, on pose $A(\lambda) = \sum_{k\geq 0} a_k \lambda^k$.

On dit que $A(\lambda)$ est la *valeur* du polynôme A en λ.

Remarques et propriétés

- $A(0)$ est le coefficient constant de A ; $A(1)$ est la somme de ses coefficients.
- Le calcul de $A(\lambda)$ est un cas particulier de composition. On compose en effet ici le polynôme constant λ par le polynôme A, et on obtient un polynôme constant.
- Les notations sont trompeuses. Par définition, un polynôme A n'est pas une application de $\mathbb{K}$ dans $\mathbb{K}$. A priori on ne doit donc pas le confondre avec celle qui à tout λ associe $A(\lambda)$.
  Cette application est appelée *fonction polynomiale* associée au polynôme A.
  Pour éviter tout risque de confusion, on peut (du moins dans un premier temps) la noter $\widetilde{A}$.
- Avec ces notations, et pour tous A, B dans $\mathbb{K}[X]$, on a $\begin{cases} \widetilde{A+B} = \widetilde{A} + \widetilde{B} \\ \widetilde{AB} = \widetilde{A}\,\widetilde{B} \end{cases}$
  Notons φ l'application de $\mathbb{K}[X]$ dans $\mathcal{F}(\mathbb{K},\mathbb{K})$ définie par $\varphi(A) = \widetilde{A}$.
  L'image du polynôme 1 (le neutre de $\mathbb{K}[X]$ pour le produit) est la fonction constante $\lambda \mapsto 1$ (le neutre de $\mathcal{F}(\mathbb{K},\mathbb{K})$ pour le produit des fonctions).
  Ainsi φ est un morphisme de l'anneau $(\mathbb{K}[X], +, \times)$ dans l'anneau $(\mathcal{F}(\mathbb{K},\mathbb{K}), +, \times)$.
  On verra que si $\mathbb{K}$ est infini (notamment si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$) alors φ est injective et réalise donc un isomorphisme de $\mathbb{K}[X]$ sur son image c'est-à-dire sur l'ensemble des *fonctions polynomiales*.
  Dans ce cas, on pourra identifier un polynôme avec la fonction polynomiale associée.

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 37 pages.

Schéma de Horner

– Soit $A = \sum_{k\geq 0} a_k \mathrm{X}^k$ un polynôme, et λ un scalaire.

On va voir comment calculer $A(\lambda)$ en un minimum d'opérations.

Posons par exemple $A = a_4\mathrm{X}^4 + a_3\mathrm{X}^3 + a_2\mathrm{X}^2 + a_1\mathrm{X} + a_0$.

◇ Le calcul de $A(\lambda) = a_4\lambda^4 + a_3\lambda^3 + a_2\lambda^2 + a_1\lambda + a_0$ nécessite à priori 14 opérations.

◇ On remarque qu'on peut écrire $A(\lambda) = (((a_4\lambda + a_3)\lambda + a_2)\,\lambda + a_1)\,\lambda + a_0$.
Sous cette forme, le calcul de $A(\lambda)$ nécessite 8 opérations.

◇ Tout repose donc sur l'expression $A = (((a_4\mathrm{X} + a_3)\mathrm{X} + a_2)\,\mathrm{X} + a_1)\,\mathrm{X} + a_0$.
On dit que cette expression est le *schéma de Horner* du polynôme A.
Elle est particulièrement adaptée si on souhaite effectuer de nombreuses évaluations de A.

Plus généralement, $A = \sum_{k=0}^{n} a_k \mathrm{X}^k = ((\cdots((a_n\mathrm{X} + a_{n-1})\mathrm{X} + a_{n-2})\,\mathrm{X} + \cdots)\,\mathrm{X} + a_1)\,\mathrm{X} + a_0$

– Voici une procédure Maple permettant d'évaluer un polynôme A en un point x, et utilisant l'algorithme de Horner sous forme itérative.

A est représenté par la liste $[a_n, \ldots, a_0]$ de ses coefficients dans l'ordre des degrés décroissants :

```
> horner:=proc(a::list,x)
    local c,t:
    t:=0; for c in a do t:=t*x+c od;
  end:
```

On teste cette fonction sur un polynôme $A = \sum_{k=0}^{5} a_k \mathrm{X}^k$:

```
> A:=[a[5-k]$k=0..5]; horner(A,X);
```

$$A := [a_5, a_4, a_3, a_2, a_1, a_0]$$

$$((((a_5X + a_4)X + a_3)X + a_2)X + a_1)X + a_0$$

Voici maintenant une version récursive de l'algorithme de Horner :

```
> horner2:=proc(a::list,x) local n;
    if a=[] then 0 else n:=nops(a); horner2(a[1..n-1],x)*x+a[n] fi
  end:
```

Et on vérifie avec le même exemple :

```
> horner2(A,X);
```

$$((((a_5X + a_4)X + a_3)X + a_2)X + a_1)X + a_0$$

La fonction intégrée *convert* possède une option permettant de convertir un polynôme (exprimé sous forme algébrique) en sa forme de Horner.

Voici comment on retrouve le résultat précédent :

```
> A:=sum(a[k]*X^k,k=0..5); convert(A,horner,X);
```

$$A := a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 + a_5X^5$$

$$((((a_5X + a_4)X + a_3)X + a_2)X + a_1)X + a_0$$

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 37 pages.

I.5 Dérivation des polynômes

Dans tout ce paragraphe, et à chaque fois qu'il sera question de polynôme dérivé, on suppose que le corps $\mathbb{K}$ est infini, ce qui revient à dire qu'il contient le corps $\mathbb{Q}$ des rationnels.

Cette précaution est nécessaire pour qu'on ait l'implication $n\lambda = 0 \Rightarrow \lambda = 0$ quand $n \in \mathbb{N}^*$.

Autrement dit, tout élément est d'ordre 0 dans le groupe additif $(\mathbb{K}, +)$.

Définition *(Polynôme dérivé)*

Soit $A = \sum_{k\geq 0} a_k X^k$ un élément de $\mathbb{K}[X]$.
On appelle *polynôme dérivé* de A, le polynôme noté A' et égal à $\sum_{k\geq 0} (k+1)a_{k+1}X^k$.

Remarques et propriétés

- Par exemple, si $A = aX^3 + bX^2 + cX + d$ alors $A' = 3aX^2 + 2bX + c$.
- Si $A = \sum_{k=0}^{n} a_k X^k$, alors $A' = \sum_{k=0}^{n-1} (k+1)a_{k+1}X^k$, ou encore $A' = \sum_{k=1}^{n} k a_k X^{k-1}$.
- Si $\mathbb{K} = \mathbb{R}$, alors la fonction polynomiale associée au polynôme A' est bien la dérivée (au sens habituel donné à ce nom) de la fonction polynomiale associée à A. Il faut ici se limiter à $\mathbb{K} = \mathbb{R}$ car le programme impose de ne dériver que des fonctions d'une variable réelle.
- Pour A, B dans $\mathbb{K}[X]$, et λ, μ dans $\mathbb{K}$, on a : $(\lambda A + \mu B)' = \lambda A' + \mu B'$ et $(AB)' = A'B + AB'$.
- Si $\deg(A) \geq 1$ on a $\deg(A') = \deg(A) - 1$ (c'est là qu'intervient l'hypothèse "$\mathbb{K}$ infini".)
  Pour cette raison, A' est le polynôme nul si et seulement si A est un polynôme constant.
  Plus généralement : $\forall (A, B) \in \mathbb{K}[X]^2,\ A' = B' \Leftrightarrow \exists\, \lambda \in \mathbb{K},\ A = B + \lambda$.

Définition *(Polynômes dérivés successifs)*

Soit A un élément de $\mathbb{K}[X]$.
On définit les polynômes dérivés successifs de A en posant $\begin{cases} A^{(0)} = A \\ \forall\, m \in \mathbb{N},\ A^{(m+1)} = (A^{(m)})' \end{cases}$
On dit que $A^{(m)}$ est le polynôme dérivé m-ième de A.

Remarques et propriétés

- On note bien sûr A' et A'' plutôt que $A^{(1)}$ et $A^{(2)}$.
- Si $A = \sum_{k\geq 0} a_k X^k$, alors $A^{(m)} = \sum_{k\geq m} \frac{k!}{(k-m)!} a_k X^{k-m} = \sum_{k\geq 0} \frac{(k+m)!}{k!} a_{k+m} X^k$.
- Si $\deg(A) = n \geq m$, on a $\deg(A^{(m)}) = n - m$.
  Si $A = \sum_{k=0}^{n} a_k X^k$, alors $A^{(m)} = \sum_{k=0}^{n-m} \frac{(k+m)!}{m!} a_{k+m} X^k$, ou encore $A^{(m)} = \sum_{k=m}^{n} \frac{k!}{(k-m)!} a_k X^{k-m}$.
  On a $A^{(m)} = 0$ si et seulement si $\deg(A) < m$.
- Si $m \leq k$, on a $(X^k)^{(m)} = k(k-1)\cdots(k-m+1)X^{k-m} = \frac{k!}{(k-m)!} X^{k-m}$.
  En particulier, $(X^m)^{(m)} = m!$, et si $m > k$ on a bien sûr $(X^k)^{(m)} = 0$.
- Si $P = \sum_{k\geq 0} a_k X^k$ est de degré n, alors $P^{(n)}$ est le polynôme constant $n!\, a_n$.

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 37 pages.

– On a toujours la propriété de linéarité : $(\lambda A+\mu B)^{(n)}=\lambda A^{(n)}+\mu B^{(n)}$.

Proposition *(formule de Leibniz)*

Soient A, B dans $\mathbb{K}[X]$, et m dans $\mathbb{N}$. On a $(AB)^{(m)}=\sum_{k=0}^{m}\binom{m}{k}A^{(k)}B^{(m-k)}$.

Remarque

On retrouve $(AB)'=A'B+AB'$, mais on a aussi $\begin{cases}(AB)''=A''B+2A'B'+AB''\\(AB)'''=A'''B+3A''B'+3A'B''+AB'''\end{cases}$

On se méfiera de l'analogie entre $(A+B)^{(n)}$ dans $\mathbb{K}[X]$ et $(a+b)^n$ dans $\mathbb{K}$.

En effet on a $A^{(0)}=A$ et $B^{(0)}=B$ aux "extrémités", alors que dans $\mathbb{K}$ on a $a^0=b^0=1$.

Proposition *(formule de Taylor en un point)*

Soit $A=\sum_{k\geq 0}a_kX^k$ un élément de $\mathbb{K}[X]$, et soit λ un élément de $\mathbb{K}$.

On a l'égalité : $A=A(\lambda)+A'(\lambda)(X-\lambda)+\frac{A''(\lambda)}{2!}(X-\lambda)^2+\cdots=\sum_{k\geq 0}\frac{A^{(k)}(\lambda)}{k!}(X-\lambda)^k$

Remarques

– La somme précédente est finie, et si $\deg(A)=n$ son dernier terme est $\frac{A^{(n)}(\lambda)}{n!}(X-\lambda)^n$.

– La formule de Taylor montre qu'un polynôme est entièrement déterminé par la valeur de ses dérivées successives en un point.

– Le cas particulier $\lambda=0$ est connu sous le nom de *formule de Mac Laurin*.

Si $A=\sum_{k\geq 0}a_kX^k$, alors $A=\sum_{k\geq 0}\frac{A^{(k)}(0)}{k!}X^k$. Ainsi : $\forall\, k\geq 0, a_k=\frac{A^{(k)}(0)}{k!}$.

– On a l'équivalence : $A(X)=\sum_{k\geq 0}\frac{A^{(k)}(\lambda)}{k!}(X-\lambda)^k \Leftrightarrow A(X+\lambda)=\sum_{k\geq 0}\frac{A^{(k)}(\lambda)}{k!}X^k$.

– La procédure suivante calcule les coefficients de $B(X)=A(X+\lambda)$, où A et B sont représentés par la liste de leurs coefficients dans l'ordre des degrés croissants.

```
> transpol:=proc(A::list,h) local j,k,a: a:=A;
    for j to nops(A)-1 do
      for k from j to 1 by -1 do a[k+1]:=a[k+1]+h*a[k] od;
    od; a:
  end:
```

Voici un exemple d'utilisation, avec $A=X^4+2X^3-X+1$ et $h=2$:

```
> A:=[1,2,0,-1,1]: A,transpol(A,2);
```

$$[1,2,0,-1,1],\quad [1,10,36,55,31]$$

Ce résultat signifie que $\begin{cases}A(X+2)=X^4+10X^3+36X^2+55X+31 \text{ ou encore :}\\A(X)=(X-2)^4+10(X-2)^3+36(X-2)^2+55(X-2)+31\end{cases}$

On vérifie avec la fonction *taylor*, intégrée à Maple :

```
> A:=sum(A[5-k]*X^k,k=0..4); taylor(A,X=2);
```

$$A:=1-X+2X^3+X^4$$

$$31+55(X-2)+36(X-2)^2+10(X-2)^3+(X-2)^4$$

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 37 pages.

II Division dans $\mathbb{K}[X]$, Pgcd et Ppcm

II.1 Divisibilité dans $\mathbb{K}[X]$

Définition *(multiples et diviseurs)*

Soient A et B deux éléments de $\mathbb{K}$[X].

On dit que B est un *diviseur* de A, ou encore que A est un *multiple* de B, et on note $B \mid A$, s'il existe un polynôme Q tel que $A = BQ$.

On note $\mathcal{D}(A)$ l'ensemble des diviseurs du polynôme A, et $A\mathbb{K}$[X] l'ensemble de ses multiples.

Remarques et propriétés

- Le polynôme nul est un multiple de tout polynôme B (en effet on a $0 = 0B$) mais il ne divise que lui-même (car $A = Q0 \Rightarrow A = 0$.)
  Autrement dit $\mathcal{D}(0) = \mathbb{K}$[X] et $0\mathbb{K}$[X] $= \{0\}$.
  Si $A = \lambda \in \mathbb{K}^*$ alors A divise tout polynôme B (car $B = QA$ avec $Q = \frac{1}{\lambda}B$).
  Mais $\lambda \neq 0$ n'est multiple que des polynômes constants non nuls ($BQ = \lambda \Rightarrow \deg(B) = 0$).
  Autrement dit, pour tout λ de $\mathbb{K}^*$: $\mathcal{D}(\lambda) = \mathbb{K}^*$ et $\lambda\mathbb{K}$[X] $= \mathbb{K}$[X].
- Si $A = BQ$ avec $B \neq 0$, alors Q (le *quotient exact* de A par B) est défini de façon unique.
  étant donnés deux polynômes A, B, avec $B \neq 0$, il est exceptionnel que B divise A.
  Si cela se produit, on évitera cependant de noter $\frac{A}{B}$ leur quotient exact.
- En posant $A \mid B$, on définit une relation binaire sur $\mathbb{K}$[X] qui est réflexive et transitive.
  Mais elle n'est pas antisymétrique (donc ce n'est pas une relation d'ordre).
  On a en effet : $(A \mid B$ et $B \mid A) \Leftrightarrow (\exists\, \lambda \in \mathbb{K}^*,\ A = \lambda B)$.
  On exprime cette situation en disant que les polynômes A et B sont *associés*.
  Si on suppose que A et B sont unitaires : $(A \mid B$ et $B \mid A) \Leftrightarrow A = B$.
- Si deux polynômes sont associés, alors ils ont les mêmes diviseurs (réciproque vraie).
  Si deux polynômes sont associés, alors ils ont les mêmes multiples (réciproque vraie).
- Soit A un polynôme non nul, et soit λ le coefficient de plus haut degré de A.
  Le polynôme $A^* = \frac{1}{\lambda}A$ est appelé le *normalisé* de A.
  Deux polynômes non nuls sont associés s'ils ont le même normalisé.
- Soit A un polynôme non nul.
  A^* est l'unique polynôme normalisé tel que $\mathcal{D}(A^*) = \mathcal{D}(A)$.
  Il est l'unique polynôme normalisé tel que $A\mathbb{K}$[X] $= A^*\mathbb{K}$[X].
- Pour tous polynômes A, B, on a : $A\mathbb{K}$[X] $\subset B\mathbb{K}$[X] $\Leftrightarrow B \mid A \Leftrightarrow \mathcal{D}(B) \subset \mathcal{D}(A)$.
  On en déduit $A\mathbb{K}$[X] $= B\mathbb{K}$[X] $\Leftrightarrow A^* = B^* \Leftrightarrow \mathcal{D}(A) = \mathcal{D}(B)$.

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 37 pages.

II.2 Division euclidienne

Proposition

Soient A et B deux éléments de $\mathbb{K}[X]$, avec $B \neq 0$.
Il existe un unique couple (Q, R) de polynômes tels que $\begin{cases} A = QB + R \\ \deg(R) < \deg B \end{cases}$
Le passage du couple (A, B) au couple (Q, R) s'appelle *division euclidienne* de A par B.
Dans cette division, A est le *dividende*, B le *diviseur*, Q le *quotient* et R le *reste*.

Remarques et propriétés

- Il ne faut jamais oublier de mentionner la condition $\deg(R) < \deg(B)$.
- Si $\deg(A) < \deg(B)$, la division euclidienne de A par B s'écrit $A = 0B + A$.
- Si $B \neq 0$, dire que B divise A, c'est dire que le reste dans la division de A par B est nul.
- Soit A dans $\mathbb{K}[X]$ et α dans $\mathbb{K}$.
  Le reste dans la division de A par $(X - \alpha)$ est la constante $A(\alpha)$.
- Plus généralement si $A = QB + R$ et si $B(\alpha) = 0$ alors $A(\alpha) = R(\alpha)$.
  Supposons par exemple qu'on veuille calculer $A(\alpha)$ avec $\deg(A) \geq 2$ et $\alpha = \frac{-1+\sqrt{13}}{2}$.
  Il est sans doute plus commode de diviser par $B = X^2 + X - 3$ car $B(\alpha) = 0$.
  Le reste R s'écrit en effet $R = aX + b$ et on a alors $A(\alpha) = a\alpha + b$.
- Soient $\mathbb{K}$ et $\mathbb{K}'$ deux corps, $\mathbb{K}$ étant un sous-corps de $\mathbb{K}'$.
  Soient A, B deux éléments de $\mathbb{K}[X]$, le polynôme B étant non nul.
  Soit $A = BQ + R$ la division euclidienne de A par B dans $\mathbb{K}[X]$.
  Par unicité, cette égalité représente aussi la division euclidienne de A par B dans $\mathbb{K}'[X]$.
  Cette propriété est souvent utilisée avec $\mathbb{K} = \mathbb{R}$ et $\mathbb{K}' = \mathbb{C}$: on part d'une division dans $\mathbb{R}[X]$, et on la considère momentanément comme une division dans $\mathbb{C}[X]$, le temps de substituer à X un nombre complexe (souvent une racine complexe du polynôme B).
- Voici un exemple de division euclidienne.
  On divise ici le polynôme $A = X^5 + 2X^3 - X^2 - 4X + 3$ par le polynôme $B = X^2 + 3X + 1$.

$$\begin{array}{rrrrrrrrrrrr|l}
X^5 & & + & 2X^3 & - & X^2 & - & 4X & + & 3 & \multicolumn{2}{|l}{X^2 + 3X + 1} \\
\cline{12-13}
 & - & 3X^4 & + & X^3 & - & X^2 & - & 4X & + & 3 & X^3 - 3X^2 + 10X - 28 \\
 & & & & 10X^3 & + & 2X^2 & - & 4X & + & 3 & \\
 & & & & & - & 28X^2 & - & 14X & + & 3 & \\
 & & & & & & & & 70X & + & 31 &
\end{array}$$

Ainsi $A = BQ + R$ avec $\begin{cases} Q = X^3 - 3X^2 + 10X - 28 \\ R = 70X + 31 \end{cases}$

 ©EduKlub S.A.
Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 37 pages.

Programmation Maple

– Voici une procédure Maple qui effectue la division euclidienne d'un polynôme A par un polynôme B (représentés par la liste de leurs coefficients suivant les degrés décroissants). Cette procédure renvoie la liste formée du quotient puis du reste. Remarquer les instructions du type `subsop(1=NULL,L)` pour supprimer le premier élément d'une liste L.

```
> division:=proc(A::list,B::list) local r,b,q,k,t; r:=A; b:=B;
    while nops(r)>=2 and r[1]=0 do r:=subsop(1=NULL,r) od;
    while nops(b)>=1 and b[1]=0 do b:=subsop(1=NULL,b) od;
    if nops(b)=0 then ERROR("Diviseur nul") fi;
    if nops(r)<nops(b) then [[0],r] else q:=NULL;
      to nops(r)-nops(b)+1 do t:=r[1]/b[1]; q:=q,t;
        for k to nops(b) do r[k]:=r[k]-t*b[k] od;
        r:=subsop(1=NULL,r);
      od;
      while nops(r)>=2 and r[1]=0 do r:=subsop(1=NULL,r) od; [[q],r];
    fi
  end:
```

– A titre d'exemple, on reprend la division précédente :

```
> division([1,0,2,-1,-4,3],[1,3,1]);
```

$$[[1,-3,10,-28],[70,31]]$$

– On peut vérifier le résultat avec les fonctions intégrées *quo* et *rem* :

```
> A:=X^5+2*X^3-X^2-4*X+3: B:=X^2+3*X+1: quo(A,B,X),rem(A,B,X);
```

$$X^3-3X^2+10X-28,\quad 31+70X$$

II.3 Algorithme d'Euclide, Pgcd

Proposition *(Pgcd de deux polynômes)*

Soient A et B deux éléments de $\mathbb{K}[X]$.
Il existe un unique polynôme normalisé ou nul D tel que $\mathcal{D}(A)\cap\mathcal{D}(B)=\mathcal{D}(D)$.
Autrement dit, pour tout polynôme P, on a $(P\mid A \text{ et } P\mid B)\Leftrightarrow P\mid D$.
On dit que D est le *pgcd* de A et de B. On note $D=\text{pgcd}(A,B)$, ou $D=A\wedge B$.
Il existe un couple de polynômes U,V tels que $AU+BV=A\wedge B$.
On dit que (U,V) est un couple de *coefficients de Bezout* du couple (A,B).

Remarques

– Si $A=B=0$, alors $\mathcal{D}(A)=\mathcal{D}(B)=\mathbb{K}[X]$.

Seul le polynôme $D=0$ vérifie $\mathbb{K}[X]=\mathcal{D}(D)$. Ainsi $0\wedge 0=0$.

Dans ce cas l'égalité $AU+BV=A\wedge B$ est vérifée pour tous polynômes U et V.

– L'unicité (si existence) de $D=A\wedge B$ vient du fait que si $\mathcal{D}(D_1)=\mathcal{D}(D_2)$ alors $D_1=D_2$ sont associés. Or deux polynômes associés et unitaires sont égaux.

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 37 pages.

Pour démontrer la proposition quand $(A, B) \neq (0, 0)$ on s'inspire de l'algorithme d'Euclide dans $\mathbb{Z}$ et on forme une succession de divisions euclidiennes partant du couple (A, B), jusqu'à obtenir un reste nul. Le pgcd de A et B est alors le normalisé du dernier reste non nul.

Mise en œuvre de l'algorithme d'Euclide

- Quitte à échanger A et B on peut supposer $B \neq 0$.
  On pose $R_0 = A$ et $R_1 = B$. Le polynôme R_1 est le premier "reste" : il est non nul.
  On effectue la division euclidienne de R_0 par R_1.
  Notons $R_0 = Q_1R_1 + R_2$ cette division. On a bien sûr $\deg(R_2) < \deg(R_1)$.
- Si $R_2 = 0$, alors le procédé s'arrête, et R_1 est le dernier reste non nul obtenu.
  Sinon on effectue la division de R_1 par R_2 : $R_1 = Q_2R_2 + R_3$, avec $\deg(R_3) < \deg(R_2)$.
- Si $R_3 = 0$, alors le procédé s'arrête, et R_2 est le dernier reste non nul obtenu.
  Sinon on effectue la division de R_2 par R_3.
- La k-ième étape de cet algorithme est une division $R_{k-1} = Q_kR_k + R_{k+1}$.
  A ce stade on a : $\deg(R_0) > \deg(R_1) > \cdots > \deg(R_k) > \deg(R_{k+1})$.
  Ce procédé est fini car la suite des $\deg(R_k)$ est strictement décroissante dans $\mathbb{N}$.
  Il existe donc une n-ième étape lors de laquelle $R_{n-1} = Q_nR_n$ c'est-à-dire $R_{n+1} = 0$.
  Le polynôme R_n est le dernier reste non nul obtenu dans cette méthode.

Pour montrer que le normalisé R_n^* du dernier reste non nul est bien le pgcd de A et de B (c'est-à-dire satisfait aux conditions de la définition), on fait les remarques suivantes :

Justification de l'algorithme d'Euclide

- Soient $S \neq 0$ et T deux polynômes, et $T = QS + R$ la division euclidienne de T par S.
  Alors $\mathcal{D}(T) \cap \mathcal{D}(S) = \mathcal{D}(S) \cap \mathcal{D}(R)$.
- Si on revient à l'algorithme précédent, on a donc :
  $$\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(R_0) \cap \mathcal{D}(R_1) = \mathcal{D}(R_1) \cap \mathcal{D}(R_2) = \cdots = \mathcal{D}(R_{n-1}) \cap \mathcal{D}(R_n)$$
  Or R_n divise R_{n-1}. Il en découle $\mathcal{D}(R_n) \subset \mathcal{D}(R_{n-1})$ donc $\mathcal{D}(R_{n-1}) \cap \mathcal{D}(R_n) = \mathcal{D}(R_n)$.
  Ainsi $\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(R_n) = \mathcal{D}(R_n^*)$.
- La k-ième étape de l'algorithme s'écrit : $R_{k+1} = R_{k-1} - Q_kR_k$. Elle montre que si
  $\begin{cases} R_{k-1} = AU_{k-1} + BV_{k-1} \\ \text{et } R_k = AU_k + BV_k \end{cases}$ alors $R_{k+1} = AU_{k+1} + BV_{k+1}$ avec $\begin{cases} U_{k+1} = U_{k-1} - Q_kU_k \\ V_{k+1} = V_{k-1} - Q_kV_k \end{cases}$
  Or $R_0 = A$ et $R_1 = 1$ s'écrivent $\begin{cases} R_0 = AU_0 + BV_0 \\ R_1 = AU_1 + BV_1 \end{cases}$. En effet $\begin{cases} A = A \cdot 1 + B \cdot 0 \\ B = A \cdot 0 + B \cdot 1 \end{cases}$
  Une récurrence finie montre donc qu'il existe U_n, V_n tels que $R_n = AU_n + BV_n$.
  En divisant par le coefficient dominant de R_n, on obtient une égalité : $R_n^* = AU + BV$.

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 37 pages.

Remarques et propriétés

– Pour tout polynôme A, on a $A \wedge 0 = A^*$.
Plus généralement, on a $A \wedge B = A^*$ si et seulement si A divise B.

– Si A et B ne sont pas tous deux nuls, alors $D = A \wedge B$ est non nul.
Le polynôme D est un diviseur commun à A et B.
Parmi tous les diviseurs communs à A et B, D est le polynôme unitaire de plus haut degré.
Cette propriété justifie l'appellation "pgcd".

– On pourrait abandonner la condition que le pgcd de A et B soit unitaire.
Dans ce cas $A \wedge B$ ne serait défini qu'à une constante multiplicative près, et $A \wedge B$ serait par exemple le dernier reste non nul dans l'algorithme d'Euclide.

– Pour tous polynômes A, B, C on a $A \wedge B = (A - BC) \wedge B$.
Par exemple, on a $A \wedge B = R_k \wedge R_{k+1}$, pour tout couple (R_k, R_{k+1}) de restes successifs non nuls dans l'algorithme d'Euclide appliqué au couple (A, B).

– Pour tous polynômes A et B, et tous scalaires λ, μ non nuls, on a $A \wedge B = (\lambda A) \wedge (\mu B)$.
Cela peut permettre de simplifier les divisions successives dans l'algorithme d'Euclide.

– Pour tous polynômes A, B, C, on a : $(CA) \wedge (CB) = C^* (A \wedge B)$.
De même, soit Δ un diviseur commun de A et B. Posons $A = \Delta\widetilde{A}$ et $B = \Delta\widetilde{B}$.
Alors $\widetilde{A} \wedge \widetilde{B}$ est un diviseur de $A \wedge B$. Plus précisément : $A \wedge B = \Delta^* (\widetilde{A} \wedge \widetilde{B})$.

Programmation Maple

– Voici une procédure Maple calculant itérativement le pgcd de deux polynômes A et B.
Les polynômes sont ici représentés par la liste de leurs coefficints (degrés décroissants).
On fait appel à la procédure *division* définie précédemment.

```
> eucl_pol:=proc(A::list,B::list)
    local a,b,r,q,t;
    a:=A; b:=B;
    while b<>[0] do
      t:=division(a,b); a:=b; b:=t[2];
    od;
    a/a[1];
  end:
```

– Voici un exemple d'utilisation, avec $\begin{cases} A = X^6 + 2X^5 - 3X^4 - 5X^3 + 4X^2 + 3X - 2 \\ B = X^5 + 4X^4 + 4X^3 - X^2 - 4X - 4 \end{cases}$

```
> A:=[1,2,-3,-5,4,3,-2]: B:=[1,4,4,-1,-4,-4]: eucl_pol(A,B);
```

$$[1, 1, -2]$$

Le pgcd de A et B est donc $D = X^2 + X - 2$.

– Voici une procédure Maple calculant récursivement le pgcd de A et B.
On écrit encore les polynômes comme des listes, et on utilise la procédure *division*.

```
> euclpol_rec:=proc(a::list,b::list)
    if b=[0] then a/a[1] else
```


Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 37 pages.