Mathématiques assistées par ordinateur

Chapitre 3 : Arithmétique des polynômes

Michael Eisermann

Mat249, DLST L2S4, Année 2008-2009
www-fourier.ujf-grenoble.fr/~eiserm/cours#mao
Document mis à jour le 6 juillet 2009

Sommaire

Sommaire

Corps

Les nombres rationnels $(\mathbb{Q}, +, \cdot)$, les nombres réels $(\mathbb{R}, +, \cdot)$, et les nombres complexes $(\mathbb{C}, +, \cdot)$ jouissent des propriétés suivantes :

Corps

Les nombres rationnels $(\mathbb{Q}, +, \cdot)$, les nombres réels $(\mathbb{R}, +, \cdot)$, et les nombres complexes $(\mathbb{C}, +, \cdot)$ jouissent des propriétés suivantes :

(A1 : associativité) $\forall a, b, c : \ (a + b) + c = a + (b + c)$

Corps

Les nombres rationnels $(\mathbb{Q}, +, \cdot)$, les nombres réels $(\mathbb{R}, +, \cdot)$, et les nombres complexes $(\mathbb{C}, +, \cdot)$ jouissent des propriétés suivantes :

(A1 : associativité) $\forall a, b, c : \ (a + b) + c = a + (b + c)$

(A2 : commutativité) $\forall a, b : \ a + b = b + a$

Corps

Les nombres rationnels $(\mathbb{Q}, +, \cdot)$, les nombres réels $(\mathbb{R}, +, \cdot)$, et les nombres complexes $(\mathbb{C}, +, \cdot)$ jouissent des propriétés suivantes :

(A1 : associativité) $\forall a, b, c : \ (a + b) + c = a + (b + c)$

(A2 : commutativité) $\forall a, b : \ a + b = b + a$

(A3 : élément neutre) $\exists 0 \ \forall a : \ 0 + a = a$

Corps

Les nombres rationnels $(\mathbb{Q}, +, \cdot)$, les nombres réels $(\mathbb{R}, +, \cdot)$, et les nombres complexes $(\mathbb{C}, +, \cdot)$ jouissent des propriétés suivantes :

(A1 : associativité)	$\forall a, b, c : \ (a + b) + c = a + (b + c)$
(A2 : commutativité)	$\forall a, b : \ a + b = b + a$
(A3 : élément neutre)	$\exists 0 \ \forall a : \ 0 + a = a$
(A4 : élément opposé)	$\forall a \ \exists b : \ a + b = 0$

Corps

Les nombres rationnels $(\mathbb{Q}, +, \cdot)$, les nombres réels $(\mathbb{R}, +, \cdot)$, et les nombres complexes $(\mathbb{C}, +, \cdot)$ jouissent des propriétés suivantes :

(A1 : associativité)	$\forall a, b, c : \ (a + b) + c = a + (b + c)$
(A2 : commutativité)	$\forall a, b : \ a + b = b + a$
(A3 : élément neutre)	$\exists 0 \ \forall a : \ 0 + a = a$
(A4 : élément opposé)	$\forall a \ \exists b : \ a + b = 0$
(M1 : associativité)	$\forall a, b, c : \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$

Corps

Les nombres rationnels $(\mathbb{Q}, +, \cdot)$, les nombres réels $(\mathbb{R}, +, \cdot)$, et les nombres complexes $(\mathbb{C}, +, \cdot)$ jouissent des propriétés suivantes :

(A1 : associativité)	$\forall a, b, c : \ (a + b) + c = a + (b + c)$
(A2 : commutativité)	$\forall a, b : \ a + b = b + a$
(A3 : élément neutre)	$\exists 0 \ \forall a : \ 0 + a = a$
(A4 : élément opposé)	$\forall a \ \exists b : \ a + b = 0$
(M1 : associativité)	$\forall a, b, c : \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$
(M2 : commutativité)	$\forall a, b : \ a \cdot b = b \cdot a$

Corps

Les nombres rationnels $(\mathbb{Q}, +, \cdot)$, les nombres réels $(\mathbb{R}, +, \cdot)$, et les nombres complexes $(\mathbb{C}, +, \cdot)$ jouissent des propriétés suivantes :

(A1 : associativité)	$\forall a, b, c : \ (a + b) + c = a + (b + c)$
(A2 : commutativité)	$\forall a, b : \ a + b = b + a$
(A3 : élément neutre)	$\exists 0 \ \forall a : \ 0 + a = a$
(A4 : élément opposé)	$\forall a \ \exists b : \ a + b = 0$
(M1 : associativité)	$\forall a, b, c : \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$
(M2 : commutativité)	$\forall a, b : \ a \cdot b = b \cdot a$
(M3 : élément neutre)	$\exists 1 \neq 0 \ \forall a : \ 1 \cdot a = a$

Corps

Les nombres rationnels $(\mathbb{Q}, +, \cdot)$, les nombres réels $(\mathbb{R}, +, \cdot)$, et les nombres complexes $(\mathbb{C}, +, \cdot)$ jouissent des propriétés suivantes :

(A1 : associativité)	$\forall a, b, c : \ (a + b) + c = a + (b + c)$
(A2 : commutativité)	$\forall a, b : \ a + b = b + a$
(A3 : élément neutre)	$\exists 0 \ \forall a : \ 0 + a = a$
(A4 : élément opposé)	$\forall a \ \exists b : \ a + b = 0$
(M1 : associativité)	$\forall a, b, c : \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$
(M2 : commutativité)	$\forall a, b : \ a \cdot b = b \cdot a$
(M3 : élément neutre)	$\exists 1 \neq 0 \ \forall a : \ 1 \cdot a = a$
(M4 : élément inverse)	$\forall a \neq 0 \ \exists b : \ a \cdot b = 1$

Corps

Les nombres rationnels $(\mathbb{Q}, +, \cdot)$, les nombres réels $(\mathbb{R}, +, \cdot)$, et les nombres complexes $(\mathbb{C}, +, \cdot)$ jouissent des propriétés suivantes :

(A1 : associativité)	$\forall a, b, c : \ (a + b) + c = a + (b + c)$
(A2 : commutativité)	$\forall a, b : \ a + b = b + a$
(A3 : élément neutre)	$\exists 0 \ \forall a : \ 0 + a = a$
(A4 : élément opposé)	$\forall a \ \exists b : \ a + b = 0$
(M1 : associativité)	$\forall a, b, c : \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$
(M2 : commutativité)	$\forall a, b : \ a \cdot b = b \cdot a$
(M3 : élément neutre)	$\exists 1 \neq 0 \ \forall a : \ 1 \cdot a = a$
(M4 : élément inverse)	$\forall a \neq 0 \ \exists b : \ a \cdot b = 1$
(D : distributivité)	$\forall a, b, c : \ a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Corps

Les nombres rationnels $(\mathbb{Q}, +, \cdot)$, les nombres réels $(\mathbb{R}, +, \cdot)$, et les nombres complexes $(\mathbb{C}, +, \cdot)$ jouissent des propriétés suivantes :

(A1 : associativité)	$\forall a, b, c : \ (a + b) + c = a + (b + c)$
(A2 : commutativité)	$\forall a, b : \ a + b = b + a$
(A3 : élément neutre)	$\exists 0 \ \forall a : \ 0 + a = a$
(A4 : élément opposé)	$\forall a \ \exists b : \ a + b = 0$
(M1 : associativité)	$\forall a, b, c : \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$
(M2 : commutativité)	$\forall a, b : \ a \cdot b = b \cdot a$
(M3 : élément neutre)	$\exists 1 \neq 0 \ \forall a : \ 1 \cdot a = a$
(M4 : élément inverse)	$\forall a \neq 0 \ \exists b : \ a \cdot b = 1$
(D : distributivité)	$\forall a, b, c : \ a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Définition (corps)

Un *corps* $(\mathbb{K}, +, \cdot)$ est un ensemble $\mathbb{K}$ muni de deux opérations, appelées addition $+ \colon \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ et multiplication $\cdot \colon \mathbb{K} \times \mathbb{K} \to \mathbb{K}$, vérifiant tous les axiomes (A1-4), (M1-4), (D) ci-dessus.

Anneaux

Les entiers $(\mathbb{Z}, +, \cdot)$ ne forment pas un corps mais un anneau :

Anneaux

Les entiers $(\mathbb{Z}, +, \cdot)$ ne forment pas un corps mais un anneau :

Définition (anneau)

Un *anneau* $(\mathbb{A}, +, \cdot)$ est un ensemble muni de deux opérations dont on exige les axiomes ci-dessus à l'exception de M4 (élément inverse).

Anneaux

Les entiers $(\mathbb{Z}, +, \cdot)$ ne forment pas un corps mais un anneau :

Définition (anneau)

Un *anneau* $(\mathbb{A}, +, \cdot)$ est un ensemble muni de deux opérations dont on exige les axiomes ci-dessus à l'exception de M4 (élément inverse).

Ici tout anneau sera donc supposé commutatif (M2) et unitaire (M3).

Anneaux

Les entiers $(\mathbb{Z}, +, \cdot)$ ne forment pas un corps mais un anneau :

Définition (anneau)

Un *anneau* $(\mathbb{A}, +, \cdot)$ est un ensemble muni de deux opérations dont on exige les axiomes ci-dessus à l'exception de M4 (élément inverse).

Ici tout anneau sera donc supposé commutatif (M2) et unitaire (M3).

Définition (éléments inversibles)

Soit $a \in \mathbb{A}$. On dit que $b \in \mathbb{A}$ est un *inverse* de a si $a \cdot b = 1$.

Anneaux

Les entiers $(\mathbb{Z}, +, \cdot)$ ne forment pas un corps mais un anneau :

Définition (anneau)

Un *anneau* $(\mathbb{A}, +, \cdot)$ est un ensemble muni de deux opérations dont on exige les axiomes ci-dessus à l'exception de M4 (élément inverse).

Ici tout anneau sera donc supposé commutatif (M2) et unitaire (M3).

Définition (éléments inversibles)

Soit $a \in \mathbb{A}$. On dit que $b \in \mathbb{A}$ est un *inverse* de a si $a \cdot b = 1$.
Dans ce cas l'inverse de a est unique et sera noté par a^{-1}.

Anneaux

Les entiers $(\mathbb{Z}, +, \cdot)$ ne forment pas un corps mais un anneau :

Définition (anneau)

Un *anneau* $(\mathbb{A}, +, \cdot)$ est un ensemble muni de deux opérations dont on exige les axiomes ci-dessus à l'exception de M4 (élément inverse).

Ici tout anneau sera donc supposé commutatif (M2) et unitaire (M3).

Définition (éléments inversibles)

Soit $a \in \mathbb{A}$. On dit que $b \in \mathbb{A}$ est un *inverse* de a si $a \cdot b = 1$.
Dans ce cas l'inverse de a est unique et sera noté par a^{-1}.
On appelle $a \in \mathbb{A}$ *inversible* s'il admet un inverse dans $\mathbb{A}$.

Anneaux

Les entiers $(\mathbb{Z}, +, \cdot)$ ne forment pas un corps mais un anneau :

Définition (anneau)

Un *anneau* $(\mathbb{A}, +, \cdot)$ est un ensemble muni de deux opérations dont on exige les axiomes ci-dessus à l'exception de M4 (élément inverse).

Ici tout anneau sera donc supposé commutatif (M2) et unitaire (M3).

Définition (éléments inversibles)

Soit $a \in \mathbb{A}$. On dit que $b \in \mathbb{A}$ est un *inverse* de a si $a \cdot b = 1$.
Dans ce cas l'inverse de a est unique et sera noté par a^{-1}.
On appelle $a \in \mathbb{A}$ *inversible* s'il admet un inverse dans $\mathbb{A}$.

Dans $\mathbb{Z}$, par exemple, les seuls éléments inversibles sont 1 et -1.

Anneaux

Les entiers $(\mathbb{Z}, +, \cdot)$ ne forment pas un corps mais un anneau :

Définition (anneau)

Un *anneau* $(\mathbb{A}, +, \cdot)$ est un ensemble muni de deux opérations dont on exige les axiomes ci-dessus à l'exception de M4 (élément inverse).

Ici tout anneau sera donc supposé commutatif (M2) et unitaire (M3).

Définition (éléments inversibles)

Soit $a \in \mathbb{A}$. On dit que $b \in \mathbb{A}$ est un *inverse* de a si $a \cdot b = 1$.
Dans ce cas l'inverse de a est unique et sera noté par a^{-1}.
On appelle $a \in \mathbb{A}$ *inversible* s'il admet un inverse dans $\mathbb{A}$.

Dans $\mathbb{Z}$, par exemple, les seuls éléments inversibles sont 1 et -1.
L'élément 0 n'est jamais inversible : on a toujours $0 \cdot b = 0 \neq 1$.

Anneaux

Les entiers $(\mathbb{Z}, +, \cdot)$ ne forment pas un corps mais un anneau :

Définition (anneau)

Un *anneau* $(\mathbb{A}, +, \cdot)$ est un ensemble muni de deux opérations dont on exige les axiomes ci-dessus à l'exception de M4 (élément inverse).

Ici tout anneau sera donc supposé commutatif (M2) et unitaire (M3).

Définition (éléments inversibles)

Soit $a \in \mathbb{A}$. On dit que $b \in \mathbb{A}$ est un *inverse* de a si $a \cdot b = 1$.
Dans ce cas l'inverse de a est unique et sera noté par a^{-1}.
On appelle $a \in \mathbb{A}$ *inversible* s'il admet un inverse dans $\mathbb{A}$.

Dans $\mathbb{Z}$, par exemple, les seuls éléments inversibles sont 1 et -1.
L'élément 0 n'est jamais inversible : on a toujours $0 \cdot b = 0 \neq 1$.
Un anneau $\mathbb{A}$ est un corps ssi tout élément $a \in \mathbb{A}$, $a \neq 0$ est inversible.

Anneaux

Les entiers $(\mathbb{Z}, +, \cdot)$ ne forment pas un corps mais un anneau :

Définition (anneau)

Un *anneau* $(\mathbb{A}, +, \cdot)$ est un ensemble muni de deux opérations dont on exige les axiomes ci-dessus à l'exception de M4 (élément inverse).

Ici tout anneau sera donc supposé commutatif (M2) et unitaire (M3).

Définition (éléments inversibles)

Soit $a \in \mathbb{A}$. On dit que $b \in \mathbb{A}$ est un *inverse* de a si $a \cdot b = 1$.
Dans ce cas l'inverse de a est unique et sera noté par a^{-1}.
On appelle $a \in \mathbb{A}$ *inversible* s'il admet un inverse dans $\mathbb{A}$.

Dans $\mathbb{Z}$, par exemple, les seuls éléments inversibles sont 1 et -1.
L'élément 0 n'est jamais inversible : on a toujours $0 \cdot b = 0 \neq 1$.
Un anneau $\mathbb{A}$ est un corps ssi tout élément $a \in \mathbb{A}$, $a \neq 0$ est inversible.

On note $\mathbb{A}^* = \mathbb{A} \setminus \{0\}$ l'ensemble des éléments non nuls,
et $\mathbb{A}^\times \subset \mathbb{A}^*$ l'ensemble des éléments inversibles dans $\mathbb{A}$.

Polynômes

Soit $\mathbb{K}$ un corps (par exemple $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$).

Polynômes

Soit $\mathbb{K}$ un corps (par exemple $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$).

Un *polynôme* sur $\mathbb{K}$ est une expression formelle

$$P = p_0 + p_1 X^1 + p_2 X^2 + \cdots + p_n X^n \qquad \text{où } p_0, p_1, p_2, \ldots, p_n \in \mathbb{K}.$$

Polynômes

Soit $\mathbb{K}$ un corps (par exemple $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$).

Un *polynôme* sur $\mathbb{K}$ est une expression formelle

$$P = p_0 + p_1 X^1 + p_2 X^2 + \cdots + p_n X^n \qquad \text{où } p_0, p_1, p_2, \ldots, p_n \in \mathbb{K}.$$

Ce qui compte est la suite des coefficients dans $\mathbb{K}$:

$$\sum_{k=0}^{n} a_k X^k = \sum_{k=0}^{n} b_k X^k \qquad \Longleftrightarrow \qquad a_k = b_k \text{ pour tout } k = 0, \ldots, n$$

Polynômes

Soit $\mathbb{K}$ un corps (par exemple $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$).

Un *polynôme* sur $\mathbb{K}$ est une expression formelle

$$P = p_0 + p_1 X^1 + p_2 X^2 + \cdots + p_n X^n \qquad \text{où } p_0, p_1, p_2, \ldots, p_n \in \mathbb{K}.$$

Ce qui compte est la suite des coefficients dans $\mathbb{K}$:

$$\sum_{k=0}^{n} a_k X^k = \sum_{k=0}^{n} b_k X^k \qquad \Longleftrightarrow \qquad a_k = b_k \text{ pour tout } k = 0, \ldots, n$$

Pour l'implémentation il suffit de stocker les coefficients non nuls. Typiquement on stocke la suite $(p_0, p_1, p_2, \ldots, p_n)$ telle que $p_n \neq 0$.

L'anneau des polynômes

On note par $\mathbb{K}[X]$ l'ensemble des polynômes sur l'anneau $\mathbb{K}$.

L'anneau des polynômes

On note par $\mathbb{K}[X]$ l'ensemble des polynômes sur l'anneau $\mathbb{K}$.
On définit l'addition terme par terme :

$$\left(\sum_{k=0}^{n} a_k X^k\right) + \left(\sum_{k=0}^{n} b_k X^k\right) := \sum_{k=0}^{n} (a_k + b_k) X^k$$

L'anneau des polynômes

On note par $\mathbb{K}[X]$ l'ensemble des polynômes sur l'anneau $\mathbb{K}$.
On définit l'addition terme par terme :

$$\Big(\sum_{k=0}^{n} a_k X^k\Big) + \Big(\sum_{k=0}^{n} b_k X^k\Big) := \sum_{k=0}^{n} (a_k + b_k) X^k$$

Pour obtenir $X^i \cdot X^j = X^{i+j}$ on définit la multiplication par

$$\Big(\sum_{i=0}^{m} a_i X^i\Big) \cdot \Big(\sum_{j=0}^{n} b_j X^j\Big) := \sum_{k=0}^{m+n} \Big(\sum_{i+j=k} a_i b_j\Big) X^k$$

L'anneau des polynômes

On note par $\mathbb{K}[X]$ l'ensemble des polynômes sur l'anneau $\mathbb{K}$.
On définit l'addition terme par terme :

$$\Big(\sum_{k=0}^{n} a_k X^k\Big) + \Big(\sum_{k=0}^{n} b_k X^k\Big) := \sum_{k=0}^{n} (a_k + b_k) X^k$$

Pour obtenir $X^i \cdot X^j = X^{i+j}$ on définit la multiplication par

$$\Big(\sum_{i=0}^{m} a_i X^i\Big) \cdot \Big(\sum_{j=0}^{n} b_j X^j\Big) := \sum_{k=0}^{m+n} \Big(\sum_{i+j=k} a_i b_j\Big) X^k$$

Ces définitions se traduisent directement en algorithme de calcul.

L'anneau des polynômes

On note par $\mathbb{K}[X]$ l'ensemble des polynômes sur l'anneau $\mathbb{K}$.
On définit l'addition terme par terme :

$$\Big(\sum_{k=0}^{n} a_k X^k\Big) + \Big(\sum_{k=0}^{n} b_k X^k\Big) := \sum_{k=0}^{n} (a_k + b_k) X^k$$

Pour obtenir $X^i \cdot X^j = X^{i+j}$ on définit la multiplication par

$$\Big(\sum_{i=0}^{m} a_i X^i\Big) \cdot \Big(\sum_{j=0}^{n} b_j X^j\Big) := \sum_{k=0}^{m+n} \Big(\sum_{i+j=k} a_i b_j\Big) X^k$$

Ces définitions se traduisent directement en algorithme de calcul.

Proposition (l'anneau des polynômes sur $\mathbb{K}$)

L'ensemble $\mathbb{K}[X]$ des polynômes sur $\mathbb{K}$ muni de l'addition $+$ et de la multiplication $\cdot$ définies ci-dessus est un anneau.

L'anneau des polynômes

On note par $\mathbb{K}[X]$ l'ensemble des polynômes sur l'anneau $\mathbb{K}$.
On définit l'addition terme par terme :

$$\Big(\sum_{k=0}^{n} a_k X^k\Big) + \Big(\sum_{k=0}^{n} b_k X^k\Big) := \sum_{k=0}^{n} (a_k + b_k) X^k$$

Pour obtenir $X^i \cdot X^j = X^{i+j}$ on définit la multiplication par

$$\Big(\sum_{i=0}^{m} a_i X^i\Big) \cdot \Big(\sum_{j=0}^{n} b_j X^j\Big) := \sum_{k=0}^{m+n} \Big(\sum_{i+j=k} a_i b_j\Big) X^k$$

Ces définitions se traduisent directement en algorithme de calcul.

Proposition (l'anneau des polynômes sur $\mathbb{K}$)

L'ensemble $\mathbb{K}[X]$ des polynômes sur $\mathbb{K}$ muni de l'addition $+$ et de la multiplication $\cdot$ définies ci-dessus est un anneau.

On remarque que $aX^0 + bX^0 = (a+b)X^0$ et $aX^0 \cdot bX^0 = (ab)X^0$.

L'anneau des polynômes

On note par $\mathbb{K}[X]$ l'ensemble des polynômes sur l'anneau $\mathbb{K}$.
On définit l'addition terme par terme :

$$\Big(\sum_{k=0}^{n} a_k X^k\Big) + \Big(\sum_{k=0}^{n} b_k X^k\Big) := \sum_{k=0}^{n} (a_k + b_k) X^k$$

Pour obtenir $X^i \cdot X^j = X^{i+j}$ on définit la multiplication par

$$\Big(\sum_{i=0}^{m} a_i X^i\Big) \cdot \Big(\sum_{j=0}^{n} b_j X^j\Big) := \sum_{k=0}^{m+n} \Big(\sum_{i+j=k} a_i b_j\Big) X^k$$

Ces définitions se traduisent directement en algorithme de calcul.

Proposition (l'anneau des polynômes sur $\mathbb{K}$)

L'ensemble $\mathbb{K}[X]$ des polynômes sur $\mathbb{K}$ muni de l'addition $+$ et de la multiplication $\cdot$ définies ci-dessus est un anneau.

On remarque que $aX^0 + bX^0 = (a+b)X^0$ et $aX^0 \cdot bX^0 = (ab)X^0$.

Ainsi on obtient $\mathbb{K} \subset \mathbb{K}[X]$ en identifiant $a \in \mathbb{K}$ avec $aX^0 \in \mathbb{K}[X]$.

Le degré des polynômes

Tout polynôme non nul s'écrit comme $P = \sum_{k=0}^{n} p_k X^k$ où $p_n \neq 0$.

Le degré des polynômes

Tout polynôme non nul s'écrit comme $P = \sum_{k=0}^{n} p_k X^k$ où $p_n \neq 0$.

Cette écriture est unique. On appelle $\deg P := n$ le *degré* de P, et $\mathrm{dom}\, P := p_n$ le *coefficient dominant* de P.

Le degré des polynômes

Tout polynôme non nul s'écrit comme $P = \sum_{k=0}^{n} p_k X^k$ où $p_n \neq 0$.

Cette écriture est unique. On appelle $\deg P := n$ le *degré* de P, et $\operatorname{dom} P := p_n$ le *coefficient dominant* de P.

Le polynôme nul est particulier ; on pose $\deg 0 := -\infty$ et $\operatorname{dom} 0 := 0$.

Le degré des polynômes

Tout polynôme non nul s'écrit comme $P = \sum_{k=0}^{n} p_k X^k$ où $p_n \neq 0$.

Cette écriture est unique. On appelle $\deg P := n$ le *degré* de P, et $\operatorname{dom} P := p_n$ le *coefficient dominant* de P.

Le polynôme nul est particulier ; on pose $\deg 0 := -\infty$ et $\operatorname{dom} 0 := 0$.

Proposition (propriétés du degré sur un corps)

On a $\deg(P+Q) \leq \sup\{\deg P, \deg Q\}$, *avec égalité si* $\deg P \neq \deg Q$.

Le degré des polynômes

Tout polynôme non nul s'écrit comme $P = \sum_{k=0}^{n} p_k X^k$ où $p_n \neq 0$.

Cette écriture est unique. On appelle $\deg P := n$ le *degré* de P, et $\operatorname{dom} P := p_n$ le *coefficient dominant* de P.

Le polynôme nul est particulier ; on pose $\deg 0 := -\infty$ et $\operatorname{dom} 0 := 0$.

Proposition (propriétés du degré sur un corps)

On a $\deg(P+Q) \leq \sup\{\deg P, \deg Q\}$, *avec égalité si* $\deg P \neq \deg Q$.
On a $\deg(PQ) = \deg P + \deg Q$ *et* $\operatorname{dom}(PQ) = \operatorname{dom} P \cdot \operatorname{dom} Q$.

Le degré des polynômes

Tout polynôme non nul s'écrit comme $P = \sum_{k=0}^{n} p_k X^k$ où $p_n \neq 0$.

Cette écriture est unique. On appelle $\deg P := n$ le *degré* de P, et $\operatorname{dom} P := p_n$ le *coefficient dominant* de P.

Le polynôme nul est particulier ; on pose $\deg 0 := -\infty$ et $\operatorname{dom} 0 := 0$.

Proposition (propriétés du degré sur un corps)

On a $\deg(P+Q) \leq \sup\{\deg P, \deg Q\}$, *avec égalité si* $\deg P \neq \deg Q$.
On a $\deg(PQ) = \deg P + \deg Q$ *et* $\operatorname{dom}(PQ) = \operatorname{dom} P \cdot \operatorname{dom} Q$.
Soulignons en particulier que $P \neq 0$ *et* $Q \neq 0$ *implique* $PQ \neq 0$.

La division euclidienne : existence et unicité

Soit $\mathbb{K}$ un corps (par exemple $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$).

La division euclidienne : existence et unicité

Soit $\mathbb{K}$ un corps (par exemple $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$).

Proposition (division euclidienne de polynômes)

Soit $P \in \mathbb{K}[X]$ un polynôme non nul. Alors pour tout $S \in \mathbb{K}[X]$ il existe une unique paire $Q, R \in \mathbb{K}[X]$ telle que $S = PQ + R$ et $\deg R < \deg P$.

La division euclidienne : existence et unicité

Soit $\mathbb{K}$ un corps (par exemple $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$).

Proposition (division euclidienne de polynômes)

Soit $P \in \mathbb{K}[X]$ un polynôme non nul. Alors pour tout $S \in \mathbb{K}[X]$ il existe une unique paire $Q, R \in \mathbb{K}[X]$ telle que $S = PQ + R$ et $\deg R < \deg P$.

Définition (quotient et reste)

Si $S = PQ + R$ et $\deg R < \deg P$, on appelle $S \operatorname{quo} P := Q$ le *quotient* et $S \operatorname{rem} P := R$ le *reste* de la division euclidienne de S par P.

La division euclidienne : algorithme

Algorithme 3 division euclidienne de deux polynômes

Entrée: deux polynômes $S, P \in \mathbb{K}[X]$, $P \neq 0$, sur un corps $\mathbb{K}$.

Sortie: les polynômes $Q, R \in \mathbb{K}[X]$ vérifiant $S = PQ + R$ et $\deg R < \deg P$.

$Q \leftarrow 0\,;\ R \leftarrow S$ // invariant $S = PQ + R$

tant que $\deg R \geq \deg P$ **faire**

  $M \leftarrow \mathrm{dom}(P)^{-1}\,\mathrm{dom}(R) \cdot X^{\deg R - \deg P}$ // $R = PM$ en degré dominant

  $Q \leftarrow Q + M\,;\ R \leftarrow R - PM$ // préserve $S = PQ + R$

fin tant que

retourner (Q, R)

La division euclidienne : algorithme

Algorithme 4 division euclidienne de deux polynômes

Entrée: deux polynômes $S, P \in \mathbb{K}[X]$, $P \neq 0$, sur un corps $\mathbb{K}$.

Sortie: les polynômes $Q, R \in \mathbb{K}[X]$ vérifiant $S = PQ + R$ et $\deg R < \deg P$.

$Q \leftarrow 0\,;\ R \leftarrow S$ // invariant $S = PQ + R$

tant que $\deg R \geq \deg P$ **faire**

  $M \leftarrow \mathrm{dom}(P)^{-1}\,\mathrm{dom}(R) \cdot X^{\deg R - \deg P}$ // $R = PM$ en degré dominant

  $Q \leftarrow Q + M\,;\ R \leftarrow R - PM$ // préserve $S = PQ + R$

fin tant que

retourner (Q, R)

Proposition

L'algorithme 3 ci-dessus est correct.

Divisibilité

Définition

Soient $A, B \in \mathbb{K}[X]$ deux polynômes sur $\mathbb{K}$. On dit que A *divise* B dans $\mathbb{K}[X]$, noté $A \mid B$, s'il existe $Q \in \mathbb{K}[X]$ de sorte que $AQ = B$.

Divisibilité

Définition

Soient $A, B \in \mathbb{K}[X]$ deux polynômes sur $\mathbb{K}$. On dit que A *divise* B dans $\mathbb{K}[X]$, noté $A \mid B$, s'il existe $Q \in \mathbb{K}[X]$ de sorte que $AQ = B$.

Par exemple, $X + 1$ divise $X^2 - 1$ car $(X + 1)(X - 1) = X^2 - 1$.

Divisibilité

Définition

Soient $A, B \in \mathbb{K}[X]$ deux polynômes sur $\mathbb{K}$. On dit que A *divise* B dans $\mathbb{K}[X]$, noté $A \mid B$, s'il existe $Q \in \mathbb{K}[X]$ de sorte que $AQ = B$.

Par exemple, $X + 1$ divise $X^2 - 1$ car $(X + 1)(X - 1) = X^2 - 1$.

Notation

On écrit $P_1 \sim P_2$ si $P_1 = cP_2$ pour un facteur constant $c \in \mathbb{K}^\times$.
Dans ce cas on dit que P_1 et P_2 sont *proportionnels*.

Divisibilité

Définition

Soient $A, B \in \mathbb{K}[X]$ deux polynômes sur $\mathbb{K}$. On dit que A *divise* B dans $\mathbb{K}[X]$, noté $A \mid B$, s'il existe $Q \in \mathbb{K}[X]$ de sorte que $AQ = B$.

Par exemple, $X + 1$ divise $X^2 - 1$ car $(X + 1)(X - 1) = X^2 - 1$.

Notation

On écrit $P_1 \sim P_2$ si $P_1 = cP_2$ pour un facteur constant $c \in \mathbb{K}^\times$.
Dans ce cas on dit que P_1 et P_2 sont *proportionnels*.

Si $P_1 \sim P_2$, alors $A \mid P_1 \Leftrightarrow A \mid P_2$ et $P_1 \mid B \Leftrightarrow P_2 \mid B$.

Divisibilité

Définition

Soient $A, B \in \mathbb{K}[X]$ deux polynômes sur $\mathbb{K}$. On dit que A *divise* B dans $\mathbb{K}[X]$, noté $A \mid B$, s'il existe $Q \in \mathbb{K}[X]$ de sorte que $AQ = B$.

Par exemple, $X + 1$ divise $X^2 - 1$ car $(X + 1)(X - 1) = X^2 - 1$.

Notation

On écrit $P_1 \sim P_2$ si $P_1 = cP_2$ pour un facteur constant $c \in \mathbb{K}^\times$.
Dans ce cas on dit que P_1 et P_2 sont *proportionnels*.

Si $P_1 \sim P_2$, alors $A \mid P_1 \Leftrightarrow A \mid P_2$ et $P_1 \mid B \Leftrightarrow P_2 \mid B$.

Observation

On a toujours $A \mid A$ (réflexivité),
$A \mid B$ et $B \mid C$ implique $A \mid C$ (transitivité),
$A \mid B$ et $B \mid A$ implique $A \sim B$ (antisymétrie).

Divisibilité

Définition

Soient $A, B \in \mathbb{K}[X]$ deux polynômes sur $\mathbb{K}$. On dit que A *divise* B dans $\mathbb{K}[X]$, noté $A \mid B$, s'il existe $Q \in \mathbb{K}[X]$ de sorte que $AQ = B$.

Par exemple, $X + 1$ divise $X^2 - 1$ car $(X + 1)(X - 1) = X^2 - 1$.

Notation

On écrit $P_1 \sim P_2$ si $P_1 = cP_2$ pour un facteur constant $c \in \mathbb{K}^\times$.
Dans ce cas on dit que P_1 et P_2 sont *proportionnels*.

Si $P_1 \sim P_2$, alors $A \mid P_1 \Leftrightarrow A \mid P_2$ et $P_1 \mid B \Leftrightarrow P_2 \mid B$.

Observation

On a toujours $A \mid A$ (réflexivité),
$A \mid B$ et $B \mid C$ implique $A \mid C$ (transitivité),
$A \mid B$ et $B \mid A$ implique $A \sim B$ (antisymétrie).

Dans ce sens la divisibilité définit un ordre partiel sur les polynômes.

Divisibilité

Définition

Soient $A, B \in \mathbb{K}[X]$ deux polynômes sur $\mathbb{K}$. On dit que A *divise* B dans $\mathbb{K}[X]$, noté $A \mid B$, s'il existe $Q \in \mathbb{K}[X]$ de sorte que $AQ = B$.

Par exemple, $X + 1$ divise $X^2 - 1$ car $(X + 1)(X - 1) = X^2 - 1$.

Notation

On écrit $P_1 \sim P_2$ si $P_1 = cP_2$ pour un facteur constant $c \in \mathbb{K}^\times$.
Dans ce cas on dit que P_1 et P_2 sont *proportionnels*.

Si $P_1 \sim P_2$, alors $A \mid P_1 \Leftrightarrow A \mid P_2$ et $P_1 \mid B \Leftrightarrow P_2 \mid B$.

Observation

On a toujours $A \mid A$ (réflexivité),
$A \mid B$ et $B \mid C$ implique $A \mid C$ (transitivité),
$A \mid B$ et $B \mid A$ implique $A \sim B$ (antisymétrie).

Dans ce sens la divisibilité définit un ordre partiel sur les polynômes.
Dans cet ordre, 1 est minimal car $1 \mid P$ pour tout $P \in \mathbb{K}[X]$.

Divisibilité

Définition

Soient $A, B \in \mathbb{K}[X]$ deux polynômes sur $\mathbb{K}$. On dit que A *divise* B dans $\mathbb{K}[X]$, noté $A \mid B$, s'il existe $Q \in \mathbb{K}[X]$ de sorte que $AQ = B$.

Par exemple, $X + 1$ divise $X^2 - 1$ car $(X + 1)(X - 1) = X^2 - 1$.

Notation

On écrit $P_1 \sim P_2$ si $P_1 = cP_2$ pour un facteur constant $c \in \mathbb{K}^\times$.
Dans ce cas on dit que P_1 et P_2 sont *proportionnels*.

Si $P_1 \sim P_2$, alors $A \mid P_1 \Leftrightarrow A \mid P_2$ et $P_1 \mid B \Leftrightarrow P_2 \mid B$.

Observation

On a toujours $A \mid A$ (réflexivité),
$A \mid B$ et $B \mid C$ implique $A \mid C$ (transitivité),
$A \mid B$ et $B \mid A$ implique $A \sim B$ (antisymétrie).

Dans ce sens la divisibilité définit un ordre partiel sur les polynômes.
Dans cet ordre, 1 est minimal car $1 \mid P$ pour tout $P \in \mathbb{K}[X]$.
De même, 0 est maximal car $P \mid 0$ pour tout $P \in \mathbb{K}[X]$.

Définition du pgcd

Définition

On dit que C est un *diviseur commun* de $A_1, \ldots, A_n$ si $C \mid A_k$ pour tout k. On note $\mathscr{D}(A_1, \ldots, A_n)$ l'ensemble des diviseurs communs.

Définition du pgcd

Définition

On dit que C est un *diviseur commun* de $A_1, \ldots, A_n$ si $C \mid A_k$ pour tout k. On note $\mathscr{D}(A_1, \ldots, A_n)$ l'ensemble des diviseurs communs.

On dit que $D \in \mathscr{D}(A_1, \ldots, A_n)$ est un *plus grand commun diviseur* (pgcd) si tout autre diviseur commun $C \in \mathscr{D}(A_1, \ldots, A_n)$ divise D.

Définition du pgcd

Définition

On dit que C est un *diviseur commun* de $A_1, \ldots, A_n$ si $C \mid A_k$ pour tout k. On note $\mathscr{D}(A_1, \ldots, A_n)$ l'ensemble des diviseurs communs.

On dit que $D \in \mathscr{D}(A_1, \ldots, A_n)$ est un *plus grand commun diviseur* (pgcd) si tout autre diviseur commun $C \in \mathscr{D}(A_1, \ldots, A_n)$ divise D.

On note $\mathrm{pgcd}(A_1, \ldots, A_n)$ le *pgcd unitaire* de $A_1, \ldots, A_n$, si non nul.

Propriétés du pgcd

Observation

On a $\mathscr{D}(A_1, \ldots, A_n) = \mathscr{D}(\mathrm{pgcd}(A_1, \ldots, A_{n-1}), A_n)$.

Propriétés du pgcd

Observation

On a $\mathscr{D}(A_1, \ldots, A_n) = \mathscr{D}(\mathrm{pgcd}(A_1, \ldots, A_{n-1}), A_n)$.
Ainsi $\mathrm{pgcd}(A_1, \ldots, A_n) = \mathrm{pgcd}(\mathrm{pgcd}(A_1, \ldots, A_{n-1}), A_n)$. □

Propriétés du pgcd

Observation

On a $\mathscr{D}(A_1, \ldots, A_n) = \mathscr{D}(\mathrm{pgcd}(A_1, \ldots, A_{n-1}), A_n)$.
Ainsi $\mathrm{pgcd}(A_1, \ldots, A_n) = \mathrm{pgcd}(\mathrm{pgcd}(A_1, \ldots, A_{n-1}), A_n)$. □

Il suffit donc de savoir calculer le pgcd de deux polynômes.

Propriétés du pgcd

Observation

On a $\mathscr{D}(A_1, \ldots, A_n) = \mathscr{D}(\mathrm{pgcd}(A_1, \ldots, A_{n-1}), A_n)$.
Ainsi $\mathrm{pgcd}(A_1, \ldots, A_n) = \mathrm{pgcd}(\mathrm{pgcd}(A_1, \ldots, A_{n-1}), A_n)$. □

Il suffit donc de savoir calculer le pgcd de deux polynômes.

Observation

On a $\mathscr{D}(A, B) = \mathscr{D}(B, A) = \mathscr{D}(B, A - QB)$,
d'où $\mathrm{pgcd}(A, B) = \mathrm{pgcd}(B, A) = \mathrm{pgcd}(B, A - QB)$. □

Propriétés du pgcd

Observation

On a $\mathscr{D}(A_1, \ldots, A_n) = \mathscr{D}(\mathrm{pgcd}(A_1, \ldots, A_{n-1}), A_n)$.
Ainsi $\mathrm{pgcd}(A_1, \ldots, A_n) = \mathrm{pgcd}(\mathrm{pgcd}(A_1, \ldots, A_{n-1}), A_n)$. □

Il suffit donc de savoir calculer le pgcd de deux polynômes.

Observation

On a $\mathscr{D}(A, B) = \mathscr{D}(B, A) = \mathscr{D}(B, A - QB)$,
d'où $\mathrm{pgcd}(A, B) = \mathrm{pgcd}(B, A) = \mathrm{pgcd}(B, A - QB)$. □

C'est l'observation clé pour l'algorithme d'Euclide.

Propriétés du pgcd

Observation

On a $\mathscr{D}(A_1, \ldots, A_n) = \mathscr{D}(\mathrm{pgcd}(A_1, \ldots, A_{n-1}), A_n)$.
Ainsi $\mathrm{pgcd}(A_1, \ldots, A_n) = \mathrm{pgcd}(\mathrm{pgcd}(A_1, \ldots, A_{n-1}), A_n)$. □

Il suffit donc de savoir calculer le pgcd de deux polynômes.

Observation

On a $\mathscr{D}(A, B) = \mathscr{D}(B, A) = \mathscr{D}(B, A - QB)$,
d'où $\mathrm{pgcd}(A, B) = \mathrm{pgcd}(B, A) = \mathrm{pgcd}(B, A - QB)$. □

C'est l'observation clé pour l'algorithme d'Euclide.

Observation

On a finalement le cas trivial $\mathrm{pgcd}(A, 0) = A/\mathrm{dom}(A)$. □

Propriétés du pgcd

Observation

On a $\mathscr{D}(A_1, \ldots, A_n) = \mathscr{D}(\mathrm{pgcd}(A_1, \ldots, A_{n-1}), A_n)$.
Ainsi $\mathrm{pgcd}(A_1, \ldots, A_n) = \mathrm{pgcd}(\mathrm{pgcd}(A_1, \ldots, A_{n-1}), A_n)$. □

Il suffit donc de savoir calculer le pgcd de deux polynômes.

Observation

On a $\mathscr{D}(A, B) = \mathscr{D}(B, A) = \mathscr{D}(B, A - QB)$,
d'où $\mathrm{pgcd}(A, B) = \mathrm{pgcd}(B, A) = \mathrm{pgcd}(B, A - QB)$. □

C'est l'observation clé pour l'algorithme d'Euclide.

Observation

On a finalement le cas trivial $\mathrm{pgcd}(A, 0) = A/\mathrm{dom}(A)$. □

C'est la condition d'arrêt dans l'algorithme d'Euclide.

L'algorithme d'Euclide, version prête à programmer

Algorithme 5 calcul du pgcd selon Euclide

Entrée: deux polynômes $A_0, B_0 \in \mathbb{K}[X]$ sur un corps $\mathbb{K}$

Sortie: le pgcd de A_0 et B_0 dans $\mathbb{K}[X]$, unitaire si non nul

$A \leftarrow A_0, \quad B \leftarrow B_0$ // $\operatorname{pgcd}(A, B) = \operatorname{pgcd}(A_0, B_0)$

tant que $B \neq 0$ **faire**

  $R \leftarrow A \operatorname{rem} B$ // $A = QB + R$ et $\deg R < \deg B$

  $A \leftarrow B, \quad B \leftarrow R$ // $\operatorname{pgcd}(A, B) = \operatorname{pgcd}(B, R)$

fin tant que

si $A = 0$ **alors retourner** 0 **sinon retourner** $A/\operatorname{dom}(A)$

L'algorithme d'Euclide, version prête à programmer

Algorithme 6 calcul du pgcd selon Euclide

Entrée: deux polynômes $A_0, B_0 \in \mathbb{K}[X]$ sur un corps $\mathbb{K}$

Sortie: le pgcd de A_0 et B_0 dans $\mathbb{K}[X]$, unitaire si non nul

$A \leftarrow A_0, \quad B \leftarrow B_0$ // $\operatorname{pgcd}(A, B) = \operatorname{pgcd}(A_0, B_0)$

tant que $B \neq 0$ **faire**

  $R \leftarrow A \operatorname{rem} B$ // $A = QB + R$ et $\deg R < \deg B$

  $A \leftarrow B, \quad B \leftarrow R$ // $\operatorname{pgcd}(A, B) = \operatorname{pgcd}(B, R)$

fin tant que

si $A = 0$ **alors retourner** 0 **sinon retourner** $A/\operatorname{dom}(A)$

Théorème

L'algorithme 5 ci-dessus est correct :

- *Il se termine [après au plus* $\deg(B_0) + 1$ *itérations].*
- *Il renvoie le pgcd unitaire de* A_0 *et* B_0*.*

L'algorithme d'Euclide-Bézout

Théorème (identité de Bézout)

Pour tout $A, B \in \mathbb{K}[X]$ *il existe* $U, V \in \mathbb{K}[X]$ *tels que* $\mathrm{pgcd}(A, B) = AU + BV$. *L'algorithme 7 les calcule.*

L'algorithme d'Euclide-Bézout

Théorème (identité de Bézout)

Pour tout $A, B \in \mathbb{K}[X]$ *il existe* $U, V \in \mathbb{K}[X]$ *tels que* $\operatorname{pgcd}(A, B) = AU + BV$. *L'algorithme 7 les calcule.*

Algorithme 8 Euclide-Bézout

Entrée: deux polynômes $A_0, B_0 \in \mathbb{K}[X]$ sur un corps $\mathbb{K}$

Sortie: trois polynômes D, U, V tels que $D = A_0U + B_0V = \operatorname{pgcd}(A_0, B_0)$

$\begin{pmatrix} A & U & V \\ B & S & T \end{pmatrix} \leftarrow \begin{pmatrix} A_0 & 1 & 0 \\ B_0 & 0 & 1 \end{pmatrix}$ // invariant $\begin{cases} A = A_0U + B_0V \\ B = A_0S + B_0T \end{cases}$

tant que $B \neq 0$ **faire**

$Q \leftarrow A \operatorname{quo} B$ // $A = QB + R$, $\deg R < \deg B$

$\begin{pmatrix} A & U & V \\ B & S & T \end{pmatrix} \leftarrow \begin{pmatrix} B & S & T \\ A - QB & U - QS & V - QT \end{pmatrix}$

fin tant que

si $A = 0$ **alors retourner** le triplet $[0, 0, 0]$ **sinon**

retourner le triplet $[A/\operatorname{dom}(A),\ U/\operatorname{dom}(A),\ V/\operatorname{dom}(A)]$

Sommaire

Fonctions polynomiales

Définition

Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme dans $\mathbb{K}[X]$.
On définit *l'évaluation* de P en $x \in \mathbb{K}$ par $P(x) := \sum_{k=0}^{n} a_k x^k$.

Fonctions polynomiales

Définition

Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme dans $\mathbb{K}[X]$.
On définit *l'évaluation* de P en $x \in \mathbb{K}$ par $P(x) := \sum_{k=0}^{n} a_k x^k$.

Pour tout $P, Q \in \mathbb{K}[X]$ l'évaluation en $x \in \mathbb{K}$ vérifie
$(P+Q)(x) = P(x) + Q(x)$ et $(P \cdot Q)(x) = P(x) \cdot Q(x)$.

Fonctions polynomiales

Définition

Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme dans $\mathbb{K}[X]$.
On définit *l'évaluation* de P en $x \in \mathbb{K}$ par $P(x) := \sum_{k=0}^{n} a_k x^k$.

Pour tout $P, Q \in \mathbb{K}[X]$ l'évaluation en $x \in \mathbb{K}$ vérifie
$(P+Q)(x) = P(x) + Q(x)$ et $(P \cdot Q)(x) = P(x) \cdot Q(x)$.

Définition

Tout polynôme $P = \sum_{k=0}^{n} a_k X^k$ dans $\mathbb{K}[X]$ induit une
fonction polynomiale $f_P : \mathbb{K} \to \mathbb{K}$ par $x \mapsto P(x) = \sum_{k=0}^{n} a_k x^k$.

Fonctions polynomiales

Définition

Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme dans $\mathbb{K}[X]$.
On définit *l'évaluation* de P en $x \in \mathbb{K}$ par $P(x) := \sum_{k=0}^{n} a_k x^k$.

Pour tout $P, Q \in \mathbb{K}[X]$ l'évaluation en $x \in \mathbb{K}$ vérifie
$(P+Q)(x) = P(x) + Q(x)$ et $(P \cdot Q)(x) = P(x) \cdot Q(x)$.

Définition

Tout polynôme $P = \sum_{k=0}^{n} a_k X^k$ dans $\mathbb{K}[X]$ induit une
fonction polynomiale $f_P : \mathbb{K} \to \mathbb{K}$ par $x \mapsto P(x) = \sum_{k=0}^{n} a_k x^k$.

 *Expression* $\neq$ *fonction !* Ne pas confondre le polynôme $P \in \mathbb{K}[X]$ et la fonction polynomiale $f_P : \mathbb{K} \to \mathbb{K}$ associée.

La méthode de Horner : calcul de $P(x_0)$

Soit $P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ un polynôme dans $\mathbb{K}[X]$.

La méthode de Horner : calcul de $P(x_0)$

Soit $P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ un polynôme dans $\mathbb{K}[X]$.
Comment calculer efficacement $P(x)$ pour $x \in \mathbb{K}$?

La méthode de Horner : calcul de $P(x_0)$

Soit $P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ un polynôme dans $\mathbb{K}[X]$.
Comment calculer efficacement $P(x)$ pour $x \in \mathbb{K}$?

Méthode naïve : On calcule $a_k x^k$ en effectuant k multiplications.

La méthode de Horner : calcul de $P(x_0)$

Soit $P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ un polynôme dans $\mathbb{K}[X]$.
Comment calculer efficacement $P(x)$ pour $x \in \mathbb{K}$?

Méthode naïve : On calcule $a_k x^k$ en effectuant k multiplications.
Implémenté ainsi, le calcul de $P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ nécessite n additions et $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ multiplications.

La méthode de Horner : calcul de $P(x_0)$

Soit $P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ un polynôme dans $\mathbb{K}[X]$.
Comment calculer efficacement $P(x)$ pour $x \in \mathbb{K}$?

Méthode naïve : On calcule $a_k x^k$ en effectuant k multiplications.
Implémenté ainsi, le calcul de $P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ nécessite n additions et $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ multiplications.

Méthode de Horner : En profitant de la distributivité on évalue
$P(x) = ((\cdots((a_n x + a_{n-1})x + a_{n-2})\cdots x + a_2)x + a_1)x + a_0$.

La méthode de Horner : calcul de $P(x_0)$

Soit $P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ un polynôme dans $\mathbb{K}[X]$.
Comment calculer efficacement $P(x)$ pour $x \in \mathbb{K}$?

Méthode naïve : On calcule $a_k x^k$ en effectuant k multiplications.
Implémenté ainsi, le calcul de $P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ nécessite n additions et $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ multiplications.

Méthode de Horner : En profitant de la distributivité on évalue
$P(x) = ((\cdots((a_n x + a_{n-1})x + a_{n-2})\cdots x + a_2)x + a_1)x + a_0$.
Ceci ne nécessite que n additions et n multiplications !

La méthode de Horner : calcul de $P(x_0)$

Soit $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ un polynôme dans $\mathbb{K}[X]$.
Comment calculer efficacement $P(x)$ pour $x \in \mathbb{K}$?

Méthode naïve : On calcule a_kx^k en effectuant k multiplications.
Implémenté ainsi, le calcul de $P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ nécessite n additions et $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ multiplications.

Méthode de Horner : En profitant de la distributivité on évalue
$P(x) = ((\cdots((a_nx + a_{n-1})x + a_{n-2})\cdots x + a_2)x + a_1)x + a_0$.
Ceci ne nécessite que n additions et n multiplications !

Exemples : Pour $n = 100$ on passe de 5050 à 100 multiplications.
Pour $n = 1000$ on passe de 500500 à 1000 multiplications.

La méthode de Horner : calcul de $P(x_0)$

Soit $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ un polynôme dans $\mathbb{K}[X]$.
Comment calculer efficacement $P(x)$ pour $x \in \mathbb{K}$?

Méthode naïve : On calcule a_kx^k en effectuant k multiplications.
Implémenté ainsi, le calcul de $P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ nécessite n additions et $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ multiplications.

Méthode de Horner : En profitant de la distributivité on évalue
$P(x) = ((\cdots((a_nx + a_{n-1})x + a_{n-2})\cdots x + a_2)x + a_1)x + a_0$.
Ceci ne nécessite que n additions et n multiplications !

Exemples : Pour $n = 100$ on passe de 5050 à 100 multiplications.
Pour $n = 1000$ on passe de 500500 à 1000 multiplications.

Algorithme 16 évaluation d'un polynôme selon Horner

Entrée: des coefficients $a_0, a_1, a_2, \ldots, a_n \in \mathbb{K}$ et un élément $x_0 \in \mathbb{K}$.

Sortie: la valeur $y = a_0 + a_1x_0 + a_2x_0^2 + \cdots + a_nx_0^n$.

$y \leftarrow a_n$
pour k **de** $n-1$ **à** 0 **faire** $y \leftarrow y \cdot x_0 + a_k$ **fin pour**
retourner y

La méthode de Horner–Taylor : calcul de $P(X + x_0)$

Objectif.
Étant donné $P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ et $x_0 \in \mathbb{K}$
on cherche $P = b_0 + \underbrace{b_1(X - x_0) + b_2(X - x_0)^2 + \cdots + b_n(X - x_0)^n}_{(X-x_0)Q}$.

La méthode de Horner–Taylor : calcul de $P(X + x_0)$

Objectif.
Étant donné $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ et $x_0 \in \mathbb{K}$
on cherche $P = b_0 + \underbrace{b_1(X - x_0) + b_2(X - x_0)^2 + \cdots + b_n(X - x_0)^n}_{(X-x_0)Q}$.

Méthode de Horner :
On effectue une division euclidienne $P = q_0 + (X - x_0)Q$.

La méthode de Horner–Taylor : calcul de $P(X + x_0)$

Objectif.
Étant donné $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ et $x_0 \in \mathbb{K}$
on cherche $P = b_0 + \underbrace{b_1(X - x_0) + b_2(X - x_0)^2 + \cdots + b_n(X - x_0)^n}_{(X-x_0)Q}$.

Méthode de Horner :
On effectue une division euclidienne $P = q_0 + (X - x_0)Q$.

Algorithme 19 division euclidienne par $(X - x_0)$

Entrée: des coefficients $a_0, a_1, a_2, \ldots, a_n \in \mathbb{K}$ et un élément $x_0 \in \mathbb{K}$.

Sortie: des coefficients $q_0, q_1, q_2, \ldots, q_n \in \mathbb{K}$ tels que $P = q_0 + (X - x_0)Q$ où $P = \sum_{k=0}^{n} a_kX^k$ et $Q = \sum_{k=0}^{n-1} q_{k+1}X^k$.

$q_n \leftarrow a_n$
pour k **de** $n-1$ **à** 0 **faire** $q_k \leftarrow q_{k+1} \cdot x_0 + a_k$ **fin pour**
retourner $q_0, q_1, q_2, \ldots, q_n$

La méthode de Horner–Taylor : calcul de $P(X + x_0)$

Objectif.
Étant donné $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ et $x_0 \in \mathbb{K}$
on cherche $P = b_0 + \underbrace{b_1(X - x_0) + b_2(X - x_0)^2 + \cdots + b_n(X - x_0)^n}_{(X-x_0)Q}$.

Méthode de Horner :
On effectue une division euclidienne $P = q_0 + (X - x_0)Q$.

Algorithme 20 division euclidienne par $(X - x_0)$

Entrée: des coefficients $a_0, a_1, a_2, \ldots, a_n \in \mathbb{K}$ et un élément $x_0 \in \mathbb{K}$.

Sortie: des coefficients $q_0, q_1, q_2, \ldots, q_n \in \mathbb{K}$ tels que $P = q_0 + (X - x_0)Q$ où $P = \sum_{k=0}^{n} a_kX^k$ et $Q = \sum_{k=0}^{n-1} q_{k+1}X^k$.

$q_n \leftarrow a_n$
pour k **de** $n-1$ **à** 0 **faire** $q_k \leftarrow q_{k+1} \cdot x_0 + a_k$ **fin pour**
retourner $q_0, q_1, q_2, \ldots, q_n$

Ainsi $b_0 = q_0$ et $b_1 + b_2(X - x_0) + \cdots + b_n(X - x_0)^{n-1} = Q$.

La méthode de Horner–Taylor : calcul de $P(X + x_0)$

Objectif.
Étant donné $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ et $x_0 \in \mathbb{K}$
on cherche $P = b_0 + \underbrace{b_1(X - x_0) + b_2(X - x_0)^2 + \cdots + b_n(X - x_0)^n}_{(X-x_0)Q}$.

Méthode de Horner :
On effectue une division euclidienne $P = q_0 + (X - x_0)Q$.

Algorithme 21 division euclidienne par $(X - x_0)$

Entrée: des coefficients $a_0, a_1, a_2, \ldots, a_n \in \mathbb{K}$ et un élément $x_0 \in \mathbb{K}$.

Sortie: des coefficients $q_0, q_1, q_2, \ldots, q_n \in \mathbb{K}$ tels que $P = q_0 + (X - x_0)Q$ où $P = \sum_{k=0}^{n} a_kX^k$ et $Q = \sum_{k=0}^{n-1} q_{k+1}X^k$.

$q_n \leftarrow a_n$
pour k **de** $n-1$ **à** 0 **faire** $q_k \leftarrow q_{k+1} \cdot x_0 + a_k$ **fin pour**
retourner $q_0, q_1, q_2, \ldots, q_n$

Ainsi $b_0 = q_0$ et $b_1 + b_2(X - x_0) + \cdots + b_n(X - x_0)^{n-1} = Q$.

On calcule ensuite les coefficients $b_1, b_2, \ldots, b_n$ par récurrence.

La méthode de Horner–Taylor, prête à programmer

L'algorithme 22 résume la méthode issue de notre discussion :

Algorithme 22 la méthode de Horner–Taylor

Entrée: $a_0, a_1, \ldots, a_n \in \mathbb{K}$ et $x_0 \in \mathbb{K}$.

Sortie: $b_0, b_1, \ldots, b_n \in \mathbb{K}$ tels que $\sum_{k=0}^{n} b_k (X - x_0)^k = \sum_{k=0}^{n} a_k X^k$.

pour j **de** 0 **à** n **faire** $b_j \leftarrow a_j$ **fin pour**
pour ℓ **de** 0 **à** $n-1$ **faire**
  pour k **de** $n-1$ **à** ℓ **faire** $b_k \leftarrow b_{k+1} \cdot x_0 + b_k$ **fin pour**
fin pour
retourner $b_0, b_1, \ldots, b_n$

La méthode de Horner–Taylor, prête à programmer

L'algorithme 22 résume la méthode issue de notre discussion :

Algorithme 23 la méthode de Horner–Taylor

Entrée: $a_0, a_1, \ldots, a_n \in \mathbb{K}$ et $x_0 \in \mathbb{K}$.

Sortie: $b_0, b_1, \ldots, b_n \in \mathbb{K}$ tels que $\sum_{k=0}^{n} b_k (X - x_0)^k = \sum_{k=0}^{n} a_k X^k$.

pour j **de** 0 **à** n **faire** $b_j \leftarrow a_j$ **fin pour**
pour ℓ **de** 0 **à** $n-1$ **faire**
  pour k **de** $n-1$ **à** ℓ **faire** $b_k \leftarrow b_{k+1} \cdot x_0 + b_k$ **fin pour**
fin pour
retourner $b_0, b_1, \ldots, b_n$

Conclusion

Étant donné $P = \sum a_k X^k$, les coefficients de $P = \sum b_k (X - x_0)^k$ peuvent être calculés avec $\frac{n(n+1)}{2}$ multiplications et $\frac{n(n+1)}{2}$ additions.

Multiplicité d'une racine

On dit que $r \in \mathbb{K}$ est une *racine* de $P \in \mathbb{K}[X]$ si $P(r) = 0$.

Multiplicité d'une racine

On dit que $r \in \mathbb{K}$ est une *racine* de $P \in \mathbb{K}[X]$ si $P(r) = 0$.

Proposition

Un élément $r \in \mathbb{K}$ est une racine de P ssi $P = (X - r)Q$ où $Q \in \mathbb{K}[X]$.

Multiplicité d'une racine

On dit que $r \in \mathbb{K}$ est une *racine* de $P \in \mathbb{K}[X]$ si $P(r) = 0$.

Proposition

Un élément $r \in \mathbb{K}$ est une racine de P ssi $P = (X - r)Q$ où $Q \in \mathbb{K}[X]$.

Démonstration. Il existe des polynômes $Q, R \in \mathbb{K}[X]$ tels que $P = (X - r)Q + R$ et $\deg R < \deg(X - r) = 1$, donc $R \in \mathbb{K}$.

Multiplicité d'une racine

On dit que $r \in \mathbb{K}$ est une *racine* de $P \in \mathbb{K}[X]$ si $P(r) = 0$.

Proposition

Un élément $r \in \mathbb{K}$ est une racine de P ssi $P = (X - r)Q$ où $Q \in \mathbb{K}[X]$.

Démonstration. Il existe des polynômes $Q, R \in \mathbb{K}[X]$ tels que $P = (X - r)Q + R$ et $\deg R < \deg(X - r) = 1$, donc $R \in \mathbb{K}$.
Ainsi $P(r) = R$ s'annule si et seulement si $R = 0$. □

Multiplicité d'une racine

On dit que $r \in \mathbb{K}$ est une *racine* de $P \in \mathbb{K}[X]$ si $P(r) = 0$.

Proposition

Un élément $r \in \mathbb{K}$ est une racine de P ssi $P = (X - r)Q$ où $Q \in \mathbb{K}[X]$.

Démonstration. Il existe des polynômes $Q, R \in \mathbb{K}[X]$ tels que $P = (X - r)Q + R$ et $\deg R < \deg(X - r) = 1$, donc $R \in \mathbb{K}$.
Ainsi $P(r) = R$ s'annule si et seulement si $R = 0$. □

Corollaire

Pour tout $P \in \mathbb{K}[X]^*$ et tout $r \in \mathbb{K}$ il existe un unique entier $m \geq 0$ tel que $P = (X - r)^m Q$ et $Q(r) \neq 0$. □

Multiplicité d'une racine

On dit que $r \in \mathbb{K}$ est une *racine* de $P \in \mathbb{K}[X]$ si $P(r) = 0$.

Proposition

Un élément $r \in \mathbb{K}$ est une racine de P ssi $P = (X - r)Q$ où $Q \in \mathbb{K}[X]$.

Démonstration. Il existe des polynômes $Q, R \in \mathbb{K}[X]$ tels que $P = (X - r)Q + R$ et $\deg R < \deg(X - r) = 1$, donc $R \in \mathbb{K}$.
Ainsi $P(r) = R$ s'annule si et seulement si $R = 0$. □

Corollaire

Pour tout $P \in \mathbb{K}[X]^*$ et tout $r \in \mathbb{K}$ il existe un unique entier $m \geq 0$ tel que $P = (X - r)^m Q$ et $Q(r) \neq 0$. □

Si $m \geq 1$ on dit que r est une racine de P de *multiplicité* m.

Multiplicité d'une racine

On dit que $r \in \mathbb{K}$ est une *racine* de $P \in \mathbb{K}[X]$ si $P(r) = 0$.

Proposition

Un élément $r \in \mathbb{K}$ est une racine de P ssi $P = (X - r)Q$ où $Q \in \mathbb{K}[X]$.

Démonstration. Il existe des polynômes $Q, R \in \mathbb{K}[X]$ tels que $P = (X - r)Q + R$ et $\deg R < \deg(X - r) = 1$, donc $R \in \mathbb{K}$.
Ainsi $P(r) = R$ s'annule si et seulement si $R = 0$. □

Corollaire

Pour tout $P \in \mathbb{K}[X]^*$ et tout $r \in \mathbb{K}$ il existe un unique entier $m \geq 0$ tel que $P = (X - r)^m Q$ et $Q(r) \neq 0$. □

Si $m \geq 1$ on dit que r est une racine de P de *multiplicité* m.
La racine est *simple* si $m = 1$, et *multiple* si $m \geq 2$.

Factorisation et racines

Corollaire

Tout $P \in \mathbb{K}[X]^*$ s'écrit comme $P = (X - r_1)^{m_1} \cdots (X - r_k)^{m_k} Q$ où $r_1, \ldots, r_k \in \mathbb{K}$ sont des racines distinctes, de multiplicité $m_1, \ldots, m_k \geq 1$, et $Q \in \mathbb{K}[X]$ n'a pas de racine dans $\mathbb{K}$.

Factorisation et racines

Corollaire

Tout $P \in \mathbb{K}[X]^*$ s'écrit comme $P = (X - r_1)^{m_1} \cdots (X - r_k)^{m_k} Q$ où $r_1, \ldots, r_k \in \mathbb{K}$ sont des racines distinctes, de multiplicité $m_1, \ldots, m_k \geq 1$, et $Q \in \mathbb{K}[X]$ n'a pas de racine dans $\mathbb{K}$.

Ainsi un polynôme de degré n sur $\mathbb{K}$ admet au plus n racines dans $\mathbb{K}$.

Factorisation et racines

Corollaire

Tout $P \in \mathbb{K}[X]^*$ s'écrit comme $P = (X - r_1)^{m_1} \cdots (X - r_k)^{m_k} Q$ où $r_1, \ldots, r_k \in \mathbb{K}$ sont des racines distinctes, de multiplicité $m_1, \ldots, m_k \geq 1$, et $Q \in \mathbb{K}[X]$ n'a pas de racine dans $\mathbb{K}$.

Ainsi un polynôme de degré n sur $\mathbb{K}$ admet au plus n racines dans $\mathbb{K}$.

Interpolation de Lagrange

Théorème

Étant donnés des points distincts $x_0, \ldots, x_n \in \mathbb{K}$ et des valeurs arbitraires $y_0, \ldots, y_n \in \mathbb{K}$, il existe un unique polynôme $P \in \mathbb{K}[X]$ de degré $\leq n$ vérifiant $P(x_k) = y_k$ pour tout $k = 0, \ldots, n$.

Interpolation de Lagrange

Théorème

Étant donnés des points distincts $x_0, \ldots, x_n \in \mathbb{K}$ et des valeurs arbitraires $y_0, \ldots, y_n \in \mathbb{K}$, il existe un unique polynôme $P \in \mathbb{K}[X]$ de degré $\leq n$ vérifiant $P(x_k) = y_k$ pour tout $k = 0, \ldots, n$.

On appelle P le polynôme interpolateur de Lagrange.

Interpolation de Lagrange

Théorème

Étant donnés des points distincts $x_0, \ldots, x_n \in \mathbb{K}$ et des valeurs arbitraires $y_0, \ldots, y_n \in \mathbb{K}$, il existe un unique polynôme $P \in \mathbb{K}[X]$ de degré $\leq n$ vérifiant $P(x_k) = y_k$ pour tout $k = 0, \ldots, n$.

On appelle P le polynôme interpolateur de Lagrange.

Dérivation des polynômes

Proposition

On définit la dérivation $\partial : \mathbb{K}[X] \to \mathbb{K}[X]$ *par*

$$\partial\Big(\sum_{k=0}^{n} p_k X^k\Big) := \sum_{k=1}^{n} k p_k X^{k-1}.$$

Dérivation des polynômes

Proposition

On définit la dérivation $\partial : \mathbb{K}[X] \to \mathbb{K}[X]$ *par*

$$\partial\Big(\sum_{k=0}^{n} p_k X^k\Big) := \sum_{k=1}^{n} k p_k X^{k-1}.$$

Cette application est $\mathbb{K}$*-linéaire et vérifie la règle de Leibniz :*

$$\partial(PQ) = (\partial P) \cdot Q + P \cdot (\partial Q).$$

Racines multiples et dérivée

Proposition

Un élément $r \in \mathbb{K}$ est une racine multiple de $P \in \mathbb{K}[X]^*$ si et seulement si r est une racine commune de P et de sa dérivée P'.

Racines multiples et dérivée

Proposition

Un élément $r \in \mathbb{K}$ est une racine multiple de $P \in \mathbb{K}[X]^*$ si et seulement si r est une racine commune de P et de sa dérivée P'.

Démonstration. Supposons $P = (X - r)^m Q$ avec $m \geq 1$ et $Q(r) \neq 0$.

Racines multiples et dérivée

Proposition

Un élément $r \in \mathbb{K}$ est une racine multiple de $P \in \mathbb{K}[X]^*$ si et seulement si r est une racine commune de P et de sa dérivée P'.

Démonstration. Supposons $P = (X - r)^m Q$ avec $m \geq 1$ et $Q(r) \neq 0$. En appliquant la règle de Leibniz on obtient la dérivée

$$P' = m(X - r)^{m-1} Q + (X - r)^m Q'.$$

Racines multiples et dérivée

Proposition

Un élément $r \in \mathbb{K}$ est une racine multiple de $P \in \mathbb{K}[X]^*$ si et seulement si r est une racine commune de P et de sa dérivée P'.

Démonstration. Supposons $P = (X - r)^m Q$ avec $m \geq 1$ et $Q(r) \neq 0$. En appliquant la règle de Leibniz on obtient la dérivée

$$P' = m(X - r)^{m-1} Q + (X - r)^m Q'.$$

Si $m = 1$, alors $P(r) = 0$ mais $P'(r) = Q(r) \neq 0$.

Racines multiples et dérivée

Proposition

Un élément $r \in \mathbb{K}$ est une racine multiple de $P \in \mathbb{K}[X]^*$ si et seulement si r est une racine commune de P et de sa dérivée P'.

Démonstration. Supposons $P = (X - r)^m Q$ avec $m \geq 1$ et $Q(r) \neq 0$. En appliquant la règle de Leibniz on obtient la dérivée

$$P' = m(X - r)^{m-1} Q + (X - r)^m Q'.$$

Si $m = 1$, alors $P(r) = 0$ mais $P'(r) = Q(r) \neq 0$.
Si $m \geq 2$, alors $P(r) = 0$ et $P'(r) = 0$. □

Racines multiples et dérivée

Proposition

Un élément $r \in \mathbb{K}$ est une racine multiple de $P \in \mathbb{K}[X]^*$ si et seulement si r est une racine commune de P et de sa dérivée P'.

Démonstration. Supposons $P = (X - r)^m Q$ avec $m \geq 1$ et $Q(r) \neq 0$. En appliquant la règle de Leibniz on obtient la dérivée

$$P' = m(X - r)^{m-1} Q + (X - r)^m Q'.$$

Si $m = 1$, alors $P(r) = 0$ mais $P'(r) = Q(r) \neq 0$.
Si $m \geq 2$, alors $P(r) = 0$ et $P'(r) = 0$. □

Corollaire

Si $\operatorname{pgcd}(P, P') = 1$ alors toute racine de P est simple.

Racines multiples et dérivée

Proposition

Un élément $r \in \mathbb{K}$ est une racine multiple de $P \in \mathbb{K}[X]^*$ si et seulement si r est une racine commune de P et de sa dérivée P'.

Démonstration. Supposons $P = (X - r)^m Q$ avec $m \geq 1$ et $Q(r) \neq 0$.
En appliquant la règle de Leibniz on obtient la dérivée

$$P' = m(X - r)^{m-1} Q + (X - r)^m Q'.$$

Si $m = 1$, alors $P(r) = 0$ mais $P'(r) = Q(r) \neq 0$.
Si $m \geq 2$, alors $P(r) = 0$ et $P'(r) = 0$. □

Corollaire

Si $\operatorname{pgcd}(P, P') = 1$ alors toute racine de P est simple.

Démonstration. Supposons $P(r) = 0$ et $P'(r) = 0$.

Racines multiples et dérivée

Proposition

Un élément $r \in \mathbb{K}$ est une racine multiple de $P \in \mathbb{K}[X]^*$ si et seulement si r est une racine commune de P et de sa dérivée P'.

Démonstration. Supposons $P = (X-r)^m Q$ avec $m \geq 1$ et $Q(r) \neq 0$.
En appliquant la règle de Leibniz on obtient la dérivée

$$P' = m(X-r)^{m-1}Q + (X-r)^m Q'.$$

Si $m = 1$, alors $P(r) = 0$ mais $P'(r) = Q(r) \neq 0$.
Si $m \geq 2$, alors $P(r) = 0$ et $P'(r) = 0$. □

Corollaire

Si $\operatorname{pgcd}(P, P') = 1$ alors toute racine de P est simple.

Démonstration. Supposons $P(r) = 0$ et $P'(r) = 0$.
Dans ce cas on aurait $P = (X-r)Q_0$ et $P' = (X-r)Q_1$,

Racines multiples et dérivée

Proposition

Un élément $r \in \mathbb{K}$ est une racine multiple de $P \in \mathbb{K}[X]^*$ si et seulement si r est une racine commune de P et de sa dérivée P'.

Démonstration. Supposons $P = (X-r)^m Q$ avec $m \geq 1$ et $Q(r) \neq 0$.
En appliquant la règle de Leibniz on obtient la dérivée

$$P' = m(X-r)^{m-1}Q + (X-r)^m Q'.$$

Si $m = 1$, alors $P(r) = 0$ mais $P'(r) = Q(r) \neq 0$.
Si $m \geq 2$, alors $P(r) = 0$ et $P'(r) = 0$. □

Corollaire

Si $\operatorname{pgcd}(P, P') = 1$ alors toute racine de P est simple.

Démonstration. Supposons $P(r) = 0$ et $P'(r) = 0$.
Dans ce cas on aurait $P = (X-r)Q_0$ et $P' = (X-r)Q_1$,
donc $\operatorname{pgcd}(P, P') = (X-r)\operatorname{pgcd}(Q_0, Q_1)$ serait de degré ≥ 1. □

Réduction aux racines simples

En général il est difficile de trouver des racines !
Par contre, il est facile de réduire leur multiplicité à 1 :

Réduction aux racines simples

En général il est difficile de trouver des racines !
Par contre, il est facile de réduire leur multiplicité à 1 :

Corollaire (sur $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$)

Pour tout polynôme $P \in \mathbb{K}[X]^*$ le quotient $P/\operatorname{pgcd}(P, P')$ a les mêmes racines que P, mais chacune est de multiplicité 1.

Réduction aux racines simples

En général il est difficile de trouver des racines !
Par contre, il est facile de réduire leur multiplicité à 1 :

Corollaire (sur $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$)

Pour tout polynôme $P \in \mathbb{K}[X]^*$ le quotient $P/\operatorname{pgcd}(P, P')$ a les mêmes racines que P, mais chacune est de multiplicité 1.

Démonstration.
Supposons $P = (X - r)^m Q$ où $m \geq 1$ et $Q(r) \neq 0$. Alors

$$P' = m(X - r)^{m-1} Q + (X - r)^m Q' = (X - r)^{m-1} R$$

où $R = mQ + (X - r)Q'$ et ainsi $R(r) = mQ(r) \neq 0$.

Réduction aux racines simples

En général il est difficile de trouver des racines !
Par contre, il est facile de réduire leur multiplicité à 1 :

Corollaire (sur $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$)

Pour tout polynôme $P \in \mathbb{K}[X]^*$ le quotient $P/\operatorname{pgcd}(P, P')$ a les mêmes racines que P, mais chacune est de multiplicité 1.

Démonstration.
Supposons $P = (X - r)^m Q$ où $m \geq 1$ et $Q(r) \neq 0$. Alors

$$P' = m(X - r)^{m-1} Q + (X - r)^m Q' = (X - r)^{m-1} R$$

où $R = mQ + (X - r)Q'$ et ainsi $R(r) = mQ(r) \neq 0$.

Autrement dit, r est une racine de P' de multiplicité $m - 1$.

Réduction aux racines simples

En général il est difficile de trouver des racines !
Par contre, il est facile de réduire leur multiplicité à 1 :

Corollaire (sur $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$)

Pour tout polynôme $P \in \mathbb{K}[X]^*$ le quotient $P/\operatorname{pgcd}(P, P')$ a les mêmes racines que P, mais chacune est de multiplicité 1.

Démonstration.
Supposons $P = (X - r)^m Q$ où $m \geq 1$ et $Q(r) \neq 0$. Alors

$$P' = m(X - r)^{m-1} Q + (X - r)^m Q' = (X - r)^{m-1} R$$

où $R = mQ + (X - r)Q'$ et ainsi $R(r) = mQ(r) \neq 0$.

Autrement dit, r est une racine de P' de multiplicité $m - 1$.
Donc r est une racine de $\operatorname{pgcd}(P, P')$ de multiplicité $m - 1$.

Réduction aux racines simples

En général il est difficile de trouver des racines !
Par contre, il est facile de réduire leur multiplicité à 1 :

Corollaire (sur $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$)

Pour tout polynôme $P \in \mathbb{K}[X]^*$ le quotient $P/\operatorname{pgcd}(P, P')$ a les mêmes racines que P, mais chacune est de multiplicité 1.

Démonstration.
Supposons $P = (X - r)^m Q$ où $m \geq 1$ et $Q(r) \neq 0$. Alors

$$P' = m(X - r)^{m-1} Q + (X - r)^m Q' = (X - r)^{m-1} R$$

où $R = mQ + (X - r)Q'$ et ainsi $R(r) = mQ(r) \neq 0$.

Autrement dit, r est une racine de P' de multiplicité $m - 1$.
Donc r est une racine de $\operatorname{pgcd}(P, P')$ de multiplicité $m - 1$.
On conclut que r est une racine simple de $P/\operatorname{pgcd}(P, P')$. □

Décomposable vs irréductible

Définition

Un polynôme $P \in \mathbb{K}[X]$ est *réductible* (ou décomposable) dans $\mathbb{K}[X]$ s'il existe $A, B \in \mathbb{K}[X]$ tels que $P = AB$ où $\deg A \geq 1$ et $\deg B \geq 1$.

Décomposable vs irréductible

Définition

Un polynôme $P \in \mathbb{K}[X]$ est *réductible* (ou décomposable) dans $\mathbb{K}[X]$ s'il existe $A, B \in \mathbb{K}[X]$ tels que $P = AB$ où $\deg A \geq 1$ et $\deg B \geq 1$.

Un polynôme $P \in \mathbb{K}[X]$ est *irréductible* (ou indécomposable) dans $\mathbb{K}[X]$ si $P = AB$ où $A, B \in \mathbb{K}[X]$ implique soit $A \in \mathbb{K}^\times$ soit $B \in \mathbb{K}^\times$.

Décomposable vs irréductible

Définition

Un polynôme $P \in \mathbb{K}[X]$ est *réductible* (ou décomposable) dans $\mathbb{K}[X]$ s'il existe $A, B \in \mathbb{K}[X]$ tels que $P = AB$ où $\deg A \geq 1$ et $\deg B \geq 1$.

Un polynôme $P \in \mathbb{K}[X]$ est *irréductible* (ou indécomposable) dans $\mathbb{K}[X]$ si $P = AB$ où $A, B \in \mathbb{K}[X]$ implique soit $A \in \mathbb{K}^\times$ soit $B \in \mathbb{K}^\times$.

Dans $\mathbb{K}[X]$ il y a donc quatre types de polynômes :

- L'élément nul : $P = 0 \Leftrightarrow \deg(P) = -\infty$.
- Les éléments inversibles : $P \in \mathbb{K}[X]^\times = \mathbb{K}^\times \Leftrightarrow \deg(P) = 0$.
- Les éléments irréductibles, nécessairement de degré ≥ 1.
- Les éléments décomposables, nécessairement de degré ≥ 2.

Décomposable vs irréductible

Définition

Un polynôme $P \in \mathbb{K}[X]$ est *réductible* (ou décomposable) dans $\mathbb{K}[X]$ s'il existe $A, B \in \mathbb{K}[X]$ tels que $P = AB$ où $\deg A \geq 1$ et $\deg B \geq 1$.

Un polynôme $P \in \mathbb{K}[X]$ est *irréductible* (ou indécomposable) dans $\mathbb{K}[X]$ si $P = AB$ où $A, B \in \mathbb{K}[X]$ implique soit $A \in \mathbb{K}^\times$ soit $B \in \mathbb{K}^\times$.

Dans $\mathbb{K}[X]$ il y a donc quatre types de polynômes :

- L'élément nul : $P = 0 \Leftrightarrow \deg(P) = -\infty$.
- Les éléments inversibles : $P \in \mathbb{K}[X]^\times = \mathbb{K}^\times \Leftrightarrow \deg(P) = 0$.
- Les éléments irréductibles, nécessairement de degré ≥ 1.
- Les éléments décomposables, nécessairement de degré ≥ 2.

 Étant donné $P \in \mathbb{K}[X]$ de degré élevé, il peut être difficile d'effectivement déterminer s'il est décomposable ou irréductible.

Décomposable vs irréductible

Définition

Un polynôme $P \in \mathbb{K}[X]$ est *réductible* (ou décomposable) dans $\mathbb{K}[X]$ s'il existe $A, B \in \mathbb{K}[X]$ tels que $P = AB$ où $\deg A \geq 1$ et $\deg B \geq 1$.

Un polynôme $P \in \mathbb{K}[X]$ est *irréductible* (ou indécomposable) dans $\mathbb{K}[X]$ si $P = AB$ où $A, B \in \mathbb{K}[X]$ implique soit $A \in \mathbb{K}^\times$ soit $B \in \mathbb{K}^\times$.

Dans $\mathbb{K}[X]$ il y a donc quatre types de polynômes :

- L'élément nul : $P = 0 \Leftrightarrow \deg(P) = -\infty$.
- Les éléments inversibles : $P \in \mathbb{K}[X]^\times = \mathbb{K}^\times \Leftrightarrow \deg(P) = 0$.
- Les éléments irréductibles, nécessairement de degré ≥ 1.
- Les éléments décomposables, nécessairement de degré ≥ 2.

 Étant donné $P \in \mathbb{K}[X]$ de degré élevé, il peut être difficile d'effectivement déterminer s'il est décomposable ou irréductible.

 Même si l'on sait d'avance que $P \in \mathbb{K}[X]$ est décomposable, il peut être difficile d'effectivement trouver une décomposition.

Décomposable vs irréductible : exemples

Observation

Tout polynôme $P = aX + b$ de degré 1 est irréductible.

Décomposable vs irréductible : exemples

Observation

Tout polynôme $P = aX + b$ de degré 1 est irréductible.

Si $\deg P \geq 2$ et $P(r) = 0$ alors $P = (X - r)Q$ est décomposable.

Décomposable vs irréductible : exemples

Observation

Tout polynôme $P = aX + b$ de degré 1 est irréductible.

Si $\deg P \geq 2$ et $P(r) = 0$ alors $P = (X - r)Q$ est décomposable.

Un polynôme $P \in \mathbb{K}[X]$ de degré 2 ou 3 est irréductible
si et seulement s'il n'admet pas de racine dans $\mathbb{K}$.

Décomposable vs irréductible : exemples

Observation

Tout polynôme $P = aX + b$ de degré 1 est irréductible.

Si $\deg P \geq 2$ et $P(r) = 0$ alors $P = (X - r)Q$ est décomposable.

Un polynôme $P \in \mathbb{K}[X]$ de degré 2 ou 3 est irréductible
si et seulement s'il n'admet pas de racine dans $\mathbb{K}$.

Exemple. Dans $\mathbb{R}[X]$ sont irréductibles les polynômes linéaires $aX - b$ où $a \neq 0$, et quadratiques $aX^2 + bX + c$ où $b^2 - 4ac < 0$.

Décomposable vs irréductible : exemples

Observation

Tout polynôme $P = aX + b$ de degré 1 est irréductible.

Si $\deg P \geq 2$ et $P(r) = 0$ alors $P = (X - r)Q$ est décomposable.

Un polynôme $P \in \mathbb{K}[X]$ de degré 2 ou 3 est irréductible
si et seulement s'il n'admet pas de racine dans $\mathbb{K}$.

Exemple. Dans $\mathbb{R}[X]$ sont irréductibles les polynômes linéaires $aX - b$ où $a \neq 0$, et quadratiques $aX^2 + bX + c$ où $b^2 - 4ac < 0$.

Exemple. $X^2 - 2$ et $X^3 - 2$ n'admettent pas de racine dans $\mathbb{Q}$ et sont donc irréductibles dans $\mathbb{Q}[X]$.

Décomposable vs irréductible : exemples

Observation

Tout polynôme $P = aX + b$ de degré 1 est irréductible.

Si $\deg P \geq 2$ et $P(r) = 0$ alors $P = (X - r)Q$ est décomposable.

Un polynôme $P \in \mathbb{K}[X]$ de degré 2 ou 3 est irréductible
si et seulement s'il n'admet pas de racine dans $\mathbb{K}$.

Exemple. Dans $\mathbb{R}[X]$ sont irréductibles les polynômes linéaires $aX - b$ où $a \neq 0$, et quadratiques $aX^2 + bX + c$ où $b^2 - 4ac < 0$.

Exemple. $X^2 - 2$ et $X^3 - 2$ n'admettent pas de racine dans $\mathbb{Q}$ et sont donc irréductibles dans $\mathbb{Q}[X]$. Ils sont décomposables dans $\mathbb{R}[X]$: $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ et $X^3 - 2 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4})$.

Décomposable vs irréductible : exemples

Observation

Tout polynôme $P = aX + b$ de degré 1 est irréductible.

Si $\deg P \geq 2$ et $P(r) = 0$ alors $P = (X - r)Q$ est décomposable.

Un polynôme $P \in \mathbb{K}[X]$ de degré 2 ou 3 est irréductible si et seulement s'il n'admet pas de racine dans $\mathbb{K}$.

Exemple. Dans $\mathbb{R}[X]$ sont irréductibles les polynômes linéaires $aX - b$ où $a \neq 0$, et quadratiques $aX^2 + bX + c$ où $b^2 - 4ac < 0$.

Exemple. $X^2 - 2$ et $X^3 - 2$ n'admettent pas de racine dans $\mathbb{Q}$ et sont donc irréductibles dans $\mathbb{Q}[X]$. Ils sont décomposables dans $\mathbb{R}[X]$: $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ et $X^3 - 2 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4})$. Sur $\mathbb{C}$ on a $X^3 - 2 = (X - \sqrt[3]{2})(X - j\sqrt[3]{2})(X - j^2\sqrt[3]{2})$ où $j = e^{2\pi i/3}$.

Décomposable vs irréductible : exemples

Observation

Tout polynôme $P = aX + b$ de degré 1 est irréductible.

Si $\deg P \geq 2$ et $P(r) = 0$ alors $P = (X - r)Q$ est décomposable.

Un polynôme $P \in \mathbb{K}[X]$ de degré 2 ou 3 est irréductible
si et seulement s'il n'admet pas de racine dans $\mathbb{K}$.

Exemple. Dans $\mathbb{R}[X]$ sont irréductibles les polynômes linéaires $aX - b$ où $a \neq 0$, et quadratiques $aX^2 + bX + c$ où $b^2 - 4ac < 0$.

Exemple. $X^2 - 2$ et $X^3 - 2$ n'admettent pas de racine dans $\mathbb{Q}$ et sont donc irréductibles dans $\mathbb{Q}[X]$. Ils sont décomposables dans $\mathbb{R}[X]$:
$X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ et $X^3 - 2 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4})$.
Sur $\mathbb{C}$ on a $X^3 - 2 = (X - \sqrt[3]{2})(X - j\sqrt[3]{2})(X - j^2\sqrt[3]{2})$ où $j = e^{2\pi i/3}$.

 Le polynôme $X^4 - 9$ n'admet pas de racine dans $\mathbb{Q}$.
Néanmoins il est décomposable : $X^4 - 9 = (X^2 - 3)(X^2 + 3)$.

Décomposition en facteurs irréductibles : existence

Lemme (existence d'une décomposition)

Pour tout $P \in \mathbb{K}[X]^*$ *il existe* $u \in \mathbb{K}^\times$ *et* $P_1, \ldots, P_k \in \mathbb{K}[X]$ *unitaires et irréductibles dans* $\mathbb{K}[X]$ *de sorte que* $P = uP_1 \cdots P_k$.

Décomposition en facteurs irréductibles : existence

Lemme (existence d'une décomposition)

Pour tout $P \in \mathbb{K}[X]^*$ il existe $u \in \mathbb{K}^\times$ et $P_1, \dots, P_k \in \mathbb{K}[X]$ unitaires et irréductibles dans $\mathbb{K}[X]$ de sorte que $P = uP_1 \cdots P_k$.

Lemme (d'Euclide)

Soit P irréductible dans $\mathbb{K}[X]$. Si $P \mid AB$ alors $P \mid A$ ou $P \mid B$.

Décomposition en facteurs irréductibles : existence

Lemme (existence d'une décomposition)

Pour tout $P \in \mathbb{K}[X]^*$ il existe $u \in \mathbb{K}^\times$ et $P_1, \dots, P_k \in \mathbb{K}[X]$ unitaires et irréductibles dans $\mathbb{K}[X]$ de sorte que $P = uP_1 \cdots P_k$.

Lemme (d'Euclide)

Soit P irréductible dans $\mathbb{K}[X]$. Si $P \mid AB$ alors $P \mid A$ ou $P \mid B$.

Démonstration. $C = \operatorname{pgcd}(P, A)$ divise P, supposé irréductible.

Décomposition en facteurs irréductibles : existence

Lemme (existence d'une décomposition)

Pour tout $P \in \mathbb{K}[X]^*$ il existe $u \in \mathbb{K}^\times$ et $P_1, \dots, P_k \in \mathbb{K}[X]$ unitaires et irréductibles dans $\mathbb{K}[X]$ de sorte que $P = uP_1 \cdots P_k$.

Lemme (d'Euclide)

Soit P irréductible dans $\mathbb{K}[X]$. Si $P \mid AB$ alors $P \mid A$ ou $P \mid B$.

Démonstration. $C = \operatorname{pgcd}(P, A)$ divise P, supposé irréductible.
On a donc ou $C = 1$ ou $C \sim P$. Si $C \sim P$ alors $P \mid A$.

Décomposition en facteurs irréductibles : existence

Lemme (existence d'une décomposition)

Pour tout $P \in \mathbb{K}[X]^*$ il existe $u \in \mathbb{K}^\times$ et $P_1, \dots, P_k \in \mathbb{K}[X]$ unitaires et irréductibles dans $\mathbb{K}[X]$ de sorte que $P = uP_1 \cdots P_k$.

Lemme (d'Euclide)

Soit P irréductible dans $\mathbb{K}[X]$. Si $P \mid AB$ alors $P \mid A$ ou $P \mid B$.

Démonstration. $C = \mathrm{pgcd}(P, A)$ divise P, supposé irréductible.
On a donc ou $C = 1$ ou $C \sim P$. Si $C \sim P$ alors $P \mid A$.

Si $C = 1$, alors il existe $U, V \in \mathbb{K}[X]$ tels que $AU + PV = 1$.

Décomposition en facteurs irréductibles : existence

Lemme (existence d'une décomposition)

Pour tout $P \in \mathbb{K}[X]^*$ il existe $u \in \mathbb{K}^\times$ et $P_1, \dots, P_k \in \mathbb{K}[X]$ unitaires et irréductibles dans $\mathbb{K}[X]$ de sorte que $P = uP_1 \cdots P_k$.

Lemme (d'Euclide)

Soit P irréductible dans $\mathbb{K}[X]$. Si $P \mid AB$ alors $P \mid A$ ou $P \mid B$.

Démonstration. $C = \operatorname{pgcd}(P, A)$ divise P, supposé irréductible.
On a donc ou $C = 1$ ou $C \sim P$. Si $C \sim P$ alors $P \mid A$.

Si $C = 1$, alors il existe $U, V \in \mathbb{K}[X]$ tels que $AU + PV = 1$.
Ainsi $PQ = AB$ entraîne $B = (AU + PV)B = P(QU + BV)$. □

Décomposition en facteurs irréductibles : unicité

Théorème (factorisation unique de polynômes)

Tout polynôme $P \in \mathbb{K}[X]^*$ s'écrit comme $P = uP_1 \cdots P_k$ où $u \in \mathbb{K}^\times$ et $P_1, \ldots, P_k \in \mathbb{K}[X]$ sont unitaires et irréductibles dans $\mathbb{K}[X]$.
Cette décomposition est unique à l'ordre des facteurs près.

Décomposition en facteurs irréductibles : unicité

Théorème (factorisation unique de polynômes)

Tout polynôme $P \in \mathbb{K}[X]^*$ s'écrit comme $P = uP_1 \cdots P_k$ où $u \in \mathbb{K}^\times$ et $P_1, \ldots, P_k \in \mathbb{K}[X]$ sont unitaires et irréductibles dans $\mathbb{K}[X]$. Cette décomposition est unique à l'ordre des facteurs près.

Unicité. Supposons $P = uP_1 \cdots P_k = vQ_1 \cdots Q_\ell$.

Décomposition en facteurs irréductibles : unicité

Théorème (factorisation unique de polynômes)

Tout polynôme $P \in \mathbb{K}[X]^*$ s'écrit comme $P = uP_1 \cdots P_k$ où $u \in \mathbb{K}^\times$ et $P_1, \ldots, P_k \in \mathbb{K}[X]$ sont unitaires et irréductibles dans $\mathbb{K}[X]$. Cette décomposition est unique à l'ordre des facteurs près.

Unicité. Supposons $P = uP_1 \cdots P_k = vQ_1 \cdots Q_\ell$.

Récurrence sur k : si $k = 0$ alors $\deg P = 0$, donc $\ell = 0$ et $P = u = v$.

Décomposition en facteurs irréductibles : unicité

Théorème (factorisation unique de polynômes)

Tout polynôme $P \in \mathbb{K}[X]^*$ s'écrit comme $P = uP_1 \cdots P_k$ où $u \in \mathbb{K}^\times$ et $P_1, \ldots, P_k \in \mathbb{K}[X]$ sont unitaires et irréductibles dans $\mathbb{K}[X]$. Cette décomposition est unique à l'ordre des facteurs près.

Unicité. Supposons $P = uP_1 \cdots P_k = vQ_1 \cdots Q_\ell$.

Récurrence sur k : si $k = 0$ alors $\deg P = 0$, donc $\ell = 0$ et $P = u = v$.

Supposons $k \geq 1$. Puisque P_k est irréductible, il divise un des facteurs $Q_1, \ldots, Q_\ell$. Après permutation on peut supposer que $P_k \mid Q_\ell$.

Décomposition en facteurs irréductibles : unicité

Théorème (factorisation unique de polynômes)

Tout polynôme $P \in \mathbb{K}[X]^*$ s'écrit comme $P = uP_1 \cdots P_k$ où $u \in \mathbb{K}^\times$ et $P_1, \ldots, P_k \in \mathbb{K}[X]$ sont unitaires et irréductibles dans $\mathbb{K}[X]$. Cette décomposition est unique à l'ordre des facteurs près.

Unicité. Supposons $P = uP_1 \cdots P_k = vQ_1 \cdots Q_\ell$.

Récurrence sur k : si $k = 0$ alors $\deg P = 0$, donc $\ell = 0$ et $P = u = v$.

Supposons $k \geq 1$. Puisque P_k est irréductible, il divise un des facteurs $Q_1, \ldots, Q_\ell$. Après permutation on peut supposer que $P_k \mid Q_\ell$.

Puisque Q_ℓ est irréductible, on a $P_k \sim Q_\ell$.

On suppose P_k et Q_ℓ unitaires, donc $P_k = Q_\ell$.

Décomposition en facteurs irréductibles : unicité

Théorème (factorisation unique de polynômes)

Tout polynôme $P \in \mathbb{K}[X]^*$ s'écrit comme $P = uP_1 \cdots P_k$ où $u \in \mathbb{K}^\times$ et $P_1, \ldots, P_k \in \mathbb{K}[X]$ sont unitaires et irréductibles dans $\mathbb{K}[X]$. Cette décomposition est unique à l'ordre des facteurs près.

Unicité. Supposons $P = uP_1 \cdots P_k = vQ_1 \cdots Q_\ell$.

Récurrence sur k : si $k = 0$ alors $\deg P = 0$, donc $\ell = 0$ et $P = u = v$.

Supposons $k \geq 1$. Puisque P_k est irréductible, il divise un des facteurs $Q_1, \ldots, Q_\ell$. Après permutation on peut supposer que $P_k \mid Q_\ell$.

Puisque Q_ℓ est irréductible, on a $P_k \sim Q_\ell$.
On suppose P_k et Q_ℓ unitaires, donc $P_k = Q_\ell$.

Par récurrence, $P/P_k = uP_1 \cdots P_{k-1} = vQ_1 \cdots Q_{\ell-1}$ implique $k = \ell$ ainsi que $u = v$ et $P_1 = Q_1$, …, $P_{k-1} = Q_{k-1}$, après permutation. □

Le théorème de Gauss-d'Alembert

Théorème (de Gauss-d'Alembert, version complexe)

Pour tout $P \in \mathbb{C}[X]$ de degré n il existe $r_1, r_2, \ldots, r_n \in \mathbb{C}$ et $u \in \mathbb{C}^\times$ tels que $P = u(X - r_1)(X - r_2) \cdots (X - r_n)$. Autrement dit, les seuls polynômes irréductibles dans $\mathbb{C}[X]$ sont ceux de degré 1. □

Le théorème de Gauss-d'Alembert

Théorème (de Gauss-d'Alembert, version complexe)

Pour tout $P \in \mathbb{C}[X]$ de degré n il existe $r_1, r_2, \ldots, r_n \in \mathbb{C}$ et $u \in \mathbb{C}^\times$ tels que $P = u(X - r_1)(X - r_2)\cdots(X - r_n)$. Autrement dit, les seuls polynômes irréductibles dans $\mathbb{C}[X]$ sont ceux de degré 1. □

Théorème (de Gauss-d'Alembert, version réelle)

Tout polynôme réel $P \in \mathbb{R}[X]$ factorise comme $P = uP_1P_2\cdots P_k$ où $u \in \mathbb{R}^\times$ et pour tout j on a ou bien $P_j = X - r_j$ avec $r_j \in \mathbb{R}$ ou bien $P_j = X^2 + p_jX + q_j$ avec $p_j, q_j \in \mathbb{R}$ et $p_j^2 - 4q_j < 0$. □

Le théorème de Gauss-d'Alembert

Théorème (de Gauss-d'Alembert, version complexe)

Pour tout $P \in \mathbb{C}[X]$ de degré n il existe $r_1, r_2, \ldots, r_n \in \mathbb{C}$ et $u \in \mathbb{C}^\times$ tels que $P = u(X - r_1)(X - r_2)\cdots(X - r_n)$. Autrement dit, les seuls polynômes irréductibles dans $\mathbb{C}[X]$ sont ceux de degré 1. □

Théorème (de Gauss-d'Alembert, version réelle)

Tout polynôme réel $P \in \mathbb{R}[X]$ factorise comme $P = uP_1P_2\cdots P_k$ où $u \in \mathbb{R}^\times$ et pour tout j on a ou bien $P_j = X - r_j$ avec $r_j \in \mathbb{R}$ ou bien $P_j = X^2 + p_jX + q_j$ avec $p_j, q_j \in \mathbb{R}$ et $p_j^2 - 4q_j < 0$. □

Par exemple, le polynôme $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$, mais se décompose comme $X^2 + 1 = (X + i)(X - i)$ dans $\mathbb{C}[X]$.

Sommaire

Le corps des fractions rationnelles

On note $\mathbb{K}(X)$ l'ensemble des fractions $\frac{A}{B}$ où $A, B \in \mathbb{K}[X]$, $B \neq 0$, avec l'identification $\frac{A}{B} = \frac{C}{D}$ dans $\mathbb{K}(X)$ ssi $AD = CB$ dans $\mathbb{K}[X]$.

Le corps des fractions rationnelles

On note $\mathbb{K}(X)$ l'ensemble des fractions $\frac{A}{B}$ où $A, B \in \mathbb{K}[X]$, $B \neq 0$, avec l'identification $\frac{A}{B} = \frac{C}{D}$ dans $\mathbb{K}(X)$ ssi $AD = CB$ dans $\mathbb{K}[X]$.

Pour ces fractions on définit l'addition et la multiplication par

$$\frac{A}{B} + \frac{C}{D} := \frac{AD + CB}{BD}, \qquad \frac{A}{B} \cdot \frac{C}{D} := \frac{AC}{BD}.$$

Le corps des fractions rationnelles

On note $\mathbb{K}(X)$ l'ensemble des fractions $\frac{A}{B}$ où $A, B \in \mathbb{K}[X]$, $B \neq 0$, avec l'identification $\frac{A}{B} = \frac{C}{D}$ dans $\mathbb{K}(X)$ ssi $AD = CB$ dans $\mathbb{K}[X]$.

Pour ces fractions on définit l'addition et la multiplication par

$$\frac{A}{B} + \frac{C}{D} := \frac{AD + CB}{BD}, \qquad \frac{A}{B} \cdot \frac{C}{D} := \frac{AC}{BD}.$$

Proposition

L'ensemble $\mathbb{K}(X)$ des fractions rationnelles sur $\mathbb{K}$ muni de l'addition $+$ et de la multiplication $\cdot$ définies ci-dessus est un corps.

Le corps des fractions rationnelles

On note $\mathbb{K}(X)$ l'ensemble des fractions $\frac{A}{B}$ où $A, B \in \mathbb{K}[X]$, $B \neq 0$, avec l'identification $\frac{A}{B} = \frac{C}{D}$ dans $\mathbb{K}(X)$ ssi $AD = CB$ dans $\mathbb{K}[X]$.

Pour ces fractions on définit l'addition et la multiplication par

$$\frac{A}{B} + \frac{C}{D} := \frac{AD + CB}{BD}, \qquad \frac{A}{B} \cdot \frac{C}{D} := \frac{AC}{BD}.$$

Proposition

L'ensemble $\mathbb{K}(X)$ des fractions rationnelles sur $\mathbb{K}$ muni de l'addition $+$ et de la multiplication $\cdot$ définies ci-dessus est un corps.

On remarque que $\frac{A}{1} + \frac{B}{1} = \frac{A+B}{1}$ et $\frac{A}{1} \cdot \frac{B}{1} = \frac{AB}{1}$.

Le corps des fractions rationnelles

On note $\mathbb{K}(X)$ l'ensemble des fractions $\frac{A}{B}$ où $A, B \in \mathbb{K}[X]$, $B \neq 0$, avec l'identification $\frac{A}{B} = \frac{C}{D}$ dans $\mathbb{K}(X)$ ssi $AD = CB$ dans $\mathbb{K}[X]$.

Pour ces fractions on définit l'addition et la multiplication par

$$\frac{A}{B} + \frac{C}{D} := \frac{AD + CB}{BD}, \qquad \frac{A}{B} \cdot \frac{C}{D} := \frac{AC}{BD}.$$

Proposition

L'ensemble $\mathbb{K}(X)$ des fractions rationnelles sur $\mathbb{K}$ muni de l'addition $+$ et de la multiplication $\cdot$ définies ci-dessus est un corps.

On remarque que $\frac{A}{1} + \frac{B}{1} = \frac{A+B}{1}$ et $\frac{A}{1} \cdot \frac{B}{1} = \frac{AB}{1}$.
Ainsi $\mathbb{K}[X] \subset \mathbb{K}(X)$ en identifiant $A \in \mathbb{K}[X]$ avec $\frac{A}{1} \in \mathbb{K}(X)$.

Le corps des fractions rationnelles

On note $\mathbb{K}(X)$ l'ensemble des fractions $\frac{A}{B}$ où $A, B \in \mathbb{K}[X]$, $B \neq 0$, avec l'identification $\frac{A}{B} = \frac{C}{D}$ dans $\mathbb{K}(X)$ ssi $AD = CB$ dans $\mathbb{K}[X]$.

Pour ces fractions on définit l'addition et la multiplication par

$$\frac{A}{B} + \frac{C}{D} := \frac{AD + CB}{BD}, \qquad \frac{A}{B} \cdot \frac{C}{D} := \frac{AC}{BD}.$$

Proposition

L'ensemble $\mathbb{K}(X)$ des fractions rationnelles sur $\mathbb{K}$ muni de l'addition $+$ et de la multiplication $\cdot$ définies ci-dessus est un corps.

On remarque que $\frac{A}{1} + \frac{B}{1} = \frac{A+B}{1}$ et $\frac{A}{1} \cdot \frac{B}{1} = \frac{AB}{1}$.
Ainsi $\mathbb{K}[X] \subset \mathbb{K}(X)$ en identifiant $A \in \mathbb{K}[X]$ avec $\frac{A}{1} \in \mathbb{K}(X)$.

Exercice (long mais bénéfique)

Vérifier la construction de $(\mathbb{K}(X), +, \cdot)$ et les axiomes de corps.

Décomposition en fractions simples

Objectif. On cherche à décomposer $\frac{Q}{P}$ en « fractions simples ».

Décomposition en fractions simples

Objectif. On cherche à décomposer $\frac{Q}{P}$ en « fractions simples ».

Factorisation (partielle) du dénominateur.
Si $P = AB$ avec $\mathrm{pgcd}(A, B) = 1$, alors il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$.

Décomposition en fractions simples

Objectif. On cherche à décomposer $\frac{Q}{P}$ en « fractions simples ».

Factorisation (partielle) du dénominateur.
Si $P = AB$ avec $\mathrm{pgcd}(A, B) = 1$, alors il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$. Ainsi notre fraction se décompose en une somme :

$$\frac{Q}{P} = \frac{Q(AU + BV)}{AB} = \frac{QU}{B} + \frac{QV}{A}.$$

Décomposition en fractions simples

Objectif. On cherche à décomposer $\frac{Q}{P}$ en « fractions simples ».

Factorisation (partielle) du dénominateur.
Si $P = AB$ avec $\mathrm{pgcd}(A, B) = 1$, alors il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$. Ainsi notre fraction se décompose en une somme :

$$\frac{Q}{P} = \frac{Q(AU + BV)}{AB} = \frac{QU}{B} + \frac{QV}{A}.$$

Étant donné A et B, c'est juste un calcul d'Euclide-Bézout.

Décomposition en fractions simples

Objectif. On cherche à décomposer $\frac{Q}{P}$ en « fractions simples ».

Factorisation (partielle) du dénominateur.
Si $P = AB$ avec $\mathrm{pgcd}(A, B) = 1$, alors il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$. Ainsi notre fraction se décompose en une somme :

$$\frac{Q}{P} = \frac{Q(AU + BV)}{AB} = \frac{QU}{B} + \frac{QV}{A}.$$

Étant donné A et B, c'est juste un calcul d'Euclide-Bézout.

Factorisation complète du dénominateur.
Tout polynôme unitaire $P \in \mathbb{K}[X]$ factorise comme $P = P_1^{m_1} \cdots P_k^{m_k}$ où tout P_i est irréductible unitaire, $m_i \geq 1$, et $P_i \neq P_j$ pour $i \neq j$.

Décomposition en fractions simples

Objectif. On cherche à décomposer $\frac{Q}{P}$ en « fractions simples ».

Factorisation (partielle) du dénominateur.
Si $P = AB$ avec $\mathrm{pgcd}(A, B) = 1$, alors il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$. Ainsi notre fraction se décompose en une somme :

$$\frac{Q}{P} = \frac{Q(AU + BV)}{AB} = \frac{QU}{B} + \frac{QV}{A}.$$


Étant donné A et B, c'est juste un calcul d'Euclide-Bézout.

Factorisation complète du dénominateur.
Tout polynôme unitaire $P \in \mathbb{K}[X]$ factorise comme $P = P_1^{m_1} \cdots P_k^{m_k}$ où tout P_i est irréductible unitaire, $m_i \geq 1$, et $P_i \neq P_j$ pour $i \neq j$.


Dans la pratique cette décomposition peut être difficile à trouver.

Décomposition en fractions simples

Objectif. On cherche à décomposer $\frac{Q}{P}$ en « fractions simples ».

Factorisation (partielle) du dénominateur.
Si $P = AB$ avec $\mathrm{pgcd}(A, B) = 1$, alors il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$. Ainsi notre fraction se décompose en une somme :

$$\frac{Q}{P} = \frac{Q(AU + BV)}{AB} = \frac{QU}{B} + \frac{QV}{A}.$$

 Étant donné A et B, c'est juste un calcul d'Euclide-Bézout.

Factorisation complète du dénominateur.
Tout polynôme unitaire $P \in \mathbb{K}[X]$ factorise comme $P = P_1^{m_1} \cdots P_k^{m_k}$ où tout P_i est irréductible unitaire, $m_i \geq 1$, et $P_i \neq P_j$ pour $i \neq j$.

 Dans la pratique cette décomposition peut être difficile à trouver.

Finalement, réduction d'une fraction $\frac{Q}{P^m}$.

Décomposition en fractions simples

Objectif. On cherche à décomposer $\frac{Q}{P}$ en « fractions simples ».

Factorisation (partielle) du dénominateur.
Si $P = AB$ avec $\operatorname{pgcd}(A, B) = 1$, alors il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$. Ainsi notre fraction se décompose en une somme :

$$\frac{Q}{P} = \frac{Q(AU + BV)}{AB} = \frac{QU}{B} + \frac{QV}{A}.$$


Étant donné A et B, c'est juste un calcul d'Euclide-Bézout.

Factorisation complète du dénominateur.
Tout polynôme unitaire $P \in \mathbb{K}[X]$ factorise comme $P = P_1^{m_1} \cdots P_k^{m_k}$ où tout P_i est irréductible unitaire, $m_i \geq 1$, et $P_i \neq P_j$ pour $i \neq j$.


Dans la pratique cette décomposition peut être difficile à trouver.

Finalement, réduction d'une fraction $\frac{Q}{P^m}$.
On développe $Q = Q_m + Q_{m-1}P + \cdots + Q_1 P^{m-1} + Q_0 P^m$ tel que $\deg Q_k < \deg P$ pour $k = 1, \ldots, m$.

Décomposition en fractions simples

Objectif. On cherche à décomposer $\frac{Q}{P}$ en « fractions simples ».

Factorisation (partielle) du dénominateur.
Si $P = AB$ avec $\operatorname{pgcd}(A, B) = 1$, alors il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$. Ainsi notre fraction se décompose en une somme :

$$\frac{Q}{P} = \frac{Q(AU + BV)}{AB} = \frac{QU}{B} + \frac{QV}{A}.$$


Étant donné A et B, c'est juste un calcul d'Euclide-Bézout.

Factorisation complète du dénominateur.
Tout polynôme unitaire $P \in \mathbb{K}[X]$ factorise comme $P = P_1^{m_1} \cdots P_k^{m_k}$ où tout P_i est irréductible unitaire, $m_i \geq 1$, et $P_i \neq P_j$ pour $i \neq j$.


Dans la pratique cette décomposition peut être difficile à trouver.

Finalement, réduction d'une fraction $\frac{Q}{P^m}$.
On développe $Q = Q_m + Q_{m-1}P + \cdots + Q_1 P^{m-1} + Q_0 P^m$ tel que $\deg Q_k < \deg P$ pour $k = 1, \ldots, m$. Ainsi on obtient

$$\frac{Q}{P^m} = Q_0 + \frac{Q_1}{P} + \cdots + \frac{Q_{m-1}}{P^{m-1}} + \frac{Q_m}{P^m}.$$

Décomposition en fractions simples

Objectif. On cherche à décomposer $\frac{Q}{P}$ en « fractions simples ».

Factorisation (partielle) du dénominateur.
Si $P = AB$ avec $\operatorname{pgcd}(A, B) = 1$, alors il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$. Ainsi notre fraction se décompose en une somme :

$$\frac{Q}{P} = \frac{Q(AU + BV)}{AB} = \frac{QU}{B} + \frac{QV}{A}.$$

 Étant donné A et B, c'est juste un calcul d'Euclide-Bézout.

Factorisation complète du dénominateur.
Tout polynôme unitaire $P \in \mathbb{K}[X]$ factorise comme $P = P_1^{m_1} \cdots P_k^{m_k}$ où tout P_i est irréductible unitaire, $m_i \geq 1$, et $P_i \neq P_j$ pour $i \neq j$.

 Dans la pratique cette décomposition peut être difficile à trouver.

Finalement, réduction d'une fraction $\frac{Q}{P^m}$.
On développe $Q = Q_m + Q_{m-1}P + \cdots + Q_1 P^{m-1} + Q_0 P^m$ tel que $\deg Q_k < \deg P$ pour $k = 1, \ldots, m$. Ainsi on obtient

$$\frac{Q}{P^m} = Q_0 + \frac{Q_1}{P} + \cdots + \frac{Q_{m-1}}{P^{m-1}} + \frac{Q_m}{P^m}.$$

 Étant donné Q et P, c'est juste une division euclidienne itérée.

Décomposition en fractions simples

Théorème (décomposition en fractions simples)

Tout polynôme unitaire $P \in \mathbb{K}[X]$ factorise comme

(1) $$P = P_1^{m_1} \cdots P_k^{m_k}$$

où tout P_i est irréductible unitaire, $m_i \geq 1$, et $P_i \neq P_j$ pour $i \neq j$.

Décomposition en fractions simples

Théorème (décomposition en fractions simples)

Tout polynôme unitaire $P \in \mathbb{K}[X]$ factorise comme

(1) $$P = P_1^{m_1} \cdots P_k^{m_k}$$

où tout P_i est irréductible unitaire, $m_i \geq 1$, et $P_i \neq P_j$ pour $i \neq j$.

Par conséquent, toute fraction $\frac{Q}{P}$ se décompose comme

(2) $$\begin{aligned} \frac{Q}{P} = Q_0 &+ \frac{Q_{11}}{P_1} + \frac{Q_{12}}{P_1^2} + \cdots + \frac{Q_{1m_1}}{P_1^{m_1}} \\ &+ \cdots \\ &+ \frac{Q_{k1}}{P_k} + \frac{Q_{k2}}{P_k^2} + \cdots + \frac{Q_{km_k}}{P_k^{m_k}}. \end{aligned}$$

pour certains polynômes $Q_0, Q_{ij} \in \mathbb{K}[X]$ vérifiant $\deg Q_{ij} < \deg P_i$.

Décomposition en fractions simples

Théorème (décomposition en fractions simples)

Tout polynôme unitaire $P \in \mathbb{K}[X]$ factorise comme

(1) $$P = P_1^{m_1} \cdots P_k^{m_k}$$

où tout P_i est irréductible unitaire, $m_i \geq 1$, et $P_i \neq P_j$ pour $i \neq j$.

Par conséquent, toute fraction $\frac{Q}{P}$ se décompose comme

(2) $$\begin{aligned} \frac{Q}{P} = Q_0 &+ \frac{Q_{11}}{P_1} + \frac{Q_{12}}{P_1^2} + \cdots + \frac{Q_{1m_1}}{P_1^{m_1}} \\ &+ \cdots \\ &+ \frac{Q_{k1}}{P_k} + \frac{Q_{k2}}{P_k^2} + \cdots + \frac{Q_{km_k}}{P_k^{m_k}}. \end{aligned}$$

pour certains polynômes $Q_0, Q_{ij} \in \mathbb{K}[X]$ vérifiant $\deg Q_{ij} < \deg P_i$.


Dans la pratique la factorisation (1) peut être difficile à expliciter.


Étant donnée (1), l'étape (2) est facile avec Euclide-Bézout.

Décomposition en fractions très simples

Corollaire (décomposition en fractions très simples)

Supposons que $P = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k}$ *où* $m_1, \ldots, m_k \geq 1$ *et* $a_1, \ldots, a_k \in \mathbb{K}$ *tels que* $a_i \neq a_j$ *pour* $i \neq j$.

Décomposition en fractions très simples

Corollaire (décomposition en fractions très simples)

Supposons que $P = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k}$ *où* $m_1, \ldots, m_k \geq 1$ *et* $a_1, \ldots, a_k \in \mathbb{K}$ *tels que* $a_i \neq a_j$ *pour* $i \neq j$. *Alors pour tout* $Q \in \mathbb{K}[X]$ *il existe un polynôme* $Q_0 \in \mathbb{K}[X]$ *et des coefficients* $\alpha_{ij} \in \mathbb{K}$ *tels que*

$$\begin{aligned}\frac{Q}{P} = Q_0 &+ \frac{\alpha_{11}}{X - a_1} + \frac{\alpha_{12}}{(X - a_1)^2} + \cdots + \frac{\alpha_{1m_1}}{(X - a_1)^{m_1}} \\ &+ \ldots \\ &+ \frac{\alpha_{k1}}{X - a_k} + \frac{\alpha_{k2}}{(X - a_k)^2} + \cdots + \frac{\alpha_{km_k}}{(X - a_k)^{m_k}}.\end{aligned}$$

Décomposition en fractions très simples

Corollaire (décomposition en fractions très simples)

Supposons que $P = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k}$ *où* $m_1, \ldots, m_k \geq 1$ *et* $a_1, \ldots, a_k \in \mathbb{K}$ *tels que* $a_i \neq a_j$ *pour* $i \neq j$. *Alors pour tout* $Q \in \mathbb{K}[X]$ *il existe un polynôme* $Q_0 \in \mathbb{K}[X]$ *et des coefficients* $\alpha_{ij} \in \mathbb{K}$ *tels que*

$$\begin{aligned}\frac{Q}{P} = Q_0 &+ \frac{\alpha_{11}}{X - a_1} + \frac{\alpha_{12}}{(X - a_1)^2} + \cdots + \frac{\alpha_{1m_1}}{(X - a_1)^{m_1}} \\ &+ \cdots \\ &+ \frac{\alpha_{k1}}{X - a_k} + \frac{\alpha_{k2}}{(X - a_k)^2} + \cdots + \frac{\alpha_{km_k}}{(X - a_k)^{m_k}}.\end{aligned}$$

Attention à l'hypothèse !

Sur $\mathbb{C}$ tout polynôme unitaire P factorise comme souhaité.

Sur $\mathbb{R}$ il peut y avoir des facteurs irréductibles de degré 2.

(Dans ce cas on revient au théorème précédent.)

Primitive d'une fraction rationnelle

Dériver un polynôme

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

dans $\mathbb{R}[X]$ est facile car

$$P' = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}.$$

Primitive d'une fraction rationnelle

Dériver un polynôme

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

dans $\mathbb{R}[X]$ est facile car

$$P' = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}.$$

Intégrer est aussi facile : le polynôme

$$S = a_0 X + \frac{1}{2} a_1 X^2 + \frac{1}{3} a_1 X^3 + \cdots + \frac{1}{n+1} a_1 X^{n+1}$$

est une primitive de P car $S' = P$.

Primitive d'une fraction rationnelle

Dériver un polynôme

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

dans $\mathbb{R}[X]$ est facile car

$$P' = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}.$$

Intégrer est aussi facile : le polynôme

$$S = a_0 X + \frac{1}{2} a_1 X^2 + \frac{1}{3} a_1 X^3 + \cdots + \frac{1}{n+1} a_1 X^{n+1}$$

est une primitive de P car $S' = P$.

Dériver une fraction rationnelle dans $\mathbb{R}(X)$ est facile car

$$\left(\frac{Q}{P}\right)' = \frac{Q'P - QP'}{P^2}.$$

Primitive d'une fraction rationnelle

Dériver un polynôme

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

dans $\mathbb{R}[X]$ est facile car

$$P' = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}.$$

Intégrer est aussi facile : le polynôme

$$S = a_0 X + \frac{1}{2} a_1 X^2 + \frac{1}{3} a_1 X^3 + \cdots + \frac{1}{n+1} a_1 X^{n+1}$$

est une primitive de P car $S' = P$.

Dériver une fraction rationnelle dans $\mathbb{R}(X)$ est facile car

$$\left(\frac{Q}{P}\right)' = \frac{Q'P - QP'}{P^2}.$$

Mais comment intégrer ? Le résultat sera-t-il à nouveau dans $\mathbb{R}(X)$?

Primitive d'une fraction rationnelle

Dériver un polynôme

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

dans $\mathbb{R}[X]$ est facile car

$$P' = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}.$$

Intégrer est aussi facile : le polynôme

$$S = a_0 X + \frac{1}{2} a_1 X^2 + \frac{1}{3} a_1 X^3 + \cdots + \frac{1}{n+1} a_1 X^{n+1}$$

est une primitive de P car $S' = P$.

Dériver une fraction rationnelle dans $\mathbb{R}(X)$ est facile car

$$\left(\frac{Q}{P}\right)' = \frac{Q'P - QP'}{P^2}.$$

Mais comment intégrer ? Le résultat sera-t-il à nouveau dans $\mathbb{R}(X)$?
En général, non ! Apparaissent deux primitives transcendantes :

$$\int \frac{dx}{x} = \ln|x| \quad \text{et} \qquad \int \frac{dx}{x^2+1} = \arctan x.$$

Primitive d'une fraction rationnelle

Rappelons que dans $\mathbb{R}[X]$ sont irréductibles les polynômes linéaires $aX - b$ où $a \neq 0$ et quadratiques $aX^2 + bX + c$ vérifiant $b^2 - 4ac < 0$:

Primitive d'une fraction rationnelle

Rappelons que dans $\mathbb{R}[X]$ sont irréductibles les polynômes linéaires $aX - b$ où $a \neq 0$ et quadratiques $aX^2 + bX + c$ vérifiant $b^2 - 4ac < 0$:

Théorème (de Gauss-d'Alembert, version réelle)

Tout polynôme réel $P \in \mathbb{R}[X]$ factorise comme $P = uP_1^{m_1} \cdots P_k^{m_k}$ où $u \in \mathbb{R}^\times$ et pour tout j on a ou bien $P_j = X - r_j$ avec $r_j \in \mathbb{R}$ ou bien $P_j = X^2 + p_j X + q_j$ avec $p_j, q_j \in \mathbb{R}$ et $p_j^2 - 4q_j < 0$. □

Primitive d'une fraction rationnelle

Rappelons que dans $\mathbb{R}[X]$ sont irréductibles les polynômes linéaires $aX - b$ où $a \neq 0$ et quadratiques $aX^2 + bX + c$ vérifiant $b^2 - 4ac < 0$:

Théorème (de Gauss-d'Alembert, version réelle)

Tout polynôme réel $P \in \mathbb{R}[X]$ factorise comme $P = uP_1^{m_1} \cdots P_k^{m_k}$ où $u \in \mathbb{R}^\times$ et pour tout j on a ou bien $P_j = X - r_j$ avec $r_j \in \mathbb{R}$ ou bien $P_j = X^2 + p_j X + q_j$ avec $p_j, q_j \in \mathbb{R}$ et $p_j^2 - 4q_j < 0$. □

Ici on peut et on va supposer que $P_i \neq P_j$ pour tout $i \neq j$.

Primitive d'une fraction rationnelle

Rappelons que dans $\mathbb{R}[X]$ sont irréductibles les polynômes linéaires $aX - b$ où $a \neq 0$ et quadratiques $aX^2 + bX + c$ vérifiant $b^2 - 4ac < 0$:

Théorème (de Gauss-d'Alembert, version réelle)

Tout polynôme réel $P \in \mathbb{R}[X]$ factorise comme $P = uP_1^{m_1} \cdots P_k^{m_k}$ où $u \in \mathbb{R}^\times$ et pour tout j on a ou bien $P_j = X - r_j$ avec $r_j \in \mathbb{R}$ ou bien $P_j = X^2 + p_j X + q_j$ avec $p_j, q_j \in \mathbb{R}$ et $p_j^2 - 4q_j < 0$. □

Ici on peut et on va supposer que $P_i \neq P_j$ pour tout $i \neq j$.
Par conséquent, toute fraction $\frac{Q}{P}$ se décompose comme

$$\begin{aligned}\frac{Q}{P} = Q_0 &+ \frac{Q_{11}}{P_1} + \frac{Q_{12}}{P_1^2} + \cdots + \frac{Q_{1m_1}}{P_1^{m_1}} \\ &+ \cdots \\ &+ \frac{Q_{k1}}{P_k} + \frac{Q_{k2}}{P_k^2} + \cdots + \frac{Q_{km_k}}{P_k^{m_k}}.\end{aligned}$$

pour certains polynômes $Q_0, Q_{ij} \in \mathbb{K}[X]$ vérifiant $\deg Q_{ij} < \deg P_i$.

Primitive d'une fraction rationnelle

Comment intégrer $\frac{Q}{P} \in \mathbb{R}(X)$?

Primitive d'une fraction rationnelle

Comment intégrer $\frac{Q}{P} \in \mathbb{R}(X)$? Voici quelques intégrales faciles :

$$\int \frac{1}{x-a} dx = \ln|x-a|$$

$$\int \frac{1}{(x-a)^n} dx = \frac{1}{(n-1)(x-a)^{n-1}}$$

Primitive d'une fraction rationnelle

Comment intégrer $\frac{Q}{P} \in \mathbb{R}(X)$? Voici quelques intégrales faciles :

$$\int \frac{1}{x-a} dx = \ln|x-a|$$

$$\int \frac{1}{(x-a)^n} dx = \frac{1}{(n-1)(x-a)^{n-1}}$$

Ceci règle le cas où P se décompose en facteurs linéaires.

Primitive d'une fraction rationnelle

Comment intégrer $\frac{Q}{P} \in \mathbb{R}(X)$? Voici quelques intégrales faciles :

$$\int \frac{1}{x-a}dx = \ln|x-a|$$

$$\int \frac{1}{(x-a)^n}dx = \frac{1}{(n-1)(x-a)^{n-1}}$$

Ceci règle le cas où P se décompose en facteurs linéaires.

Regardons ensuite les dénominateurs irréductibles de degré 2 :

$$\int \frac{2x+p}{x^2+px+q}dx = \ln|x^2+px+q|$$

$$\int \frac{1}{x^2+px+q}dx = \frac{2}{\sqrt{4q-p^2}} \arctan \frac{2x+p}{\sqrt{4q-p^2}}$$

Primitive d'une fraction rationnelle

Comment intégrer $\frac{Q}{P} \in \mathbb{R}(X)$? Voici quelques intégrales faciles :

$$\int \frac{1}{x-a}dx = \ln|x-a|$$
$$\int \frac{1}{(x-a)^n}dx = \frac{1}{(n-1)(x-a)^{n-1}}$$

Ceci règle le cas où P se décompose en facteurs linéaires.

Regardons ensuite les dénominateurs irréductibles de degré 2 :

$$\int \frac{2x+p}{x^2+px+q}dx = \ln|x^2+px+q|$$
$$\int \frac{1}{x^2+px+q}dx = \frac{2}{\sqrt{4q-p^2}} \arctan \frac{2x+p}{\sqrt{4q-p^2}}$$

Démonstration. Une fois la formule trouvée, il suffit de dériver. □

Primitive d'une fraction rationnelle

On établit finalement deux intégrales plus compliquées pour les dénominateurs irréductibles de degré 2 et de multiplicité $n \geq 2$:

Primitive d'une fraction rationnelle

On établit finalement deux intégrales plus compliquées pour les dénominateurs irréductibles de degré 2 et de multiplicité $n \geq 2$:

$$\int \frac{2x+p}{(x^2+px+q)^n}dx = -\frac{1}{(n-1)(x^2+px+q)^{n-1}}$$

$$\int \frac{1}{(x^2+px+q)^n}dx = \frac{2x+p}{(n-1)(4q-p^2)(x^2+px+q)^{n-1}} + \frac{2(2n-3)}{(n-1)(4q-p^2)}\int \frac{1}{(x^2+px+q)^{n-1}}dx$$

Primitive d'une fraction rationnelle

On établit finalement deux intégrales plus compliquées pour les dénominateurs irréductibles de degré 2 et de multiplicité $n \geq 2$:

$$\int \frac{2x+p}{(x^2+px+q)^n}dx = -\frac{1}{(n-1)(x^2+px+q)^{n-1}}$$

$$\int \frac{1}{(x^2+px+q)^n}dx = \frac{2x+p}{(n-1)(4q-p^2)(x^2+px+q)^{n-1}} + \frac{2(2n-3)}{(n-1)(4q-p^2)}\int \frac{1}{(x^2+px+q)^{n-1}}dx$$

Théorème

Toute fraction rationnelle $\frac{Q}{P} \in \mathbb{R}(X)$ admet une primitive dans

$$\mathbb{R}(X)\{\ \ln|x-a|,\ \ln|x^2+px+q|,\ \arctan|ax+b|\ \}.$$

Primitive d'une fraction rationnelle

On établit finalement deux intégrales plus compliquées pour les dénominateurs irréductibles de degré 2 et de multiplicité $n \geq 2$:

$$\int \frac{2x+p}{(x^2+px+q)^n}dx = -\frac{1}{(n-1)(x^2+px+q)^{n-1}}$$

$$\int \frac{1}{(x^2+px+q)^n}dx = \frac{2x+p}{(n-1)(4q-p^2)(x^2+px+q)^{n-1}} + \frac{2(2n-3)}{(n-1)(4q-p^2)}\int \frac{1}{(x^2+px+q)^{n-1}}dx$$

Théorème

Toute fraction rationnelle $\frac{Q}{P} \in \mathbb{R}(X)$ admet une primitive dans

$$\mathbb{R}(X)\big\{\ln|x-a|,\ \ln|x^2+px+q|,\ \arctan|ax+b|\ \big\}.$$

Étant donnée la décomposition de P en facteurs irréductibles, la primitive peut être explicitée comme indiqué ci-dessus.

Résumé

1. Arithmétique des polynômes sur un corps, Euclide, Bézout
   - Polynômes sur un corps
   - La division euclidienne
   - Les algorithmes d'Euclide et de Bézout

2. Évaluation, racines, décomposition en facteurs irréductibles
   - Fonctions polynomiales, méthode de Horner, Horner–Taylor
   - Multiplicité d'une racine, réduction aux racines simples
   - Décomposition de polynômes en facteurs irréductibles

3. Fractions rationnelles, éléments simples, intégration symbolique
   - Le corps des fractions rationnelles
   - Décomposition d'une fraction en fractions simples
   - Primitive d'une fraction rationnelle