Introduction à la Cryptologie

Chapitre 9 : Anneaux de polynômes

Michael Eisermann (Institut Fourier, UJF Grenoble)

Année 2008-2009
IF / IMAG, Master 1, S1-S2

document mis à jour le 7 juillet 2009

www-fourier.ujf-grenoble.fr/~eiserm/cours#crypto

Sommaire

Sommaire

L'anneau des polynômes

Théorème

Pour tout anneau commutatif $\mathbb{K}$ il existe un anneau commutatif $\mathbb{K}[X]$ tel que :

L'anneau des polynômes

Théorème

Pour tout anneau commutatif $\mathbb{K}$ il existe un anneau commutatif $\mathbb{K}[X]$ tel que :

- *L'anneau $\mathbb{K}[X]$ contient $\mathbb{K}$ comme sous-anneau et X comme élément.*

L'anneau des polynômes

Théorème

Pour tout anneau commutatif $\mathbb{K}$ il existe un anneau commutatif $\mathbb{K}[X]$ tel que :

- *L'anneau $\mathbb{K}[X]$ contient $\mathbb{K}$ comme sous-anneau et X comme élément.*
- *Tout élément $P \in \mathbb{K}[X]^*$ s'écrit de manière unique comme*

$$P = a_0 + a_1 X^1 + \cdots + a_n X^n \quad \text{où} \quad n \in \mathbb{N},\ a_0, a_1, \ldots, a_n \in \mathbb{K},\ a_n \neq 0.$$

L'anneau des polynômes

Théorème

Pour tout anneau commutatif $\mathbb{K}$ il existe un anneau commutatif $\mathbb{K}[X]$ tel que :

- *L'anneau $\mathbb{K}[X]$ contient $\mathbb{K}$ comme sous-anneau et X comme élément.*
- *Tout élément $P \in \mathbb{K}[X]^*$ s'écrit de manière unique comme*

$$P = a_0 + a_1 X^1 + \cdots + a_n X^n \quad \text{où} \quad n \in \mathbb{N},\ a_0, a_1, \ldots, a_n \in \mathbb{K},\ a_n \neq 0.$$

Définition

Dans ce cas on dit que $\mathbb{K}[X]$ est *l'anneau des polynômes* sur l'anneau des coefficients $\mathbb{K}$ en la variable X.

L'anneau des polynômes

Théorème

Pour tout anneau commutatif $\mathbb{K}$ il existe un anneau commutatif $\mathbb{K}[X]$ tel que :

- *L'anneau $\mathbb{K}[X]$ contient $\mathbb{K}$ comme sous-anneau et X comme élément.*
- *Tout élément $P \in \mathbb{K}[X]^*$ s'écrit de manière unique comme*

$$P = a_0 + a_1 X^1 + \cdots + a_n X^n \quad \text{où} \quad n \in \mathbb{N},\ a_0, a_1, \ldots, a_n \in \mathbb{K},\ a_n \neq 0.$$

Définition

Dans ce cas on dit que $\mathbb{K}[X]$ est *l'anneau des polynômes* sur l'anneau des coefficients $\mathbb{K}$ en la variable X. On appelle P un *polynôme* sur $\mathbb{K}$ en X.

L'anneau des polynômes

Théorème

Pour tout anneau commutatif $\mathbb{K}$ il existe un anneau commutatif $\mathbb{K}[X]$ tel que :

- *L'anneau $\mathbb{K}[X]$ contient $\mathbb{K}$ comme sous-anneau et X comme élément.*
- *Tout élément $P \in \mathbb{K}[X]^*$ s'écrit de manière unique comme*

$$P = a_0 + a_1 X^1 + \cdots + a_n X^n \quad \text{où} \quad n \in \mathbb{N},\ a_0, a_1, \ldots, a_n \in \mathbb{K},\ a_n \neq 0.$$

Définition

Dans ce cas on dit que $\mathbb{K}[X]$ est *l'anneau des polynômes* sur l'anneau des coefficients $\mathbb{K}$ en la variable X. On appelle P un *polynôme* sur $\mathbb{K}$ en X.

On définit le *degré* $\deg P := n$ et le *coefficient dominant* $\operatorname{dom} P := a_n$.

L'anneau des polynômes

Théorème

Pour tout anneau commutatif $\mathbb{K}$ il existe un anneau commutatif $\mathbb{K}[X]$ tel que :

- *L'anneau $\mathbb{K}[X]$ contient $\mathbb{K}$ comme sous-anneau et X comme élément.*
- *Tout élément $P \in \mathbb{K}[X]^*$ s'écrit de manière unique comme*

$$P = a_0 + a_1 X^1 + \cdots + a_n X^n \quad \text{où} \quad n \in \mathbb{N},\ a_0, a_1, \ldots, a_n \in \mathbb{K},\ a_n \neq 0.$$

Définition

Dans ce cas on dit que $\mathbb{K}[X]$ est *l'anneau des polynômes* sur l'anneau des coefficients $\mathbb{K}$ en la variable X. On appelle P un *polynôme* sur $\mathbb{K}$ en X.

On définit le *degré* $\deg P := n$ et le *coefficient dominant* $\operatorname{dom} P := a_n$.

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

L'anneau des polynômes

Théorème

Pour tout anneau commutatif $\mathbb{K}$ il existe un anneau commutatif $\mathbb{K}[X]$ tel que :

- *L'anneau $\mathbb{K}[X]$ contient $\mathbb{K}$ comme sous-anneau et X comme élément.*
- *Tout élément $P \in \mathbb{K}[X]^*$ s'écrit de manière unique comme*

$$P = a_0 + a_1 X^1 + \cdots + a_n X^n \quad \text{où} \quad n \in \mathbb{N},\ a_0, a_1, \ldots, a_n \in \mathbb{K},\ a_n \neq 0.$$

Définition

Dans ce cas on dit que $\mathbb{K}[X]$ est *l'anneau des polynômes* sur l'anneau des coefficients $\mathbb{K}$ en la variable X. On appelle P un *polynôme* sur $\mathbb{K}$ en X.

On définit le *degré* $\deg P := n$ et le *coefficient dominant* $\operatorname{dom} P := a_n$.

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

Tout polynôme $P \in \mathbb{K}[X]$ peut être écrit de manière unique comme

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

L'anneau des polynômes

Théorème

Pour tout anneau commutatif $\mathbb{K}$ il existe un anneau commutatif $\mathbb{K}[X]$ tel que :

- *L'anneau $\mathbb{K}[X]$ contient $\mathbb{K}$ comme sous-anneau et X comme élément.*
- *Tout élément $P \in \mathbb{K}[X]^*$ s'écrit de manière unique comme*

$$P = a_0 + a_1 X^1 + \cdots + a_n X^n \quad \textit{où} \quad n \in \mathbb{N},\ a_0, a_1, \ldots, a_n \in \mathbb{K},\ a_n \neq 0.$$

Définition

Dans ce cas on dit que $\mathbb{K}[X]$ est *l'anneau des polynômes* sur l'anneau des coefficients $\mathbb{K}$ en la variable X. On appelle P un *polynôme* sur $\mathbb{K}$ en X.

On définit le *degré* $\deg P := n$ et le *coefficient dominant* $\operatorname{dom} P := a_n$.

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

Tout polynôme $P \in \mathbb{K}[X]$ peut être écrit de manière unique comme

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

sous-entendant que seul un nombre fini de coefficients a_k sont non nuls.

L'anneau des polynômes

Théorème

Pour tout anneau commutatif $\mathbb{K}$ il existe un anneau commutatif $\mathbb{K}[X]$ tel que :

- *L'anneau $\mathbb{K}[X]$ contient $\mathbb{K}$ comme sous-anneau et X comme élément.*
- *Tout élément $P \in \mathbb{K}[X]^*$ s'écrit de manière unique comme*

$$P = a_0 + a_1 X^1 + \cdots + a_n X^n \quad \textit{où} \quad n \in \mathbb{N},\ a_0, a_1, \ldots, a_n \in \mathbb{K},\ a_n \neq 0.$$

Définition

Dans ce cas on dit que $\mathbb{K}[X]$ est *l'anneau des polynômes* sur l'anneau des coefficients $\mathbb{K}$ en la variable X. On appelle P un *polynôme* sur $\mathbb{K}$ en X.

On définit le *degré* $\deg P := n$ et le *coefficient dominant* $\operatorname{dom} P := a_n$.

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

Tout polynôme $P \in \mathbb{K}[X]$ peut être écrit de manière unique comme

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

sous-entendant que seul un nombre fini de coefficients a_k sont non nuls.
Ainsi $\deg P = \sup\{k \in \mathbb{N} \mid a_k \neq 0\}$ avec la convention $\sup \emptyset = -\infty$.

L'anneau des polynômes : opérations

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

$$\sum_{k=0}^{\infty} a_k X^k = \sum_{k=0}^{\infty} b_k X^k \qquad \Longleftrightarrow \qquad a_k = b_k \text{ pour tout } k \in \mathbb{N}.$$

L'anneau des polynômes : opérations

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

$$\sum_{k=0}^{\infty} a_k X^k = \sum_{k=0}^{\infty} b_k X^k \qquad \Longleftrightarrow \qquad a_k = b_k \text{ pour tout } k \in \mathbb{N}.$$

Pour l'implémentation il suffit donc de stocker les coefficients :

L'anneau des polynômes : opérations

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

$$\sum_{k=0}^{\infty} a_k X^k = \sum_{k=0}^{\infty} b_k X^k \qquad \Longleftrightarrow \qquad a_k = b_k \text{ pour tout } k \in \mathbb{N}.$$

Pour l'implémentation il suffit donc de stocker les coefficients :

- Pour un polynôme « dense » on stocke toute la suite initiale $(a_0, a_1, a_2, \ldots, a_n)$ telle que $a_n \neq 0$ et $a_k = 0$ pour $k > n$.

L'anneau des polynômes : opérations

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

$$\sum_{k=0}^{\infty} a_k X^k = \sum_{k=0}^{\infty} b_k X^k \qquad \Longleftrightarrow \qquad a_k = b_k \text{ pour tout } k \in \mathbb{N}.$$

Pour l'implémentation il suffit donc de stocker les coefficients :

- Pour un polynôme « dense » on stocke toute la suite initiale $(a_0, a_1, a_2, \ldots, a_n)$ telle que $a_n \neq 0$ et $a_k = 0$ pour $k > n$.
- Pour un polynôme « creux » on ne stocke que les monômes non nuls.

L'anneau des polynômes : opérations

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

$$\sum_{k=0}^{\infty} a_k X^k = \sum_{k=0}^{\infty} b_k X^k \qquad \Longleftrightarrow \qquad a_k = b_k \text{ pour tout } k \in \mathbb{N}.$$

- Pour l'implémentation il suffit donc de stocker les coefficients :
  - Pour un polynôme « dense » on stocke toute la suite initiale $(a_0, a_1, a_2, \ldots, a_n)$ telle que $a_n \neq 0$ et $a_k = 0$ pour $k > n$.
  - Pour un polynôme « creux » on ne stocke que les monômes non nuls.

L'addition et la multiplication des polynômes sont données par

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

$$\left(\sum_{i=0}^{\infty} a_i X^i\right) \cdot \left(\sum_{j=0}^{\infty} b_j X^j\right) = \sum_{s=0}^{\infty} \left(\sum_{i+j=s} a_i b_j\right) X^s$$

- Ces formules se traduisent immédiatement en algorithmes.

L'anneau des polynômes : opérations

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

$$\sum_{k=0}^{\infty} a_k X^k = \sum_{k=0}^{\infty} b_k X^k \qquad \Longleftrightarrow \qquad a_k = b_k \text{ pour tout } k \in \mathbb{N}.$$

 Pour l'implémentation il suffit donc de stocker les coefficients :

- Pour un polynôme « dense » on stocke toute la suite initiale $(a_0, a_1, a_2, \ldots, a_n)$ telle que $a_n \neq 0$ et $a_k = 0$ pour $k > n$.
- Pour un polynôme « creux » on ne stocke que les monômes non nuls.

L'addition et la multiplication des polynômes sont données par

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

$$\left(\sum_{i=0}^{\infty} a_i X^i\right) \cdot \left(\sum_{j=0}^{\infty} b_j X^j\right) = \sum_{s=0}^{\infty} \left(\sum_{i+j=s} a_i b_j\right) X^s$$

 Ces formules se traduisent immédiatement en algorithmes.
Si l'on sait implémenter $\mathbb{K}$, alors on sait implémenter $\mathbb{K}[X]$.

L'anneau des polynômes : preuve d'existence par construction

Pour la construction on considère les suites dans $\mathbb{K}$ à support fini,

$$\mathbb{K}^{(\mathbb{N})} := \left\{ (a_k)_{k\in\mathbb{N}} \;\middle|\; \begin{array}{c} \text{On a } a_k \in \mathbb{K} \text{ pour tout } k \in \mathbb{N} \text{ et il existe} \\ n \in \mathbb{N} \text{ tel que } a_k = 0 \text{ pour tout } k > n. \end{array} \right\}$$

L'anneau des polynômes : preuve d'existence par construction

Pour la construction on considère les suites dans $\mathbb{K}$ à support fini,

$$\mathbb{K}^{(\mathbb{N})} := \left\{ (a_k)_{k\in\mathbb{N}} \;\middle|\; \begin{array}{c} \text{On a } a_k \in \mathbb{K} \text{ pour tout } k \in \mathbb{N} \text{ et il existe} \\ n \in \mathbb{N} \text{ tel que } a_k = 0 \text{ pour tout } k > n. \end{array} \right\}$$

Sur $\mathbb{K}^{(\mathbb{N})}$ on définit une addition et une multiplication par

$$\big(a_k\big)_{k\in\mathbb{N}} + \big(b_k\big)_{k\in\mathbb{N}} := \big(a_k + b_k\big)_{k\in\mathbb{N}} \qquad \text{et}$$

$$\big(a_i\big)_{i\in\mathbb{N}} \cdot \big(b_j\big)_{j\in\mathbb{N}} := \Big(\sum_{i+j=s} a_i b_j\Big)_{s\in\mathbb{N}}.$$

L'anneau des polynômes : preuve d'existence par construction

Pour la construction on considère les suites dans $\mathbb{K}$ à support fini,

$$\mathbb{K}^{(\mathbb{N})} := \left\{ (a_k)_{k\in\mathbb{N}} \;\middle|\; \begin{array}{c} \text{On a } a_k \in \mathbb{K} \text{ pour tout } k \in \mathbb{N} \text{ et il existe} \\ n \in \mathbb{N} \text{ tel que } a_k = 0 \text{ pour tout } k > n. \end{array} \right\}$$

Sur $\mathbb{K}^{(\mathbb{N})}$ on définit une addition et une multiplication par

$$\big(a_k\big)_{k\in\mathbb{N}} + \big(b_k\big)_{k\in\mathbb{N}} := \big(a_k + b_k\big)_{k\in\mathbb{N}} \qquad \text{et}$$

$$\big(a_i\big)_{i\in\mathbb{N}} \cdot \big(b_j\big)_{j\in\mathbb{N}} := \Big(\sum_{i+j=s} a_i b_j\Big)_{s\in\mathbb{N}}.$$

Lemme (exercice long mais bénéfique)

$(\mathbb{K}^{(\mathbb{N})}, +, \cdot)$ *est un anneau commutatif.*

L'anneau des polynômes : preuve d'existence par construction

Pour la construction on considère les suites dans $\mathbb{K}$ à support fini,

$$\mathbb{K}^{(\mathbb{N})} := \left\{ (a_k)_{k\in\mathbb{N}} \;\middle|\; \begin{array}{c} \text{On a } a_k \in \mathbb{K} \text{ pour tout } k \in \mathbb{N} \text{ et il existe} \\ n \in \mathbb{N} \text{ tel que } a_k = 0 \text{ pour tout } k > n. \end{array} \right\}$$

Sur $\mathbb{K}^{(\mathbb{N})}$ on définit une addition et une multiplication par

$$\big(a_k\big)_{k\in\mathbb{N}} + \big(b_k\big)_{k\in\mathbb{N}} := \big(a_k + b_k\big)_{k\in\mathbb{N}} \qquad \text{et}$$

$$\big(a_i\big)_{i\in\mathbb{N}} \cdot \big(b_j\big)_{j\in\mathbb{N}} := \Big(\sum_{i+j=s} a_i b_j\Big)_{s\in\mathbb{N}}.$$

Lemme (exercice long mais bénéfique)

$(\mathbb{K}^{(\mathbb{N})}, +, \cdot)$ *est un anneau commutatif.*

On identifie tout élément $a \in \mathbb{K}$ avec $(a, 0, 0, 0, \dots) \in \mathbb{K}^{(\mathbb{N})}$.

L'anneau des polynômes : preuve d'existence par construction

Pour la construction on considère les suites dans $\mathbb{K}$ à support fini,

$$\mathbb{K}^{(\mathbb{N})} := \left\{ (a_k)_{k\in\mathbb{N}} \;\middle|\; \begin{array}{c} \text{On a } a_k \in \mathbb{K} \text{ pour tout } k \in \mathbb{N} \text{ et il existe} \\ n \in \mathbb{N} \text{ tel que } a_k = 0 \text{ pour tout } k > n. \end{array} \right\}$$

Sur $\mathbb{K}^{(\mathbb{N})}$ on définit une addition et une multiplication par

$$\big(a_k\big)_{k\in\mathbb{N}} + \big(b_k\big)_{k\in\mathbb{N}} := \big(a_k + b_k\big)_{k\in\mathbb{N}} \qquad \text{et}$$

$$\big(a_i\big)_{i\in\mathbb{N}} \cdot \big(b_j\big)_{j\in\mathbb{N}} := \Big(\sum_{i+j=s} a_i b_j\Big)_{s\in\mathbb{N}}.$$

Lemme (exercice long mais bénéfique)

$(\mathbb{K}^{(\mathbb{N})}, +, \cdot)$ *est un anneau commutatif.*

On identifie tout élément $a \in \mathbb{K}$ avec $(a, 0, 0, 0, \dots) \in \mathbb{K}^{(\mathbb{N})}$.
Ainsi l'anneau $\mathbb{K}$ devient un sous-anneau de l'anneau $\mathbb{K}^{(\mathbb{N})}$.

L'anneau des polynômes : preuve d'existence par construction

Pour la construction on considère les suites dans $\mathbb{K}$ à support fini,

$$\mathbb{K}^{(\mathbb{N})} := \left\{ (a_k)_{k\in\mathbb{N}} \;\middle|\; \begin{array}{c} \text{On a } a_k \in \mathbb{K} \text{ pour tout } k \in \mathbb{N} \text{ et il existe} \\ n \in \mathbb{N} \text{ tel que } a_k = 0 \text{ pour tout } k > n. \end{array} \right\}$$

Sur $\mathbb{K}^{(\mathbb{N})}$ on définit une addition et une multiplication par

$$\big(a_k\big)_{k\in\mathbb{N}} + \big(b_k\big)_{k\in\mathbb{N}} := \big(a_k + b_k\big)_{k\in\mathbb{N}} \qquad \text{et}$$

$$\big(a_i\big)_{i\in\mathbb{N}} \cdot \big(b_j\big)_{j\in\mathbb{N}} := \Big(\sum_{i+j=s} a_i b_j\Big)_{s\in\mathbb{N}}.$$

Lemme (exercice long mais bénéfique)

$(\mathbb{K}^{(\mathbb{N})}, +, \cdot)$ *est un anneau commutatif.*

On identifie tout élément $a \in \mathbb{K}$ avec $(a, 0, 0, 0, \dots) \in \mathbb{K}^{(\mathbb{N})}$.
Ainsi l'anneau $\mathbb{K}$ devient un sous-anneau de l'anneau $\mathbb{K}^{(\mathbb{N})}$.

On pose $X := (0, 1, 0, 0, \dots)$, ce qui entraîne $X^2 = (0, 0, 1, 0, \dots)$, etc.

L'anneau des polynômes : preuve d'existence par construction

Pour la construction on considère les suites dans $\mathbb{K}$ à support fini,

$$\mathbb{K}^{(\mathbb{N})} := \left\{ (a_k)_{k\in\mathbb{N}} \;\middle|\; \begin{array}{c} \text{On a } a_k \in \mathbb{K} \text{ pour tout } k \in \mathbb{N} \text{ et il existe} \\ n \in \mathbb{N} \text{ tel que } a_k = 0 \text{ pour tout } k > n. \end{array} \right\}$$

Sur $\mathbb{K}^{(\mathbb{N})}$ on définit une addition et une multiplication par

$$\big(a_k\big)_{k\in\mathbb{N}} + \big(b_k\big)_{k\in\mathbb{N}} := \big(a_k + b_k\big)_{k\in\mathbb{N}} \qquad \text{et}$$

$$\big(a_i\big)_{i\in\mathbb{N}} \cdot \big(b_j\big)_{j\in\mathbb{N}} := \Big(\sum_{i+j=s} a_i b_j\Big)_{s\in\mathbb{N}}.$$

Lemme (exercice long mais bénéfique)

$(\mathbb{K}^{(\mathbb{N})}, +, \cdot)$ *est un anneau commutatif.*

On identifie tout élément $a \in \mathbb{K}$ avec $(a, 0, 0, 0, \dots) \in \mathbb{K}^{(\mathbb{N})}$.
Ainsi l'anneau $\mathbb{K}$ devient un sous-anneau de l'anneau $\mathbb{K}^{(\mathbb{N})}$.

On pose $X := (0, 1, 0, 0, \dots)$, ce qui entraîne $X^2 = (0, 0, 1, 0, \dots)$, etc.

Tout $P \in \mathbb{K}^{(\mathbb{N})}$ non nul est de la forme $P = (a_0, a_1, \dots, a_n, 0, \dots)$ où $a_0, a_1, \dots, a_n \in \mathbb{K}$ et $a_n \neq 0$:

L'anneau des polynômes : preuve d'existence par construction

Pour la construction on considère les suites dans $\mathbb{K}$ à support fini,

$$\mathbb{K}^{(\mathbb{N})} := \left\{ (a_k)_{k\in\mathbb{N}} \;\middle|\; \begin{array}{c} \text{On a } a_k \in \mathbb{K} \text{ pour tout } k \in \mathbb{N} \text{ et il existe} \\ n \in \mathbb{N} \text{ tel que } a_k = 0 \text{ pour tout } k > n. \end{array} \right\}$$

Sur $\mathbb{K}^{(\mathbb{N})}$ on définit une addition et une multiplication par

$$\big(a_k\big)_{k\in\mathbb{N}} + \big(b_k\big)_{k\in\mathbb{N}} := \big(a_k + b_k\big)_{k\in\mathbb{N}} \qquad \text{et}$$

$$\big(a_i\big)_{i\in\mathbb{N}} \cdot \big(b_j\big)_{j\in\mathbb{N}} := \Big(\sum_{i+j=s} a_i b_j\Big)_{s\in\mathbb{N}}.$$

Lemme (exercice long mais bénéfique)

$(\mathbb{K}^{(\mathbb{N})}, +, \cdot)$ *est un anneau commutatif.*

On identifie tout élément $a \in \mathbb{K}$ avec $(a, 0, 0, 0, \dots) \in \mathbb{K}^{(\mathbb{N})}$.
Ainsi l'anneau $\mathbb{K}$ devient un sous-anneau de l'anneau $\mathbb{K}^{(\mathbb{N})}$.

On pose $X := (0, 1, 0, 0, \dots)$, ce qui entraîne $X^2 = (0, 0, 1, 0, \dots)$, etc.

Tout $P \in \mathbb{K}^{(\mathbb{N})}$ non nul est de la forme $P = (a_0, a_1, \dots, a_n, 0, \dots)$ où $a_0, a_1, \dots, a_n \in \mathbb{K}$ et $a_n \neq 0$: il s'écrit donc de manière unique comme

$$P = a_0 + a_1 X^1 + \cdots + a_n X^n.$$

L'anneau des polynômes : preuve d'existence par construction

Pour la construction on considère les suites dans $\mathbb{K}$ à support fini,

$$\mathbb{K}^{(\mathbb{N})} := \left\{ (a_k)_{k\in\mathbb{N}} \;\middle|\; \begin{array}{c} \text{On a } a_k \in \mathbb{K} \text{ pour tout } k \in \mathbb{N} \text{ et il existe} \\ n \in \mathbb{N} \text{ tel que } a_k = 0 \text{ pour tout } k > n. \end{array} \right\}$$

Sur $\mathbb{K}^{(\mathbb{N})}$ on définit une addition et une multiplication par

$$\big(a_k\big)_{k\in\mathbb{N}} + \big(b_k\big)_{k\in\mathbb{N}} := \big(a_k + b_k\big)_{k\in\mathbb{N}} \qquad \text{et}$$

$$\big(a_i\big)_{i\in\mathbb{N}} \cdot \big(b_j\big)_{j\in\mathbb{N}} := \Big(\sum_{i+j=s} a_i b_j\Big)_{s\in\mathbb{N}}.$$

Lemme (exercice long mais bénéfique)

$(\mathbb{K}^{(\mathbb{N})}, +, \cdot)$ *est un anneau commutatif.*

On identifie tout élément $a \in \mathbb{K}$ avec $(a, 0, 0, 0, \dots) \in \mathbb{K}^{(\mathbb{N})}$.
Ainsi l'anneau $\mathbb{K}$ devient un sous-anneau de l'anneau $\mathbb{K}^{(\mathbb{N})}$.

On pose $X := (0, 1, 0, 0, \dots)$, ce qui entraîne $X^2 = (0, 0, 1, 0, \dots)$, etc.

Tout $P \in \mathbb{K}^{(\mathbb{N})}$ non nul est de la forme $P = (a_0, a_1, \dots, a_n, 0, \dots)$ où $a_0, a_1, \dots, a_n \in \mathbb{K}$ et $a_n \neq 0$: il s'écrit donc de manière unique comme

$$P = a_0 + a_1 X^1 + \cdots + a_n X^n.$$

Ceci prouve que $\mathbb{K}^{(\mathbb{N})}$ est l'anneau des polynômes sur $\mathbb{K}$ en la variable X.

Algorithme 9.1 addition de deux polynômes

Entrée: les coefficients de $A = \sum_{k=0}^{n} a_k X^k$ et $B = \sum_{k=0}^{n} b_k X^k$ sur $\mathbb{K}$.

Sortie: les coefficients de la somme $C = A + B$ sous la forme $C = \sum_{k=0}^{n} c_k X^k$

pour k **de** 0 **à** n **faire** $c_k \leftarrow a_k + b_k$ **fin pour**
retourner $(c_0, \ldots, c_n)$

Algorithme 9.3 addition de deux polynômes

Entrée: les coefficients de $A = \sum_{k=0}^{n} a_k X^k$ et $B = \sum_{k=0}^{n} b_k X^k$ sur $\mathbb{K}$.

Sortie: les coefficients de la somme $C = A + B$ sous la forme $C = \sum_{k=0}^{n} c_k X^k$

pour k **de** 0 **à** n **faire** $c_k \leftarrow a_k + b_k$ **fin pour**
retourner $(c_0, \ldots, c_n)$

Algorithme 9.4 multiplication de deux polynômes

Entrée: les coefficients de $A = \sum_{i=0}^{m} a_i X^i$ et $B = \sum_{j=0}^{n} b_j X^j$ sur $\mathbb{K}$.

Sortie: les coefficients du produit $C = A \cdot B$ sous la forme $C = \sum_{k=0}^{m+n} c_k X^k$

pour k **de** 0 **à** $m+n$ **faire** $c_k \leftarrow 0$ **fin pour**
pour i **de** 0 **à** m **faire**
  pour j **de** 0 **à** n **faire**
    $c_{i+j} \leftarrow c_{i+j} + a_i b_j$
  fin pour
fin pour
retourner $(c_0, \ldots, c_{m+n})$

Algorithme 9.5 addition de deux polynômes

Entrée: les coefficients de $A = \sum_{k=0}^{n} a_k X^k$ et $B = \sum_{k=0}^{n} b_k X^k$ sur $\mathbb{K}$.

Sortie: les coefficients de la somme $C = A + B$ sous la forme $C = \sum_{k=0}^{n} c_k X^k$

pour k **de** 0 **à** n **faire** $c_k \leftarrow a_k + b_k$ **fin pour**
retourner $(c_0, \ldots, c_n)$

Algorithme 9.6 multiplication de deux polynômes

Entrée: les coefficients de $A = \sum_{i=0}^{m} a_i X^i$ et $B = \sum_{j=0}^{n} b_j X^j$ sur $\mathbb{K}$.

Sortie: les coefficients du produit $C = A \cdot B$ sous la forme $C = \sum_{k=0}^{m+n} c_k X^k$

pour k **de** 0 **à** $m+n$ **faire** $c_k \leftarrow 0$ **fin pour**
pour i **de** 0 **à** m **faire**
  pour j **de** 0 **à** n **faire**
    $c_{i+j} \leftarrow c_{i+j} + a_i b_j$
  fin pour
fin pour
retourner $(c_0, \ldots, c_{m+n})$

Cette méthode de multiplication est de complexité quadratique : elle effectue $(m+1)(n+1)$ additions et multiplications dans $\mathbb{K}$.

La propriété universelle de l'anneau des polynômes

Proposition

Soit $\varphi : \mathbb{K} \to \mathbb{L}$ un morphisme d'anneaux.

La propriété universelle de l'anneau des polynômes

Proposition

Soit $\varphi : \mathbb{K} \to \mathbb{L}$ un morphisme d'anneaux. Soit $\mathbb{K}[X]$ l'anneau des polynômes.

La propriété universelle de l'anneau des polynômes

Proposition

Soit $\varphi : \mathbb{K} \to \mathbb{L}$ un morphisme d'anneaux. Soit $\mathbb{K}[X]$ l'anneau des polynômes. Pour tout $x \in \mathbb{L}$ il existe un unique morphisme d'anneaux $\tilde{\varphi} : \mathbb{K}[X] \to \mathbb{L}$ tel que $\tilde{\varphi}|_{\mathbb{K}} = \varphi$ et $\tilde{\varphi}(X) = x$.

La propriété universelle de l'anneau des polynômes

Proposition

Soit $\varphi\colon \mathbb{K} \to \mathbb{L}$ un morphisme d'anneaux. Soit $\mathbb{K}[X]$ l'anneau des polynômes. Pour tout $x \in \mathbb{L}$ il existe un unique morphisme d'anneaux $\tilde{\varphi}\colon \mathbb{K}[X] \to \mathbb{L}$ tel que $\tilde{\varphi}|_{\mathbb{K}} = \varphi$ et $\tilde{\varphi}(X) = x$. Explicitement, ce morphisme est donné par

$$\tilde{\varphi}(a_0 + a_1 X^1 + \cdots + a_n X^n) = \varphi(a_0) + \varphi(a_1) x^1 + \cdots + \varphi(a_n) x^n.$$

La propriété universelle de l'anneau des polynômes

Proposition

Soit $\varphi\colon \mathbb{K} \to \mathbb{L}$ un morphisme d'anneaux. Soit $\mathbb{K}[X]$ l'anneau des polynômes. Pour tout $x \in \mathbb{L}$ il existe un unique morphisme d'anneaux $\tilde{\varphi}\colon \mathbb{K}[X] \to \mathbb{L}$ tel que $\tilde{\varphi}|_{\mathbb{K}} = \varphi$ et $\tilde{\varphi}(X) = x$. Explicitement, ce morphisme est donné par

$$\tilde{\varphi}(a_0 + a_1 X^1 + \cdots + a_n X^n) = \varphi(a_0) + \varphi(a_1) x^1 + \cdots + \varphi(a_n) x^n.$$

Notation

Si $\mathbb{K} = \mathbb{L}$ et $\varphi\colon \mathbb{K} \to \mathbb{L}$ est l'identité,

La propriété universelle de l'anneau des polynômes

Proposition

Soit $\varphi\colon \mathbb{K} \to \mathbb{L}$ un morphisme d'anneaux. Soit $\mathbb{K}[X]$ l'anneau des polynômes. Pour tout $x \in \mathbb{L}$ il existe un unique morphisme d'anneaux $\tilde{\varphi}\colon \mathbb{K}[X] \to \mathbb{L}$ tel que $\tilde{\varphi}|_{\mathbb{K}} = \varphi$ et $\tilde{\varphi}(X) = x$. Explicitement, ce morphisme est donné par

$$\tilde{\varphi}(a_0 + a_1 X^1 + \cdots + a_n X^n) = \varphi(a_0) + \varphi(a_1) x^1 + \cdots + \varphi(a_n) x^n.$$

Notation

Si $\mathbb{K} = \mathbb{L}$ et $\varphi\colon \mathbb{K} \to \mathbb{L}$ est l'identité, ou si $\mathbb{K} \subset \mathbb{L}$ et $\varphi\colon \mathbb{K} \hookrightarrow \mathbb{L}$ est l'inclusion,

La propriété universelle de l'anneau des polynômes

Proposition

Soit $\varphi\colon \mathbb{K} \to \mathbb{L}$ un morphisme d'anneaux. Soit $\mathbb{K}[X]$ l'anneau des polynômes. Pour tout $x \in \mathbb{L}$ il existe un unique morphisme d'anneaux $\tilde{\varphi}\colon \mathbb{K}[X] \to \mathbb{L}$ tel que $\tilde{\varphi}|_{\mathbb{K}} = \varphi$ et $\tilde{\varphi}(X) = x$. Explicitement, ce morphisme est donné par

$$\tilde{\varphi}(a_0 + a_1 X^1 + \cdots + a_n X^n) = \varphi(a_0) + \varphi(a_1) x^1 + \cdots + \varphi(a_n) x^n.$$

Notation

Si $\mathbb{K} = \mathbb{L}$ et $\varphi\colon \mathbb{K} \to \mathbb{L}$ est l'identité, ou si $\mathbb{K} \subset \mathbb{L}$ et $\varphi\colon \mathbb{K} \hookrightarrow \mathbb{L}$ est l'inclusion, alors on écrit simplement $P(x)$ pour $\tilde{\varphi}(P)$:

La propriété universelle de l'anneau des polynômes

Proposition

Soit $\varphi\colon \mathbb{K} \to \mathbb{L}$ un morphisme d'anneaux. Soit $\mathbb{K}[X]$ l'anneau des polynômes. Pour tout $x \in \mathbb{L}$ il existe un unique morphisme d'anneaux $\tilde{\varphi}\colon \mathbb{K}[X] \to \mathbb{L}$ tel que $\tilde{\varphi}|_{\mathbb{K}} = \varphi$ et $\tilde{\varphi}(X) = x$. Explicitement, ce morphisme est donné par

$$\tilde{\varphi}(a_0 + a_1 X^1 + \cdots + a_n X^n) = \varphi(a_0) + \varphi(a_1) x^1 + \cdots + \varphi(a_n) x^n.$$

Notation

Si $\mathbb{K} = \mathbb{L}$ et $\varphi\colon \mathbb{K} \to \mathbb{L}$ est l'identité, ou si $\mathbb{K} \subset \mathbb{L}$ et $\varphi\colon \mathbb{K} \hookrightarrow \mathbb{L}$ est l'inclusion, alors on écrit simplement $P(x)$ pour $\tilde{\varphi}(P)$:

$$P = a_0 + a_1 X^1 + \cdots + a_n X^n \quad \Longrightarrow \quad P(x) = a_0 + a_1 x^1 + \cdots + a_n x^n.$$

La propriété universelle de l'anneau des polynômes

Proposition

Soit $\varphi\colon \mathbb{K} \to \mathbb{L}$ un morphisme d'anneaux. Soit $\mathbb{K}[X]$ l'anneau des polynômes. Pour tout $x \in \mathbb{L}$ il existe un unique morphisme d'anneaux $\tilde{\varphi}\colon \mathbb{K}[X] \to \mathbb{L}$ tel que $\tilde{\varphi}|_{\mathbb{K}} = \varphi$ et $\tilde{\varphi}(X) = x$. Explicitement, ce morphisme est donné par

$$\tilde{\varphi}(a_0 + a_1 X^1 + \cdots + a_n X^n) = \varphi(a_0) + \varphi(a_1) x^1 + \cdots + \varphi(a_n) x^n.$$

Notation

Si $\mathbb{K} = \mathbb{L}$ et $\varphi\colon \mathbb{K} \to \mathbb{L}$ est l'identité, ou si $\mathbb{K} \subset \mathbb{L}$ et $\varphi\colon \mathbb{K} \hookrightarrow \mathbb{L}$ est l'inclusion, alors on écrit simplement $P(x)$ pour $\tilde{\varphi}(P)$:

$$P = a_0 + a_1 X^1 + \cdots + a_n X^n \quad \Longrightarrow \quad P(x) = a_0 + a_1 x^1 + \cdots + a_n x^n.$$

Autrement dit, on substitue la variable X par l'élément x.

Polynômes vs fonctions polynomiales

Corollaire

Tout polynôme $P \in \mathbb{K}[X]$ définit une fonction $f_P : \mathbb{K} \to \mathbb{K}$ par $x \mapsto P(x)$.

Polynômes vs fonctions polynomiales

Corollaire

Tout polynôme $P \in \mathbb{K}[X]$ définit une fonction $f_P : \mathbb{K} \to \mathbb{K}$ par $x \mapsto P(x)$.
Pour $a \in \mathbb{K}$ la fonction $f_a = a$ est constante. Nous avons $f_X = \mathrm{id}_{\mathbb{K}}$ et

$$f_{P+Q} = f_P + f_Q \quad \text{et} \quad f_{P \cdot Q} = f_P \cdot f_Q.$$

Polynômes vs fonctions polynomiales

Corollaire

Tout polynôme $P \in \mathbb{K}[X]$ définit une fonction $f_P : \mathbb{K} \to \mathbb{K}$ par $x \mapsto P(x)$.
Pour $a \in \mathbb{K}$ la fonction $f_a = a$ est constante. Nous avons $f_X = \mathrm{id}_{\mathbb{K}}$ et

$$f_{P+Q} = f_P + f_Q \quad \text{et} \quad f_{P \cdot Q} = f_P \cdot f_Q.$$

Autrement dit, nous avons un morphisme d'anneaux $\mathbb{K}[X] \to \mathbb{K}^{\mathbb{K}}$, $X \mapsto \mathrm{id}_{\mathbb{K}}$.

Polynômes vs fonctions polynomiales

Corollaire

Tout polynôme $P \in \mathbb{K}[X]$ définit une fonction $f_P : \mathbb{K} \to \mathbb{K}$ par $x \mapsto P(x)$.
Pour $a \in \mathbb{K}$ la fonction $f_a = a$ est constante. Nous avons $f_X = \mathrm{id}_{\mathbb{K}}$ et

$$f_{P+Q} = f_P + f_Q \quad \text{et} \quad f_{P \cdot Q} = f_P \cdot f_Q.$$

Autrement dit, nous avons un morphisme d'anneaux $\mathbb{K}[X] \to \mathbb{K}^{\mathbb{K}}$, $X \mapsto \mathrm{id}_{\mathbb{K}}$.

Pour $\mathbb{K} = \mathbb{R}$ nous avons l'habitude d'identifier P et f_P.

Polynômes vs fonctions polynomiales

Corollaire

Tout polynôme $P \in \mathbb{K}[X]$ définit une fonction $f_P : \mathbb{K} \to \mathbb{K}$ par $x \mapsto P(x)$.
Pour $a \in \mathbb{K}$ la fonction $f_a = a$ est constante. Nous avons $f_X = \mathrm{id}_{\mathbb{K}}$ et

$$f_{P+Q} = f_P + f_Q \quad \text{et} \quad f_{P \cdot Q} = f_P \cdot f_Q.$$

Autrement dit, nous avons un morphisme d'anneaux $\mathbb{K}[X] \to \mathbb{K}^{\mathbb{K}}$, $X \mapsto \mathrm{id}_{\mathbb{K}}$.

Pour $\mathbb{K} = \mathbb{R}$ nous avons l'habitude d'identifier P et f_P.
On verra plus bas que c'est possible si l'anneau $\mathbb{K}$ est intègre et infini.

Polynômes vs fonctions polynomiales

Corollaire

Tout polynôme $P \in \mathbb{K}[X]$ définit une fonction $f_P : \mathbb{K} \to \mathbb{K}$ par $x \mapsto P(x)$.
Pour $a \in \mathbb{K}$ la fonction $f_a = a$ est constante. Nous avons $f_X = \mathrm{id}_{\mathbb{K}}$ et

$$f_{P+Q} = f_P + f_Q \quad \textit{et} \quad f_{P \cdot Q} = f_P \cdot f_Q.$$

Autrement dit, nous avons un morphisme d'anneaux $\mathbb{K}[X] \to \mathbb{K}^{\mathbb{K}}$, $X \mapsto \mathrm{id}_{\mathbb{K}}$.

Pour $\mathbb{K} = \mathbb{R}$ nous avons l'habitude d'identifier P et f_P.
On verra plus bas que c'est possible si l'anneau $\mathbb{K}$ est intègre et infini.
En général ce n'est pas possible car $f_P = f_Q$ ne garantit pas que $P = Q$.

Polynômes vs fonctions polynomiales

Corollaire

Tout polynôme $P \in \mathbb{K}[X]$ définit une fonction $f_P : \mathbb{K} \to \mathbb{K}$ par $x \mapsto P(x)$.
Pour $a \in \mathbb{K}$ la fonction $f_a = a$ est constante. Nous avons $f_X = \mathrm{id}_{\mathbb{K}}$ et

$$f_{P+Q} = f_P + f_Q \quad \text{et} \quad f_{P \cdot Q} = f_P \cdot f_Q.$$

Autrement dit, nous avons un morphisme d'anneaux $\mathbb{K}[X] \to \mathbb{K}^{\mathbb{K}}$, $X \mapsto \mathrm{id}_{\mathbb{K}}$.

Pour $\mathbb{K} = \mathbb{R}$ nous avons l'habitude d'identifier P et f_P.
On verra plus bas que c'est possible si l'anneau $\mathbb{K}$ est intègre et infini.
En général ce n'est pas possible car $f_P = f_Q$ ne garantit pas que $P = Q$.

Exemple

Soit $\mathbb{K} = \mathbb{Z}/p$ ou $p \in \mathbb{N}$ est premier.

Polynômes vs fonctions polynomiales

Corollaire

Tout polynôme $P \in \mathbb{K}[X]$ définit une fonction $f_P : \mathbb{K} \to \mathbb{K}$ par $x \mapsto P(x)$.
Pour $a \in \mathbb{K}$ la fonction $f_a = a$ est constante. Nous avons $f_X = \mathrm{id}_{\mathbb{K}}$ et

$$f_{P+Q} = f_P + f_Q \quad \text{et} \quad f_{P \cdot Q} = f_P \cdot f_Q.$$

Autrement dit, nous avons un morphisme d'anneaux $\mathbb{K}[X] \to \mathbb{K}^{\mathbb{K}}$, $X \mapsto \mathrm{id}_{\mathbb{K}}$.

Pour $\mathbb{K} = \mathbb{R}$ nous avons l'habitude d'identifier P et f_P.
On verra plus bas que c'est possible si l'anneau $\mathbb{K}$ est intègre et infini.
En général ce n'est pas possible car $f_P = f_Q$ ne garantit pas que $P = Q$.

Exemple

Soit $\mathbb{K} = \mathbb{Z}/p$ ou $p \in \mathbb{N}$ est premier. Considérons $P = X^p - X$ dans $\mathbb{Z}/p[X]$.

Polynômes vs fonctions polynomiales

Corollaire

Tout polynôme $P \in \mathbb{K}[X]$ définit une fonction $f_P : \mathbb{K} \to \mathbb{K}$ par $x \mapsto P(x)$.
Pour $a \in \mathbb{K}$ la fonction $f_a = a$ est constante. Nous avons $f_X = \mathrm{id}_{\mathbb{K}}$ et

$$f_{P+Q} = f_P + f_Q \quad \textit{et} \quad f_{P \cdot Q} = f_P \cdot f_Q.$$

Autrement dit, nous avons un morphisme d'anneaux $\mathbb{K}[X] \to \mathbb{K}^{\mathbb{K}}$, $X \mapsto \mathrm{id}_{\mathbb{K}}$.

Pour $\mathbb{K} = \mathbb{R}$ nous avons l'habitude d'identifier P et f_P.
On verra plus bas que c'est possible si l'anneau $\mathbb{K}$ est intègre et infini.
En général ce n'est pas possible car $f_P = f_Q$ ne garantit pas que $P = Q$.

Exemple

Soit $\mathbb{K} = \mathbb{Z}/p$ ou $p \in \mathbb{N}$ est premier. Considérons $P = X^p - X$ dans $\mathbb{Z}/p[X]$.
Alors $P \neq 0$ mais $f_P = 0$ d'après le petit théorème de Fermat.

Évaluation d'un polynôme d'après Horner

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

Évaluation d'un polynôme d'après Horner

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

Évaluation d'un polynôme d'après Horner

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

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

Évaluation d'un polynôme d'après Horner

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

Méthode naïve : On calcule $a_k x^k = a_k x \cdots x$ 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.

Évaluation d'un polynôme d'après Horner

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

Méthode naïve : On calcule $a_k x^k = a_k x \cdots x$ 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 : On évalue $P(x)$ par l'expression équivalente suivante :

$$P(x) = ((\cdots((a_n x + a_{n-1})x + a_{n-2})\cdots x + a_2)x + a_1)x + a_0.$$

Évaluation d'un polynôme d'après Horner

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

Méthode naïve : On calcule $a_k x^k = a_k x \cdots x$ 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 : On évalue $P(x)$ par l'expression équivalente suivante :

$$P(x) = ((\cdots((a_n x + a_{n-1})x + a_{n-2})\cdots x + a_2)x + a_1)x + a_0.$$

Ceci ne nécessite que n additions et n multiplications !

Évaluation d'un polynôme d'après Horner

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

Méthode naïve : On calcule $a_k x^k = a_k x \cdots x$ 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 : On évalue $P(x)$ par l'expression équivalente suivante :

$$P(x) = ((\cdots((a_n x + a_{n-1})x + a_{n-2})\cdots x + a_2)x + a_1)x + a_0.$$

Ceci ne nécessite que n additions et n multiplications !
Pour $n = 100$ on passe de 5050 à 100 multiplications.

Évaluation d'un polynôme d'après Horner

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

Méthode naïve : On calcule $a_k x^k = a_k x \cdots x$ 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 : On évalue $P(x)$ par l'expression équivalente suivante :

$$P(x) = ((\cdots((a_n x + a_{n-1})x + a_{n-2})\cdots x + a_2)x + a_1)x + a_0.$$

Ceci ne nécessite que n additions et n multiplications !
Pour $n = 100$ on passe de 5050 à 100 multiplications.
Pour $n = 1000$ on passe de 500500 à 1000 multiplications.

Évaluation d'un polynôme d'après Horner

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

Méthode naïve : On calcule $a_k x^k = a_k x \cdots x$ 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 : On évalue $P(x)$ par l'expression équivalente suivante :

$$P(x) = ((\cdots((a_n x + a_{n-1})x + a_{n-2})\cdots x + a_2)x + a_1)x + a_0.$$

Ceci ne nécessite que n additions et n multiplications !
Pour $n = 100$ on passe de 5050 à 100 multiplications.
Pour $n = 1000$ on passe de 500500 à 1000 multiplications.

Algorithme 9.15 évaluation d'un polynôme selon Horner

Entrée: des coefficients $a_0, a_1, a_2, \ldots, a_n \in \mathbb{K}$ et un élément $x \in \mathbb{K}$.
Sortie: la valeur $y = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$.

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

Sommaire

Propriétés du degré

Proposition

Par construction, tout anneau de polynômes $\mathbb{K}[X]$ *sur un anneau* $\mathbb{K}$ *vient avec une fonction* $\deg : \mathbb{K}[X] \to \mathbb{N} \cup \{-\infty\}$.

Propriétés du degré

Proposition

Par construction, tout anneau de polynômes $\mathbb{K}[X]$ *sur un anneau* $\mathbb{K}$ *vient avec une fonction* $\deg\colon \mathbb{K}[X] \to \mathbb{N} \cup \{-\infty\}$*.*

1. $\deg(P+Q) \leq \sup\{\deg P, \deg Q\}$,
   avec égalité ssi $\deg P \neq \deg Q$ *ou* $\operatorname{dom} P + \operatorname{dom} Q \neq 0$*.*

Propriétés du degré

Proposition

Par construction, tout anneau de polynômes $\mathbb{K}[X]$ *sur un anneau* $\mathbb{K}$ *vient avec une fonction* $\deg\colon \mathbb{K}[X] \to \mathbb{N} \cup \{-\infty\}$*.*

1. $\deg(P+Q) \leq \sup\{\deg P, \deg Q\}$,
   avec égalité ssi $\deg P \neq \deg Q$ *ou* $\operatorname{dom} P + \operatorname{dom} Q \neq 0$*.*
2. $\deg(PQ) \leq \deg P + \deg Q$,
   avec égalité ssi $P = 0$ *ou* $Q = 0$ *ou* $\operatorname{dom} P \cdot \operatorname{dom} Q \neq 0$*.*

Propriétés du degré

Proposition

Par construction, tout anneau de polynômes $\mathbb{K}[X]$ *sur un anneau* $\mathbb{K}$ *vient avec une fonction* $\deg\colon \mathbb{K}[X] \to \mathbb{N} \cup \{-\infty\}$*.*

1. $\deg(P+Q) \leq \sup\{\deg P, \deg Q\}$,
   avec égalité ssi $\deg P \neq \deg Q$ *ou* $\operatorname{dom} P + \operatorname{dom} Q \neq 0$*.*
2. $\deg(PQ) \leq \deg P + \deg Q$,
   avec égalité ssi $P = 0$ *ou* $Q = 0$ *ou* $\operatorname{dom} P \cdot \operatorname{dom} Q \neq 0$*.*

Si $\operatorname{dom} P \cdot \operatorname{dom} Q \neq 0$*, alors* $\operatorname{dom}(PQ) = \operatorname{dom} P \cdot \operatorname{dom} Q$*.*

Corollaire

Pour tout anneau $\mathbb{K}$ les conditions suivantes sont équivalentes :

Corollaire

Pour tout anneau $\mathbb{K}$ les conditions suivantes sont équivalentes :

1. *L'anneau $\mathbb{K}$ est intègre.*

Corollaire

Pour tout anneau $\mathbb{K}$ les conditions suivantes sont équivalentes :

1. *L'anneau $\mathbb{K}$ est intègre.*
2. *On a $\deg(PQ) = \deg P + \deg Q$ pour tout $P, Q \in \mathbb{K}[X]$.*

Corollaire

Pour tout anneau $\mathbb{K}$ les conditions suivantes sont équivalentes :

1. *L'anneau $\mathbb{K}$ est intègre.*
2. *On a $\deg(PQ) = \deg P + \deg Q$ pour tout $P, Q \in \mathbb{K}[X]$.*
3. *L'anneau des polynômes $\mathbb{K}[X]$ sur $\mathbb{K}$ est intègre.*

Corollaire

Pour tout anneau $\mathbb{K}$ les conditions suivantes sont équivalentes :

1. *L'anneau $\mathbb{K}$ est intègre.*
2. *On a $\deg(PQ) = \deg P + \deg Q$ pour tout $P, Q \in \mathbb{K}[X]$.*
3. *L'anneau des polynômes $\mathbb{K}[X]$ sur $\mathbb{K}$ est intègre.*

Exemple (Avertissement dans le cas d'un anneau non intègre)

Dans $\mathbb{Z}/6[X]$ on considère $P = \bar{1} + \bar{2}X$ et $Q = \bar{1} + \bar{3}X$.

Corollaire

Pour tout anneau $\mathbb{K}$ les conditions suivantes sont équivalentes :

1. *L'anneau $\mathbb{K}$ est intègre.*
2. *On a $\deg(PQ) = \deg P + \deg Q$ pour tout $P, Q \in \mathbb{K}[X]$.*
3. *L'anneau des polynômes $\mathbb{K}[X]$ sur $\mathbb{K}$ est intègre.*

Exemple (Avertissement dans le cas d'un anneau non intègre)

Dans $\mathbb{Z}/6[X]$ on considère $P = \bar{1} + \bar{2}X$ et $Q = \bar{1} + \bar{3}X$.
On a $\deg P + \deg Q = 2$, mais pour le produit on trouve $\deg(P \cdot Q) = 1$ car

$$P \cdot Q = (\bar{1} + \bar{2}X) \cdot (\bar{1} + \bar{3}X) = \bar{1} + \bar{5}X + \bar{6}X^2 = \bar{1} + \bar{5}X$$

Éléments inversibles

Corollaire

Pour tout anneau intègre $\mathbb{K}$ nous avons $\mathbb{K}[X]^\times = \mathbb{K}^\times$.

Éléments inversibles

Corollaire

Pour tout anneau intègre $\mathbb{K}$ *nous avons* $\mathbb{K}[X]^\times = \mathbb{K}^\times$.

Exemple (Avertissement dans le cas d'un anneau non intègre)

Dans $\mathbb{Z}/4[X]$ on considère $P = \bar{1} + \bar{2}X$ de degré 1.

Éléments inversibles

Corollaire

Pour tout anneau intègre $\mathbb{K}$ *nous avons* $\mathbb{K}[X]^\times = \mathbb{K}^\times$.

Exemple (Avertissement dans le cas d'un anneau non intègre)

Dans $\mathbb{Z}/4[X]$ on considère $P = \bar{1} + \bar{2}X$ de degré 1. On trouve

$$P \cdot P = (\bar{1} + \bar{2}X) \cdot (\bar{1} + \bar{2}X) = \bar{1} + \bar{4}X + \bar{4}X^2 = \bar{1}.$$

Éléments inversibles

Corollaire

Pour tout anneau intègre $\mathbb{K}$ *nous avons* $\mathbb{K}[X]^\times = \mathbb{K}^\times$.

Exemple (Avertissement dans le cas d'un anneau non intègre)

Dans $\mathbb{Z}/4[X]$ on considère $P = \bar{1} + \bar{2}X$ de degré 1. On trouve

$$P \cdot P = (\bar{1} + \bar{2}X) \cdot (\bar{1} + \bar{2}X) = \bar{1} + \bar{4}X + \bar{4}X^2 = \bar{1}.$$

Exercice : expliciter le groupe $\mathbb{Z}/4[X]^\times$ des éléments inversibles dans $\mathbb{Z}/4[X]$.

Division euclidienne de polynômes

Proposition (Division euclidienne de polynômes)

Soit $P \in \mathbb{K}[X]$ un polynôme à coefficient dominant inversible, $\mathrm{dom}\, P \in \mathbb{K}^\times$.

Division euclidienne de polynômes

Proposition (Division euclidienne de polynômes)

Soit $P \in \mathbb{K}[X]$ un polynôme à coefficient dominant inversible, $\operatorname{dom} P \in \mathbb{K}^\times$. Alors pour tout $S \in \mathbb{K}[X]$ il existe une unique paire $Q, R \in \mathbb{K}[X]$ telle que

$$S = PQ + R \quad \textit{et} \quad \deg R < \deg P.$$

Division euclidienne de polynômes

Proposition (Division euclidienne de polynômes)

Soit $P \in \mathbb{K}[X]$ un polynôme à coefficient dominant inversible, $\operatorname{dom} P \in \mathbb{K}^\times$.
Alors pour tout $S \in \mathbb{K}[X]$ il existe une unique paire $Q, R \in \mathbb{K}[X]$ telle que

$$S = PQ + R \quad \textit{et} \quad \deg R < \deg P.$$

Dans cette situation 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.

Division euclidienne de polynômes

Proposition (Division euclidienne de polynômes)

Soit $P \in \mathbb{K}[X]$ un polynôme à coefficient dominant inversible, $\operatorname{dom} P \in \mathbb{K}^\times$.
Alors pour tout $S \in \mathbb{K}[X]$ il existe une unique paire $Q, R \in \mathbb{K}[X]$ telle que

$$S = PQ + R \quad \textit{et} \quad \deg R < \deg P.$$

Dans cette situation 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 9.16 division euclidienne de deux polynômes

Entrée: deux polynômes $S, P \in \mathbb{K}[X]$ tel que $\operatorname{dom} P \in \mathbb{K}^\times$.

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

$Q \leftarrow 0\,; \quad R \leftarrow S$
tant que $\deg R \geq \deg P$ **faire**
  $M \leftarrow \operatorname{dom}(P)^{-1} \operatorname{dom}(R) \cdot X^{\deg R - \deg P}$
  $Q \leftarrow Q + M\,; \quad R \leftarrow R - PM$
fin tant que
retourner (Q, R)

La division euclidienne : algorithme

Algorithme 9.17 division euclidienne de deux polynômes

Entrée: deux polynômes $S, P \in \mathbb{K}[X]$ tel que $\operatorname{dom} P \in \mathbb{K}^\times$.

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

$Q \leftarrow 0\,; \quad R \leftarrow S$
tant que $\deg R \geq \deg P$ **faire**
  $M \leftarrow \operatorname{dom}(P)^{-1} \operatorname{dom}(R) \cdot X^{\deg R - \deg P}$
  $Q \leftarrow Q + M\,; \quad R \leftarrow R - PM$
fin tant que
retourner (Q, R)

Proposition

L'algorithme 9.16 ci-dessus est correct.

Application aux anneaux quotients

Corollaire

Soit $P \in \mathbb{K}[X]$ *un polynôme tel que* $\operatorname{dom} P \in \mathbb{K}^\times$.

Application aux anneaux quotients

Corollaire

Soit $P \in \mathbb{K}[X]$ *un polynôme tel que* $\operatorname{dom} P \in \mathbb{K}^\times$*. Alors l'anneau quotient* $\mathbb{K}[X]/(P)$ *admet une description pratique :*

Application aux anneaux quotients

Corollaire

Soit $P \in \mathbb{K}[X]$ *un polynôme tel que* $\operatorname{dom} P \in \mathbb{K}^\times$*. Alors l'anneau quotient* $\mathbb{K}[X]/(P)$ *admet une description pratique : pour toute classe* $x \in \mathbb{K}[X]/(P)$ *il existe un unique représentant* $R \in \mathbb{K}[X]$ *tel que* $\deg R < \deg P$*.*

Application aux anneaux quotients

Corollaire

Soit $P \in \mathbb{K}[X]$ un polynôme tel que $\operatorname{dom} P \in \mathbb{K}^\times$. Alors l'anneau quotient $\mathbb{K}[X]/(P)$ admet une description pratique : pour toute classe $x \in \mathbb{K}[X]/(P)$ il existe un unique représentant $R \in \mathbb{K}[X]$ tel que $\deg R < \deg P$.

Remarque

Soulignons l'analogie entre $\mathbb{Z}/m$ et $\mathbb{K}[X]/(P)$: dans les deux cas on peut choisir un représentant *préféré* pour chaque classe du quotient.

Application aux anneaux quotients

Corollaire

Soit $P \in \mathbb{K}[X]$ *un polynôme tel que* $\operatorname{dom} P \in \mathbb{K}^\times$*. Alors l'anneau quotient* $\mathbb{K}[X]/(P)$ *admet une description pratique : pour toute classe* $x \in \mathbb{K}[X]/(P)$ *il existe un unique représentant* $R \in \mathbb{K}[X]$ *tel que* $\deg R < \deg P$*.*

Remarque

Soulignons l'analogie entre $\mathbb{Z}/m$ et $\mathbb{K}[X]/(P)$: dans les deux cas on peut choisir un représentant *préféré* pour chaque classe du quotient.

$$\mathbb{Z}/m = \{\bar{r} \mid r \in \mathbb{N}, r < m\} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$$
$$\mathbb{K}[X]/(P) = \{\bar{R} \mid R \in \mathbb{K}[X], \deg R < \deg P\}$$

Application aux anneaux quotients

Corollaire

Soit $P \in \mathbb{K}[X]$ un polynôme tel que $\operatorname{dom} P \in \mathbb{K}^\times$. Alors l'anneau quotient $\mathbb{K}[X]/(P)$ admet une description pratique : pour toute classe $x \in \mathbb{K}[X]/(P)$ il existe un unique représentant $R \in \mathbb{K}[X]$ tel que $\deg R < \deg P$.

Remarque

Soulignons l'analogie entre $\mathbb{Z}/m$ et $\mathbb{K}[X]/(P)$: dans les deux cas on peut choisir un représentant *préféré* pour chaque classe du quotient.

$$\mathbb{Z}/m = \{\bar{r} \mid r \in \mathbb{N}, r < m\} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$$
$$\mathbb{K}[X]/(P) = \{\bar{R} \mid R \in \mathbb{K}[X], \deg R < \deg P\}$$

Ainsi calculer dans $\mathbb{K}[X]/(P)$ c'est calculer dans $\mathbb{K}[X]$ en ne retenant que le reste modulo P (c'est-à-dire l'unique reste de la division euclidienne par P).

Exercice

Soit $\mathbb{F}_4 := \mathbb{Z}/2[X]/(X^2 + X + 1)$. On pose $x := \bar{X} \in \mathbb{F}_4$.

1. Donner la liste des éléments de $\mathbb{F}_4$.
2. Écrire les tables d'addition et de multiplication pour $\mathbb{F}_4$.
3. Est-ce que $\mathbb{F}_4$ est un corps ?

Exercices

Exercice

Soit $\mathbb{F}_4 := \mathbb{Z}/2[X]/(X^2 + X + 1)$. On pose $x := \bar{X} \in \mathbb{F}_4$.

1. Donner la liste des éléments de $\mathbb{F}_4$.
2. Écrire les tables d'addition et de multiplication pour $\mathbb{F}_4$.
3. Est-ce que $\mathbb{F}_4$ est un corps ?

Exercice

Soit $P \in \mathbb{Z}/m[X]$ un polynôme avec $\deg P = d$ et $\mathrm{dom}\, P = 1$.

1. Déterminer le cardinal de l'anneau quotient $\mathbb{Z}/m[X]/(P)$.
2. Si $\mathbb{Z}/m[X]/(P)$ est un corps, alors nécessairement m est premier et P est irréductible, c'est-à-dire $P = QR$ implique $Q \in \mathbb{Z}/m^\times$ ou $R \in \mathbb{Z}/m^\times$. (On verra plus bas que ces conditions sont aussi suffisantes.)

Sommaire

Racines d'un polynôme

Définition

Soit $\mathbb{K}$ un anneau et soit $P \in \mathbb{K}[X]$ un polynôme sur $\mathbb{K}$.

Racines d'un polynôme

Définition

Soit $\mathbb{K}$ un anneau et soit $P \in \mathbb{K}[X]$ un polynôme sur $\mathbb{K}$.
On appelle $a \in \mathbb{K}$ une *racine* ou un *zéro* de P si $P(a) = 0$.

Racines d'un polynôme

Définition

Soit $\mathbb{K}$ un anneau et soit $P \in \mathbb{K}[X]$ un polynôme sur $\mathbb{K}$.
On appelle $a \in \mathbb{K}$ une *racine* ou un *zéro* de P si $P(a) = 0$.

Proposition

Un élément $a \in \mathbb{K}$ est une racine de $P \in \mathbb{K}[X]$ si et seulement s'il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $P = (X - a)Q$. Dans ce cas Q est unique.

Racines d'un polynôme

Définition

Soit $\mathbb{K}$ un anneau et soit $P \in \mathbb{K}[X]$ un polynôme sur $\mathbb{K}$.
On appelle $a \in \mathbb{K}$ une *racine* ou un *zéro* de P si $P(a) = 0$.

Proposition

Un élément $a \in \mathbb{K}$ est une racine de $P \in \mathbb{K}[X]$ si et seulement s'il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $P = (X - a)Q$. Dans ce cas Q est unique.

Corollaire

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

Racines d'un polynôme

Définition

Soit $\mathbb{K}$ un anneau et soit $P \in \mathbb{K}[X]$ un polynôme sur $\mathbb{K}$.
On appelle $a \in \mathbb{K}$ une *racine* ou un *zéro* de P si $P(a) = 0$.

Proposition

Un élément $a \in \mathbb{K}$ est une racine de $P \in \mathbb{K}[X]$ si et seulement s'il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $P = (X - a)Q$. Dans ce cas Q est unique.

Corollaire

Pour tout $P \in \mathbb{K}[X]^*$ et tout $a \in \mathbb{K}$ il existe un unique entier $m \geq 0$ et un unique polynôme $Q \in \mathbb{K}[X]$ tels que $P = (X - a)^m Q$ et $Q(a) \neq 0$.
Si $m \geq 1$ on dit que a est une racine de multiplicité m.

Racines d'un polynôme

Définition

Soit $\mathbb{K}$ un anneau et soit $P \in \mathbb{K}[X]$ un polynôme sur $\mathbb{K}$.
On appelle $a \in \mathbb{K}$ une *racine* ou un *zéro* de P si $P(a) = 0$.

Proposition

Un élément $a \in \mathbb{K}$ est une racine de $P \in \mathbb{K}[X]$ si et seulement s'il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $P = (X - a)Q$. Dans ce cas Q est unique.

Corollaire

Pour tout $P \in \mathbb{K}[X]^*$ et tout $a \in \mathbb{K}$ il existe un unique entier $m \geq 0$ et un unique polynôme $Q \in \mathbb{K}[X]$ tels que $P = (X - a)^m Q$ et $Q(a) \neq 0$.
Si $m \geq 1$ on dit que a est une racine de multiplicité m.
On dit que a est une racine simple si $m = 1$, et multiple si $m \geq 2$. □

Mise en facteur des racines d'un polynôme

Corollaire

Tout $P \in \mathbb{K}[X]^*$ *s'écrit comme* $P = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k} Q$

Mise en facteur des racines d'un polynôme

Corollaire

Tout $P \in \mathbb{K}[X]^*$ *s'écrit comme* $P = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k} Q$
où $a_1, \ldots, a_k \in \mathbb{K}$ *sont des racines distinctes, de multiplicité* $m_1, \ldots, m_k \geq 1$,

Mise en facteur des racines d'un polynôme

Corollaire

Tout $P \in \mathbb{K}[X]^*$ s'écrit comme $P = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k} Q$
où $a_1, \ldots, a_k \in \mathbb{K}$ sont des racines distinctes, de multiplicité $m_1, \ldots, m_k \geq 1$,
et le polynôme $Q \in \mathbb{K}[X]$ n'a pas de racine dans $\mathbb{K}$.

Mise en facteur des racines d'un polynôme

Corollaire

Tout $P \in \mathbb{K}[X]^*$ s'écrit comme $P = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k} Q$
où $a_1, \ldots, a_k \in \mathbb{K}$ sont des racines distinctes, de multiplicité $m_1, \ldots, m_k \geq 1$,
et le polynôme $Q \in \mathbb{K}[X]$ n'a pas de racine dans $\mathbb{K}$.

Cette factorisation n'est en général pas unique !

Mise en facteur des racines d'un polynôme

Corollaire

Tout $P \in \mathbb{K}[X]^*$ s'écrit comme $P = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k} Q$
où $a_1, \ldots, a_k \in \mathbb{K}$ sont des racines distinctes, de multiplicité $m_1, \ldots, m_k \geq 1$,
et le polynôme $Q \in \mathbb{K}[X]$ n'a pas de racine dans $\mathbb{K}$.


Cette factorisation n'est en général pas unique !
De même, il n'est pas vrai qu'un polynôme de degré n ait au plus n racines :

Mise en facteur des racines d'un polynôme

Corollaire

Tout $P \in \mathbb{K}[X]^*$ s'écrit comme $P = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k} Q$
où $a_1, \ldots, a_k \in \mathbb{K}$ sont des racines distinctes, de multiplicité $m_1, \ldots, m_k \geq 1$,
et le polynôme $Q \in \mathbb{K}[X]$ n'a pas de racine dans $\mathbb{K}$.


Cette factorisation n'est en général pas unique !
De même, il n'est pas vrai qu'un polynôme de degré n ait au plus n racines :

Exemple (Avertissement dans le cas d'un anneau non intègre)

Sur l'anneau $\mathbb{Z}/8$ le polynôme $P = X^2 - \bar{1}$ admet quatre racines distinctes, à savoir $\pm\bar{1}$ et $\pm\bar{3}$.

Mise en facteur des racines d'un polynôme

Corollaire

Tout $P \in \mathbb{K}[X]^*$ s'écrit comme $P = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k} Q$
où $a_1, \ldots, a_k \in \mathbb{K}$ sont des racines distinctes, de multiplicité $m_1, \ldots, m_k \geq 1$,
et le polynôme $Q \in \mathbb{K}[X]$ n'a pas de racine dans $\mathbb{K}$.

 Cette factorisation n'est en général pas unique !
De même, il n'est pas vrai qu'un polynôme de degré n ait au plus n racines :

Exemple (Avertissement dans le cas d'un anneau non intègre)

Sur l'anneau $\mathbb{Z}/8$ le polynôme $P = X^2 - \bar{1}$ admet quatre racines distinctes, à savoir $\pm\bar{1}$ et $\pm\bar{3}$. Effectivement $P = (X - \bar{1})(X + \bar{1}) = (X - \bar{3})(X + \bar{3})$.

Le nombre des racines d'un polynôme

Proposition

Soit $\mathbb{K}$ un anneau commutatif intègre.

Le nombre des racines d'un polynôme

Proposition

Soit $\mathbb{K}$ un anneau commutatif intègre. Alors un polynôme $P \in \mathbb{K}[X]$ de degré n admet au plus n racines dans $\mathbb{K}$ (comptées avec multiplicité).

Remarque

Nous ne regardons ici que des anneaux commutatifs.

Le nombre des racines d'un polynôme

Proposition

Soit $\mathbb{K}$ un anneau commutatif intègre. Alors un polynôme $P \in \mathbb{K}[X]$ de degré n admet au plus n racines dans $\mathbb{K}$ (comptées avec multiplicité).

Remarque

Nous ne regardons ici que des anneaux commutatifs.

Dans l'anneau non commutatif $\mathrm{Mat}(2 \times 2, \mathbb{C})$ le polynôme $X^2 + 1$ admet une infinité de racines :

Le nombre des racines d'un polynôme

Proposition

Soit $\mathbb{K}$ un anneau commutatif intègre. Alors un polynôme $P \in \mathbb{K}[X]$ de degré n admet au plus n racines dans $\mathbb{K}$ (comptées avec multiplicité).

Remarque

Nous ne regardons ici que des anneaux commutatifs.

Dans l'anneau non commutatif $\mathrm{Mat}(2 \times 2, \mathbb{C})$ le polynôme $X^2 + 1$ admet une infinité de racines : pour tout triplet $(x, y, z) \in \mathbb{R}^3$ vérifiant $x^2 + y^2 + z^2 = 1$ on voit que la matrice $M = \left(\begin{smallmatrix} ix & y+iz \\ -y+iz & -ix \end{smallmatrix} \right)$ vérifie $M^2 = -1$.

Le nombre des racines d'un polynôme

Proposition

Soit $\mathbb{K}$ un anneau commutatif intègre. Alors un polynôme $P \in \mathbb{K}[X]$ de degré n admet au plus n racines dans $\mathbb{K}$ (comptées avec multiplicité).

Remarque

Nous ne regardons ici que des anneaux commutatifs.

Dans l'anneau non commutatif $\mathrm{Mat}(2 \times 2, \mathbb{C})$ le polynôme $X^2 + 1$ admet une infinité de racines : pour tout triplet $(x, y, z) \in \mathbb{R}^3$ vérifiant $x^2 + y^2 + z^2 = 1$ on voit que la matrice $M = \left(\begin{smallmatrix} ix & y+iz \\ -y+iz & -ix \end{smallmatrix} \right)$ vérifie $M^2 = -1$.

Il en est de même dans le corps non commutatif des quaternions :

$$\mathbb{H} = \left\{ \left(\begin{smallmatrix} r+ix & -y-iz \\ y-iz & r-ix \end{smallmatrix} \right) \mid r, x, y, z \in \mathbb{R} \right\} \subset \mathrm{Mat}(2 \times 2, \mathbb{C}).$$

Racines multiples et dérivée

Proposition

La dérivation $\partial : \mathbb{K}[X] \to \mathbb{K}[X]$ *est définie par* $\partial(\sum_k a_k X^k) := \sum_k k a_k X^{k-1}$.

Racines multiples et dérivée

Proposition

La dérivation $\partial : \mathbb{K}[X] \to \mathbb{K}[X]$ *est définie par* $\partial(\sum_k a_k X^k) := \sum_k k a_k X^{k-1}$.
Elle 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

La dérivation $\partial : \mathbb{K}[X] \to \mathbb{K}[X]$ *est définie par* $\partial(\sum_k a_k X^k) := \sum_k k a_k X^{k-1}$. *Elle est* $\mathbb{K}$*-linéaire et vérifie la règle de Leibniz :* $\partial(PQ) = (\partial P) \cdot Q + P \cdot (\partial Q)$.

Proposition

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

Racines multiples et dérivée : exemples

Exercice

Considérons $P = X^p - X$ dans $\mathbb{Z}/_p[X]$, p premier. A-t-il de racines multiples ?

Racines multiples et dérivée : exemples

Exercice

Considérons $P = X^p - X$ dans $\mathbb{Z}/_p[X]$, p premier. A-t-il de racines multiples ?

1ère solution On trouve $P' = pX^{p-1} - 1 = -1$ car on travaille sur $\mathbb{Z}/_p$.

Racines multiples et dérivée : exemples

Exercice

Considérons $P = X^p - X$ dans $\mathbb{Z}/_p[X]$, p premier. A-t-il de racines multiples ?

1ère solution On trouve $P' = pX^{p-1} - 1 = -1$ car on travaille sur $\mathbb{Z}/_p$.
Par conséquent il n'existe pas de racines communes de P et P'. ☺

Racines multiples et dérivée : exemples

Exercice

Considérons $P = X^p - X$ dans $\mathbb{Z}/p[X]$, p premier. A-t-il de racines multiples ?

1ère solution On trouve $P' = pX^{p-1} - 1 = -1$ car on travaille sur $\mathbb{Z}/p$.
Par conséquent il n'existe pas de racines communes de P et P'. ☺
2nde solution Par chance, on connaît toutes les racines de P !

Racines multiples et dérivée : exemples

Exercice

Considérons $P = X^p - X$ dans $\mathbb{Z}/p[X]$, p premier. A-t-il de racines multiples ?

1ère solution On trouve $P' = pX^{p-1} - 1 = -1$ car on travaille sur $\mathbb{Z}/p$.
Par conséquent il n'existe pas de racines communes de P et P'. ☺
2nde solution Par chance, on connaît toutes les racines de P !
Tout $a \in \mathbb{Z}/p$ vérifie $a^p = a$ d'après le petit théorème de Fermat.

Racines multiples et dérivée : exemples

Exercice

Considérons $P = X^p - X$ dans $\mathbb{Z}/p[X]$, p premier. A-t-il de racines multiples ?

1ère solution On trouve $P' = pX^{p-1} - 1 = -1$ car on travaille sur $\mathbb{Z}/p$.
Par conséquent il n'existe pas de racines communes de P et P'. ☺
2nde solution Par chance, on connaît toutes les racines de P !
Tout $a \in \mathbb{Z}/p$ vérifie $a^p = a$ d'après le petit théorème de Fermat.
Avec $0, 1, 2, \ldots, p-1$ nous avons donc trouvé p racines distinctes.

Racines multiples et dérivée : exemples

Exercice

Considérons $P = X^p - X$ dans $\mathbb{Z}/p[X]$, p premier. A-t-il de racines multiples ?

1ère solution On trouve $P' = pX^{p-1} - 1 = -1$ car on travaille sur $\mathbb{Z}/p$.
Par conséquent il n'existe pas de racines communes de P et P'. ☺
2nde solution Par chance, on connaît toutes les racines de P !
Tout $a \in \mathbb{Z}/p$ vérifie $a^p = a$ d'après le petit théorème de Fermat.
Avec $0, 1, 2, \ldots, p-1$ nous avons donc trouvé p racines distinctes.
Ainsi $X^P - X = \prod_{a \in \mathbb{Z}/p} (X - a) = X(X-1)(X-2)\cdots(X-p+1)$. ☺

Racines multiples et dérivée : exemples

Exercice

Considérons $P = X^p - X$ dans $\mathbb{Z}/p[X]$, p premier. A-t-il de racines multiples ?

1ère solution On trouve $P' = pX^{p-1} - 1 = -1$ car on travaille sur $\mathbb{Z}/p$.
Par conséquent il n'existe pas de racines communes de P et P'. ☺
2nde solution Par chance, on connaît toutes les racines de P !
Tout $a \in \mathbb{Z}/p$ vérifie $a^p = a$ d'après le petit théorème de Fermat.
Avec $0, 1, 2, \ldots, p-1$ nous avons donc trouvé p racines distinctes.
Ainsi $X^P - X = \prod_{a \in \mathbb{Z}/p} (X - a) = X(X-1)(X-2)\cdots(X-p+1)$. ☺

Exercice

Considérons $P = X^n - 1$ dans $\mathbb{Z}/p[X]$, p premier. A-t-il de racines multiples ?

Racines multiples et dérivée : exemples

Exercice

Considérons $P = X^p - X$ dans $\mathbb{Z}/p[X]$, p premier. A-t-il de racines multiples ?

1ère solution On trouve $P' = pX^{p-1} - 1 = -1$ car on travaille sur $\mathbb{Z}/p$.
Par conséquent il n'existe pas de racines communes de P et P'. ☺
2nde solution Par chance, on connaît toutes les racines de P !
Tout $a \in \mathbb{Z}/p$ vérifie $a^p = a$ d'après le petit théorème de Fermat.
Avec $0, 1, 2, \ldots, p-1$ nous avons donc trouvé p racines distinctes.
Ainsi $X^P - X = \prod_{a \in \mathbb{Z}/p} (X - a) = X(X-1)(X-2)\cdots(X-p+1)$. ☺

Exercice

Considérons $P = X^n - 1$ dans $\mathbb{Z}/p[X]$, p premier. A-t-il de racines multiples ?

Solution. On trouve la dérivée $P' = nX^{n-1}$.

Racines multiples et dérivée : exemples

Exercice

Considérons $P = X^p - X$ dans $\mathbb{Z}/p[X]$, p premier. A-t-il de racines multiples ?

1ère solution On trouve $P' = pX^{p-1} - 1 = -1$ car on travaille sur $\mathbb{Z}/p$.
Par conséquent il n'existe pas de racines communes de P et P'. ☺
2nde solution Par chance, on connaît toutes les racines de P !
Tout $a \in \mathbb{Z}/p$ vérifie $a^p = a$ d'après le petit théorème de Fermat.
Avec $0, 1, 2, \ldots, p-1$ nous avons donc trouvé p racines distinctes.
Ainsi $X^P - X = \prod_{a \in \mathbb{Z}/p} (X - a) = X(X-1)(X-2)\cdots(X-p+1)$. ☺

Exercice

Considérons $P = X^n - 1$ dans $\mathbb{Z}/p[X]$, p premier. A-t-il de racines multiples ?

Solution. On trouve la dérivée $P' = nX^{n-1}$.

Si $p \nmid n$, alors P' s'annule seulement en 0,

Racines multiples et dérivée : exemples

Exercice

Considérons $P = X^p - X$ dans $\mathbb{Z}/p[X]$, p premier. A-t-il de racines multiples ?

1ère solution On trouve $P' = pX^{p-1} - 1 = -1$ car on travaille sur $\mathbb{Z}/p$.
Par conséquent il n'existe pas de racines communes de P et P'. ☺
2nde solution Par chance, on connaît toutes les racines de P !
Tout $a \in \mathbb{Z}/p$ vérifie $a^p = a$ d'après le petit théorème de Fermat.
Avec $0, 1, 2, \ldots, p-1$ nous avons donc trouvé p racines distinctes.
Ainsi $X^P - X = \prod_{a \in \mathbb{Z}/p} (X - a) = X(X-1)(X-2)\cdots(X-p+1)$. ☺

Exercice

Considérons $P = X^n - 1$ dans $\mathbb{Z}/p[X]$, p premier. A-t-il de racines multiples ?

Solution. On trouve la dérivée $P' = nX^{n-1}$.

Si $p \nmid n$, alors P' s'annule seulement en 0,
et il n'existe pas de racines communes de P et P'.

Racines multiples et dérivée : exemples

Exercice

Considérons $P = X^p - X$ dans $\mathbb{Z}/p[X]$, p premier. A-t-il de racines multiples ?

1ère solution On trouve $P' = pX^{p-1} - 1 = -1$ car on travaille sur $\mathbb{Z}/p$.
Par conséquent il n'existe pas de racines communes de P et P'. ☺
2nde solution Par chance, on connaît toutes les racines de P !
Tout $a \in \mathbb{Z}/p$ vérifie $a^p = a$ d'après le petit théorème de Fermat.
Avec $0, 1, 2, \ldots, p-1$ nous avons donc trouvé p racines distinctes.
Ainsi $X^P - X = \prod_{a \in \mathbb{Z}/p} (X - a) = X(X-1)(X-2)\cdots(X-p+1)$. ☺

Exercice

Considérons $P = X^n - 1$ dans $\mathbb{Z}/p[X]$, p premier. A-t-il de racines multiples ?

Solution. On trouve la dérivée $P' = nX^{n-1}$.

Si $p \nmid n$, alors P' s'annule seulement en 0,
et il n'existe pas de racines communes de P et P'.

Si $n = mp$, alors toute racine de P est multiple :

Racines multiples et dérivée : exemples

Exercice

Considérons $P = X^p - X$ dans $\mathbb{Z}/p[X]$, p premier. A-t-il de racines multiples ?

1ère solution On trouve $P' = pX^{p-1} - 1 = -1$ car on travaille sur $\mathbb{Z}/p$.
Par conséquent il n'existe pas de racines communes de P et P'. ☺
2nde solution Par chance, on connaît toutes les racines de P !
Tout $a \in \mathbb{Z}/p$ vérifie $a^p = a$ d'après le petit théorème de Fermat.
Avec $0, 1, 2, \ldots, p-1$ nous avons donc trouvé p racines distinctes.
Ainsi $X^P - X = \prod_{a \in \mathbb{Z}/p} (X - a) = X(X-1)(X-2)\cdots(X-p+1)$. ☺

Exercice

Considérons $P = X^n - 1$ dans $\mathbb{Z}/p[X]$, p premier. A-t-il de racines multiples ?

Solution. On trouve la dérivée $P' = nX^{n-1}$.

Si $p \nmid n$, alors P' s'annule seulement en 0,
et il n'existe pas de racines communes de P et P'.

Si $n = mp$, alors toute racine de P est multiple :
par Frobenius on trouve $X^n - 1 = (X^m - 1)^p$. ☺

Racines multiples et dérivée : exemples

Exercice

Considérons $P = X^p - X$ dans $\mathbb{Z}/p[X]$, p premier. A-t-il de racines multiples ?

1ère solution On trouve $P' = pX^{p-1} - 1 = -1$ car on travaille sur $\mathbb{Z}/p$.
Par conséquent il n'existe pas de racines communes de P et P'. ☺
2nde solution Par chance, on connaît toutes les racines de P !
Tout $a \in \mathbb{Z}/p$ vérifie $a^p = a$ d'après le petit théorème de Fermat.
Avec $0, 1, 2, \ldots, p-1$ nous avons donc trouvé p racines distinctes.
Ainsi $X^P - X = \prod_{a \in \mathbb{Z}/p} (X - a) = X(X-1)(X-2)\cdots(X-p+1)$. ☺

Exercice

Considérons $P = X^n - 1$ dans $\mathbb{Z}/p[X]$, p premier. A-t-il de racines multiples ?

Solution. On trouve la dérivée $P' = nX^{n-1}$.

Si $p \nmid n$, alors P' s'annule seulement en 0,
et il n'existe pas de racines communes de P et P'.

Si $n = mp$, alors toute racine de P est multiple :
par Frobenius on trouve $X^n - 1 = (X^m - 1)^p$. ☺

 En général, sur un corps $\mathbb{K}$, on pourra utiliser l'algorithme d'Euclide dans $\mathbb{K}[X]$ pour trouver les facteurs communs de P et P' en calculant $\mathrm{pgcd}(P, P')$.

Sous-groupes multiplicatifs finis : exemples

Exemple

Dans l'anneau $\mathbb{Z}$ des entiers, le groupe $\mathbb{Z}^\times = \{\pm 1\}$ est d'ordre 2.
Les seuls sous-groupes sont le groupe trivial $\{1\}$ et le groupe $\{\pm 1\}$.

Sous-groupes multiplicatifs finis : exemples

Exemple

Dans l'anneau $\mathbb{Z}$ des entiers, le groupe $\mathbb{Z}^\times = \{\pm 1\}$ est d'ordre 2.
Les seuls sous-groupes sont le groupe trivial $\{1\}$ et le groupe $\{\pm 1\}$.

Exemple

Dans le corps $\mathbb{R}$ des réels, le groupe $\mathbb{R}^\times = \mathbb{R} \smallsetminus \{0\}$ est infini,
mais les sous-groupes finis ne sont que $\{1\}$ et $\{\pm 1\}$, comme avant.
(Tout élément $a \in \mathbb{R}^\times$ vérifiant $|a| \neq 1$ engendre un sous-groupe infini.)

Sous-groupes multiplicatifs finis : exemples

Exemple

Dans l'anneau $\mathbb{Z}$ des entiers, le groupe $\mathbb{Z}^\times = \{\pm 1\}$ est d'ordre 2.
Les seuls sous-groupes sont le groupe trivial $\{1\}$ et le groupe $\{\pm 1\}$.

Exemple

Dans le corps $\mathbb{R}$ des réels, le groupe $\mathbb{R}^\times = \mathbb{R} \smallsetminus \{0\}$ est infini,
mais les sous-groupes finis ne sont que $\{1\}$ et $\{\pm 1\}$, comme avant.
(Tout élément $a \in \mathbb{R}^\times$ vérifiant $|a| \neq 1$ engendre un sous-groupe infini.)

Exemple

Dans $\mathbb{C}^\times$ il existe un sous-groupe fini pour tout ordre $n \in \mathbb{N}_{\geq 1}$, à savoir

$$\left\langle e^{2\pi i/n} \right\rangle = \left\{ e^{2\pi i k/n} \;\middle|\; k = 0, \ldots, n-1 \right\}$$

C'est le seul sous-groupe de $\mathbb{C}^\times$ d'ordre n. (Voir la proposition suivante.)

Sous-groupes multiplicatifs finis : exemples

Exemple

Dans l'anneau $\mathbb{Z}$ des entiers, le groupe $\mathbb{Z}^\times = \{\pm 1\}$ est d'ordre 2.
Les seuls sous-groupes sont le groupe trivial $\{1\}$ et le groupe $\{\pm 1\}$.

Exemple

Dans le corps $\mathbb{R}$ des réels, le groupe $\mathbb{R}^\times = \mathbb{R} \smallsetminus \{0\}$ est infini,
mais les sous-groupes finis ne sont que $\{1\}$ et $\{\pm 1\}$, comme avant.
(Tout élément $a \in \mathbb{R}^\times$ vérifiant $|a| \neq 1$ engendre un sous-groupe infini.)

Exemple

Dans $\mathbb{C}^\times$ il existe un sous-groupe fini pour tout ordre $n \in \mathbb{N}_{\geq 1}$, à savoir

$$\left\langle e^{2\pi i/n} \right\rangle = \left\{ e^{2\pi i k/n} \;\middle|\; k = 0, \ldots, n-1 \right\}$$

C'est le seul sous-groupe de $\mathbb{C}^\times$ d'ordre n. (Voir la proposition suivante.)

Exemple

Soit $\mathbb{K}$ un anneau unitaire et soit G un groupe (commutatif ou non) d'ordre n.
Alors G est isomorphe à un sous-groupe de $\mathrm{Mat}(n \times n, \mathbb{K})^\times = \mathrm{GL}(n, \mathbb{K})$.
Effectivement, on a d'abord $G \hookrightarrow S_n$ puis $S_n \hookrightarrow \mathrm{GL}(n, \mathbb{K})$.

Sous-groupes multiplicatifs finis : exemples

Proposition

Dans un anneau intègre $\mathbb{K}$ il existe au plus un sous-groupe $G \subset \mathbb{K}^\times$ pour tout ordre donné.

Exemple

Cet énoncé ne tient plus si $\mathbb{K}$ n'est pas intègre. Le groupe $\mathbb{Z}/8^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ admet trois sous-groupes d'ordre 2, à savoir $\{\bar{1}, \bar{3}\}$ et $\{\bar{1}, \bar{5}\}$ et $\{\bar{1}, \bar{7}\}$.

Sous-groupes multiplicatifs finis : cyclicité

Théorème

Soit $\mathbb{K}$ un anneau intègre et soit $G \subset \mathbb{K}^\times$ un sous-groupe fini du groupe $\mathbb{K}^\times$.

Sous-groupes multiplicatifs finis : cyclicité

Théorème

Soit $\mathbb{K}$ un anneau intègre et soit $G \subset \mathbb{K}^\times$ un sous-groupe fini du groupe $\mathbb{K}^\times$. Alors G est cyclique, c'est-à-dire qu'il existe $g \in G$ tel que $G = \langle g \rangle$.

Sous-groupes multiplicatifs finis : cyclicité

Théorème

Soit $\mathbb{K}$ un anneau intègre et soit $G \subset \mathbb{K}^\times$ un sous-groupe fini du groupe $\mathbb{K}^\times$. Alors G est cyclique, c'est-à-dire qu'il existe $g \in G$ tel que $G = \langle g \rangle$.

Exemples

Comme $\mathbb{Z}/7$ est un corps, le groupe $\mathbb{Z}/7^\times$ est cyclique d'ordre 6.

Sous-groupes multiplicatifs finis : cyclicité

Théorème

Soit $\mathbb{K}$ un anneau intègre et soit $G \subset \mathbb{K}^\times$ un sous-groupe fini du groupe $\mathbb{K}^\times$. Alors G est cyclique, c'est-à-dire qu'il existe $g \in G$ tel que $G = \langle g \rangle$.

Exemples

Comme $\mathbb{Z}/7$ est un corps, le groupe $\mathbb{Z}/7^\times$ est cyclique d'ordre 6. Le théorème ne garantit que l'existence d'un générateur, sans en expliciter aucun.

Sous-groupes multiplicatifs finis : cyclicité

Théorème

Soit $\mathbb{K}$ un anneau intègre et soit $G \subset \mathbb{K}^\times$ un sous-groupe fini du groupe $\mathbb{K}^\times$. Alors G est cyclique, c'est-à-dire qu'il existe $g \in G$ tel que $G = \langle g \rangle$.

Exemples

Comme $\mathbb{Z}/7$ est un corps, le groupe $\mathbb{Z}/7^\times$ est cyclique d'ordre 6. Le théorème ne garantit que l'existence d'un générateur, sans en expliciter aucun.
Par tâtonnement on trouve $\mathrm{ord}(\bar{2}) = 3$ puis $\mathrm{ord}(\bar{3}) = 6$, donc $\mathbb{Z}/7^\times = \langle \bar{3} \rangle$.

Sous-groupes multiplicatifs finis : cyclicité

Théorème

Soit $\mathbb{K}$ un anneau intègre et soit $G \subset \mathbb{K}^\times$ un sous-groupe fini du groupe $\mathbb{K}^\times$. Alors G est cyclique, c'est-à-dire qu'il existe $g \in G$ tel que $G = \langle g \rangle$.

Exemples

Comme $\mathbb{Z}/7$ est un corps, le groupe $\mathbb{Z}/7^\times$ est cyclique d'ordre 6. Le théorème ne garantit que l'existence d'un générateur, sans en expliciter aucun.
Par tâtonnement on trouve $\mathrm{ord}(\bar{2}) = 3$ puis $\mathrm{ord}(\bar{3}) = 6$, donc $\mathbb{Z}/7^\times = \langle \bar{3} \rangle$.

L'anneau $\mathbb{Z}/8$ n'est pas intègre, et le groupe $\mathbb{Z}/8^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ n'est pas cyclique :

Sous-groupes multiplicatifs finis : cyclicité

Théorème

Soit $\mathbb{K}$ un anneau intègre et soit $G \subset \mathbb{K}^\times$ un sous-groupe fini du groupe $\mathbb{K}^\times$. Alors G est cyclique, c'est-à-dire qu'il existe $g \in G$ tel que $G = \langle g \rangle$.

Exemples

Comme $\mathbb{Z}/7$ est un corps, le groupe $\mathbb{Z}/7^\times$ est cyclique d'ordre 6. Le théorème ne garantit que l'existence d'un générateur, sans en expliciter aucun.
Par tâtonnement on trouve $\mathrm{ord}(\bar{2}) = 3$ puis $\mathrm{ord}(\bar{3}) = 6$, donc $\mathbb{Z}/7^\times = \langle \bar{3} \rangle$.

L'anneau $\mathbb{Z}/8$ n'est pas intègre, et le groupe $\mathbb{Z}/8^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ n'est pas cyclique : $\bar{1}$ est d'ordre 1, alors que $\bar{3}$, $\bar{5}$, $\bar{7}$ sont tous d'ordre 2.

Racines primitives

Corollaire

Si tout corps fini $\mathbb{K}$ le groupe multiplicatif $\mathbb{K}^\times$ est cyclique.

Racines primitives

Corollaire

Si tout corps fini $\mathbb{K}$ le groupe multiplicatif $\mathbb{K}^\times$ est cyclique.
Tout générateur du groupe $\mathbb{K}^\times$ est appelé racine primitive de $\mathbb{K}$. □

Corollaire

Si tout corps fini $\mathbb{K}$ le groupe multiplicatif $\mathbb{K}^\times$ est cyclique.
Tout générateur du groupe $\mathbb{K}^\times$ est appelé racine primitive de $\mathbb{K}$. □

Algorithme 9.20 Trouver une racine primitive g d'un corps fini $\mathbb{K}$

Entrée: un corps $\mathbb{K}$ et la factorisation de $n = |\mathbb{K}^\times|$, $n = p_1^{e_1} \cdots p_k^{e_k}$.

Sortie: un générateur g du groupe cyclique $\mathbb{K}^\times$.

$g \leftarrow 1$
pour i **de** 1 **à** k **faire**
  $m \leftarrow n/p_i$
  répéter
    choisir $x \in \mathbb{K}^\times$ de manière aléatoire // voir l'exercice suivant
  jusqu'à $x^m \neq 1$ // avec la puissance rapide !
  $g \leftarrow g x^{n/p_i^{e_i}}$ // avec la puissance rapide !
fin pour
retourner g

Racines primitives

Corollaire

Si tout corps fini $\mathbb{K}$ le groupe multiplicatif $\mathbb{K}^\times$ est cyclique.
Tout générateur du groupe $\mathbb{K}^\times$ est appelé racine primitive de $\mathbb{K}$. □

Algorithme 9.21 Trouver une racine primitive g d'un corps fini $\mathbb{K}$

Entrée: un corps $\mathbb{K}$ et la factorisation de $n = |\mathbb{K}^\times|$, $n = p_1^{e_1} \cdots p_k^{e_k}$.

Sortie: un générateur g du groupe cyclique $\mathbb{K}^\times$.

$g \leftarrow 1$
pour i **de** 1 **à** k **faire**
  $m \leftarrow n/p_i$
  répéter
    choisir $x \in \mathbb{K}^\times$ de manière aléatoire // voir l'exercice suivant
  jusqu'à $x^m \neq 1$ // avec la puissance rapide !
  $g \leftarrow gx^{n/p_i^{e_i}}$ // avec la puissance rapide !
fin pour
retourner g

Exercice

Vérifier la validité de cet algorithme. Justifier qu'un choix aléatoire de x tombera avec probabilité $1 - \frac{1}{p_i}$ sur un élément vérifiant $x^m \neq 1$.

Exercices

Exercice

Considérer quelques corps de petit cardinal (disons < 20) et expliciter leur racines primitives. Combien y en a-t-il ? Comment en trouver une ? toutes ?

Exercices

Exercice

Considérer quelques corps de petit cardinal (disons < 20) et expliciter leur racines primitives. Combien y en a-t-il ? Comment en trouver une ? toutes ?

Exercice

1. Pour $p = 2^8 + 1 = 257$ quel est l'ordre du groupe $\mathbb{Z}/_p^\times$?
2. Comment déterminer efficacement l'ordre d'un élément $x \in \mathbb{Z}/_{257}^\times$?
   Déterminer ainsi l'ordre de $\bar{2}$ puis de $\bar{3}$ dans $\mathbb{Z}/_{257}^\times$.
   (Justifiez votre réponse en détaillant les calculs effectués.)
3. Définir ce qui est une racine primitive de $\mathbb{Z}/_p^\times$ où p est premier.
4. Expliciter une racine primitive x de $\mathbb{Z}/_{257}^\times$. Combien y en a-t-il ?
   Comment expliciter toutes les racines primitives de $\mathbb{Z}/_{257}^\times$ à partir de x ?

Exercices

Exercice

Considérer quelques corps de petit cardinal (disons < 20) et expliciter leur racines primitives. Combien y en a-t-il ? Comment en trouver une ? toutes ?

Exercice

1. Pour $p = 2^8 + 1 = 257$ quel est l'ordre du groupe $\mathbb{Z}/_p^\times$?
2. Comment déterminer efficacement l'ordre d'un élément $x \in \mathbb{Z}/_{257}^\times$? Déterminer ainsi l'ordre de $\bar{2}$ puis de $\bar{3}$ dans $\mathbb{Z}/_{257}^\times$. (Justifiez votre réponse en détaillant les calculs effectués.)
3. Définir ce qui est une racine primitive de $\mathbb{Z}/_p^\times$ où p est premier.
4. Expliciter une racine primitive x de $\mathbb{Z}/_{257}^\times$. Combien y en a-t-il ? Comment expliciter toutes les racines primitives de $\mathbb{Z}/_{257}^\times$ à partir de x ?

Exercice

Soit $m = 2^k + 1$ un entier avec $k \in \mathbb{N}$, $k \geq 1$. Supposons qu'un élément $x \in \mathbb{Z}/_m$ vérifie $x^{2^k} = 1$ et $x^{2^{k-1}} \neq 1$. Peut-on en déduire que m est premier ?

Exercices

Exercice

Évaluer $P = 1 + 8X + 28X^2 + 56X^3 + 70X^4 + 56X^5 + 28X^6 + 8X^7 + X^8$ en un point $x \in \mathbb{K}$ avec un nombre minimal d'opérations dans $\mathbb{K}$.

Exercice

Soit $\mathbb{K}$ un anneau intègre de cardinal infini. Alors l'application $\mathbb{K}[X] \to \mathbb{K}^{\mathbb{K}}$ donnée par $P \mapsto f_P$ est un morphisme d'anneaux injectif.

Si $\mathbb{K}$ est intègre de cardinal $q \in \mathbb{N}$, alors $\mathbb{K}[X]_{<q} \to \mathbb{K}^{\mathbb{K}}$ est injectif.
Dans ce cas $\mathbb{K}$ est un corps et $P = X^q - X$ est envoyé sur $f_P = 0$.

Et si $\mathbb{K}$ est de caractéristique 0, intègre ou non ?

Exercices

Exercice

Évaluer $P = 1 + 8X + 28X^2 + 56X^3 + 70X^4 + 56X^5 + 28X^6 + 8X^7 + X^8$ en un point $x \in \mathbb{K}$ avec un nombre minimal d'opérations dans $\mathbb{K}$.

Exercice

Soit $\mathbb{K}$ un anneau intègre de cardinal infini. Alors l'application $\mathbb{K}[X] \to \mathbb{K}^{\mathbb{K}}$ donnée par $P \mapsto f_P$ est un morphisme d'anneaux injectif.

Si $\mathbb{K}$ est intègre de cardinal $q \in \mathbb{N}$, alors $\mathbb{K}[X]_{<q} \to \mathbb{K}^{\mathbb{K}}$ est injectif.
Dans ce cas $\mathbb{K}$ est un corps et $P = X^q - X$ est envoyé sur $f_P = 0$.

Et si $\mathbb{K}$ est de caractéristique 0, intègre ou non ?

Exercice

$P \in \mathbb{Z}[X]$ n'admet pas de racines dans $\mathbb{Z}$ si $P(0)$ et $P(1)$ sont impairs.

Exercices

Exercice

Évaluer $P = 1 + 8X + 28X^2 + 56X^3 + 70X^4 + 56X^5 + 28X^6 + 8X^7 + X^8$ en un point $x \in \mathbb{K}$ avec un nombre minimal d'opérations dans $\mathbb{K}$.

Exercice

Soit $\mathbb{K}$ un anneau intègre de cardinal infini. Alors l'application $\mathbb{K}[X] \to \mathbb{K}^{\mathbb{K}}$ donnée par $P \mapsto f_P$ est un morphisme d'anneaux injectif.

Si $\mathbb{K}$ est intègre de cardinal $q \in \mathbb{N}$, alors $\mathbb{K}[X]_{<q} \to \mathbb{K}^{\mathbb{K}}$ est injectif.
Dans ce cas $\mathbb{K}$ est un corps et $P = X^q - X$ est envoyé sur $f_P = 0$.

Et si $\mathbb{K}$ est de caractéristique 0, intègre ou non ?

Exercice

$P \in \mathbb{Z}[X]$ n'admet pas de racines dans $\mathbb{Z}$ si $P(0)$ et $P(1)$ sont impairs.

Exercice

Soit $p \geq 2$. Dans $\mathbb{Z}[X]$ montrer que le reste de la division euclidienne de $M = X^{p^m} - X$ par $N = X^{p^n} - X$ est $R = X^{p^r} - X$ où $r = m \operatorname{rem} n$.
(Indication : calculer modulo $X^{p^n} - X$, ce qui veut dire que $X^{p^n} \equiv X$.)

En déduire par récurrence que $\operatorname{pgcd}(M, N) = X^{p^d} - X$ où $d = \operatorname{pgcd}(m, n)$.
En particulier, $X^{p^m} - X$ divise $X^{p^n} - X$ si et seulement si m divise n.