

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

1/32

Sommaire

- 1 L'anneau des polynômes
 - Définition et construction de l'anneau des polynômes
 - Algorithmes pour l'addition et la multiplication
 - Propriété universelle et fonctions polynomiales
- 2 La division euclidienne
 - Propriétés du degré
 - La division euclidienne de polynômes
 - Application aux anneaux quotients
- 3 Racines
 - Racines d'un polynôme
 - Racines multiples et dérivée
 - Sous-groupes multiplicatifs finis d'un anneau intègre

3/32 11.1

Objectifs de ce chapitre

Les polynômes sont un outil omniprésent en algèbre et dans ses nombreuses applications comme la cryptologie.

Développement mathématique :

- Division euclidienne $S = PQ + R$ telle que $\deg R < \deg P$.
- Sur un anneau intègre un polynôme de degré n a au plus n racines.
- Sous-groupes multiplicatifs finis $G \subset \mathbb{K}^*$ d'un anneau intègre \mathbb{K} .

Développement algorithmique :

- Arithmétique des polynômes, notamment la division euclidienne.
- Application aux anneaux quotients : représentants et algorithmes.
- Recherche d'une racine primitive de \mathbb{K}^* dans un corps fini.

2/32

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

$$P = a_0 + a_1X + \dots + a_nX^n \quad \text{où } n \in \mathbb{N}, a_0, a_1, \dots, a_n \in \mathbb{K}, a_n \neq 0.$$

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** $\text{dom } P := a_n$.

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

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 $\sup \emptyset = -\infty$.

4/32

L'anneau des polynômes : opérations

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

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

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

- Pour un polynôme « dense » on stocke toute la suite initiale $(a_0, a_1, a_2, \dots, a_n)$ 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 $\mathbb{K}[X]$.

§1.1

§1.1

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

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

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

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

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

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

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

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

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

§1.2

L'anneau des polynômes : vérification des axiomes

Pour prouver que $(\mathbb{K}^{(\mathbb{N})}, +, \cdot)$ est un anneau il faut vérifier les axiomes.

L'associativité de $(\mathbb{K}^{(\mathbb{N})}, +)$ découle de celle de $(\mathbb{K}, +)$:

$$[(a_k)_k + (b_k)_k] + (c_k)_k = (a_k + b_k)_k + (c_k)_k = [(a_k + b_k) + c_k]_k$$

$$= [a_k + (b_k + c_k)]_k = (a_k)_k + (b_k + c_k)_k = (a_k)_k + [(b_k)_k + (c_k)_k]$$

La commutativité de $(\mathbb{K}^{(\mathbb{N})}, +)$ découle de celle de $(\mathbb{K}, +)$:

$$(a_k)_k + (b_k)_k = (a_k + b_k)_k = (b_k + a_k)_k = (b_k)_k + (a_k)_k$$

L'élément neutre de $(\mathbb{K}^{(\mathbb{N})}, +)$ est le polynôme nul :

$$(0)_k + (a_k)_k = (0 + a_k)_k = (a_k)_k.$$

Dans $(\mathbb{K}^{(\mathbb{N})}, +)$ l'élément opposé de $(a_k)_k$ est $(-a_k)_k$:

$$(a_k)_k + (-a_k)_k = (a_k + (-a_k))_k = (0)_k.$$

§1.1

§1.1

L'anneau des polynômes : vérification des axiomes

L'associativité de $(\mathbb{K}^{(\mathbb{N})}, \cdot)$ repose sur celle de (\mathbb{K}, \cdot) :

$$[(a_i)_i \cdot (b_j)_j] \cdot (c_k)_k = \left(\sum_{i+j=s} a_i b_j \right)_s \cdot (c_k)_k = \left(\sum_{i+j+k=t} (a_i b_j) c_k \right)_t$$

$$= \left(\sum_{i+j+k=t} a_i (b_j c_k) \right)_t = (a_i)_i \cdot \left(\sum_{j+k=s} b_j c_k \right)_s = (a_i)_i \cdot [(b_j)_j \cdot (c_k)_k]$$

La commutativité de $(\mathbb{K}^{(\mathbb{N})}, \cdot)$ repose sur celle de (\mathbb{K}, \cdot) :

$$(a_i)_i \cdot (b_j)_j = \left(\sum_{i+j=s} a_i b_j \right)_s = \left(\sum_{j+i=s} b_j a_i \right)_s = (b_j)_j \cdot (a_i)_i$$

L'élément neutre est $(1, 0, 0, \dots) = (\delta_i)_i$ où $\delta_0 = 1$ et $\delta_i = 0$ pour $i > 0$:

$$(\delta_i)_i \cdot (a_j)_j = \left(\sum_{i+j=s} \delta_i a_j \right)_s = (a_s)_s$$

La distributivité de $(\mathbb{K}^{(\mathbb{N})}, +, \cdot)$ repose sur celle de $(\mathbb{K}, +, \cdot)$:

$$(a_i)_i \cdot [(b_j)_j + (c_j)_j] = (a_i)_i \cdot (b_j + c_j)_j = \left(\sum_{i+j=s} a_i (b_j + c_j) \right)_s$$

$$= \left(\sum_{i+j=s} a_i b_j + a_i c_j \right)_s = \left(\sum_{i+j=s} a_i b_j \right)_s + \left(\sum_{i+j=s} a_i c_j \right)_s = (a_i)_i \cdot (b_j)_j + (a_i)_i \cdot (c_j)_j$$

§1.2

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, \dots, c_n)

Algorithme 9.2 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, \dots, c_{m+n})

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

L'arithmétique des polynômes et des entiers naturels sont très similaires. L'analogie est la plus frappante quand on travaille en base p :

- Tout entier naturel $A \in \mathbb{N}^*$ s'écrit de manière unique comme $A = a_0 + a_1 p + a_2 p^2 + \dots + a_n p^n$ ou $0 \leq a_k < p, a_n \neq 0$.
- Tout polynôme $A \in \mathbb{Z}_p[X]^*$ s'écrit de manière unique comme $A = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n$ ou $a_k \in \mathbb{Z}_p, a_n \neq 0$.

L'addition et la multiplication dans $\mathbb{Z}_p[X]$ sont très similaires à celles dans \mathbb{N} . Une seule différence est cruciale : dans le cas des entiers la propagation des retenues fait que le calcul au rang k peut avoir un effet au rang $k+1$.

Pour les polynômes il n'y pas de retenue : ainsi l'arithmétique des polynômes est **plus simple** que l'arithmétique des entiers !

On verra plus tard d'autres similarités :

- Les anneaux \mathbb{Z} et $\mathbb{Z}_p[X]$ sont tous les deux euclidiens.
- Ils ont la même asymptotique des éléments premiers.

Proposition

Soit $\varphi: \mathbb{K} \rightarrow \mathbb{L}$ un morphisme d'anneaux. Soit $\mathbb{K}[X]$ l'anneau des polynômes. Pour tout $x \in \mathbb{L}$, il existe une unique morphisme d'anneaux $\tilde{\varphi}: \mathbb{K}[X] \rightarrow \mathbb{L}$ tel que $\tilde{\varphi}|_{\mathbb{K}} = \varphi$ et $\tilde{\varphi}(X) = x$. Explicitement, ce morphisme est donné par $\tilde{\varphi}(a_0 + a_1 X^1 + \dots + a_n X^n) = \varphi(a_0) + \varphi(a_1)x^1 + \dots + \varphi(a_n)x^n$.

Démonstration. Unicité. — Tout morphisme d'anneaux $\tilde{\varphi}: \mathbb{K}[X] \rightarrow \mathbb{L}$ vérifiant $\tilde{\varphi}|_{\mathbb{K}} = \varphi$ et $\tilde{\varphi}(X) = x$ est de la forme explicitée dans l'énoncé.

Existence. — La formule définit une application $\tilde{\varphi}: \mathbb{K}[X] \rightarrow \mathbb{L}$. Exercice : vérifier qu'il s'agit d'un morphisme d'anneaux. (Où utilise-t-on les propriétés de l'anneau des polynômes $\mathbb{K}[X]$?) □

Notation

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

$$P = a_0 + a_1 X^1 + \dots + a_n X^n \implies P(x) = a_0 + a_1 x^1 + \dots + a_n x^n.$$

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

Corollaire

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

⚠ 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.

Remarque (Exercice)

Pour tout anneau \mathbb{K} et tout ensemble Ω , l'ensemble \mathbb{K}^{Ω} des fonctions $f: \Omega \rightarrow \mathbb{K}$ est un anneau pour l'addition et la multiplication « point par point » : $(f+g)(x) = f(x) + g(x)$ et $(f \cdot g)(x) = f(x) \cdot g(x)$ pour tout $x \in \Omega$. En particulier ceci explique l'anneau $\mathbb{K}^{\mathbb{K}}$ des fonctions $\mathbb{K} \rightarrow \mathbb{K}$ ci-dessus.

Évaluation d'un polynôme d'après Horner

Soit $P = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$ un polynôme sur \mathbb{K} .
Comment calculer efficacement l'évaluation $P(x)$ pour $x \in \mathbb{K}$?

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

Méthode de Horner : On évalue $P(x)$ par l'expression équivalente suivante :

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

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 9.3 évaluation d'un polynôme selon Horner

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

Sortie : la valeur $y = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$.

```

y ← a_n
pour k de n - 1 à 0 faire y ← y · x + a_k fin pour
retourner y
```

§1.3

15.32 §2.1

Anneaux intègres

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.

Démonstration. (1) \Rightarrow (2) : Clair pour $P = 0$ ou $Q = 0$. Si $P, Q \in \mathbb{K}[X]^*$, alors $\text{dom } P \neq \emptyset$ et $\text{dom } Q \neq \emptyset$, donc $\text{dom } P \cdot \text{dom } Q \neq \emptyset$ grâce à (1). D'après la proposition on conclut que $\deg(PQ) = \deg P + \deg Q$.

(2) \Rightarrow (3) : Si $P \neq 0$ et $Q \neq 0$, alors $\deg P \geq 0$ et $\deg Q \geq 0$, et grâce à (2) on obtient $\deg(PQ) = \deg P + \deg Q \geq 0$. En particulier $PQ \neq 0$.

(3) \Rightarrow (1) : Dans un anneau intègre tout sous-anneau est intègre. \square

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

Dans $\mathbb{Z}_6[X]$ on considère $P = \bar{1} + 2X$ et $Q = \bar{1} + 3X$.
On a $\deg P + \deg Q = 2$, mais pour le produit on trouve $\deg(P \cdot Q) = 1$ car

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

§2.1

15.32 §2.1

Propriétés du degré

Proposition

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

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

Si $\text{dom } P \cdot \text{dom } Q \neq \emptyset$, alors $\text{dom}(PQ) = \text{dom } P \cdot \text{dom } Q$.

Démonstration. L'assertion (1) est claire.

L'assertion (2) est triviale si $P = 0$ ou $Q = 0$, suivant la convention $(-\infty) + \deg Q = -\infty$ et $\deg P + (-\infty) = -\infty$ dans ces deux cas.

Si $P \neq 0$ et $Q \neq 0$, il suffit d'expliquer le produit : Supposons que

$$P = a_0 + a_1X^1 + \dots + a_nX^n \quad \text{où } a_n \neq 0, \\ Q = b_0 + b_1X^1 + \dots + b_mX^m \quad \text{où } b_m \neq 0.$$

Alors

$$PQ = a_0b_0 + (a_0b_1 + a_1b_0)X^1 + \dots + (a_n b_m)X^{m+n}.$$

Si $a_n b_m \neq 0$, alors $\deg(PQ) = n + m$ et $\text{dom}(PQ) = \text{dom } P \cdot \text{dom } Q$. \square

§1.32

Éléments inversibles

Corollaire

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

Démonstration. Évidemment on a toujours $\mathbb{K}^\times \subset \mathbb{K}[X]^\times$.

Montrons $\mathbb{K}[X]^\times = \mathbb{K}^\times$ si \mathbb{K} est intègre : Si $P \in \mathbb{K}[X]^\times$, alors il existe $Q \in \mathbb{K}[X]$ tel que $PQ = 1$. On a donc $0 = \deg(PQ) = \deg P + \deg Q$. Ceci implique $\deg P = \deg Q = 0$, donc $P, Q \in \mathbb{K}$ et ainsi $P, Q \in \mathbb{K}^\times$. \square

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

Dans $\mathbb{Z}_4[X]$ on considère $P = \bar{1} + 2X$ de degré 1. On trouve

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

Exercice : expliciter le groupe $\mathbb{Z}_4[X]^\times$ des éléments inversibles dans $\mathbb{Z}_4[X]$.

§1.32

Division euclidienne de polynômes

Proposition (Division euclidienne de polynômes)

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

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

Dans cette situation on appelle S quo P : Q le **quotient** et $S \text{ rem } P := R$ le **reste** de la division euclidienne de S par P .

Démonstration. Unicité. — Si $PQ + R = P'Q' + R'$ et $\deg R, \deg R' < \deg P$, alors $P(Q - Q') = R' - R$. Puisque $\text{dom } P \in \mathbb{K}^\times$, nous avons

$$\deg P + \deg(Q - Q') = \deg[P(Q - Q')] = \deg(R - R') < \deg P.$$

Ceci n'est possible que pour $\deg(Q - Q') < 0$, c'est-à-dire $Q - Q' = 0$. On conclut que $Q = Q'$ puis $R = R'$.

Existence. — Si $\deg S < \deg P$ alors $Q = 0$ et $R = S$ conviennent.

Pour $\deg S \geq \deg P$ on procède par récurrence sur $n = \deg S$.

On suppose le résultat vrai pour tout polynôme \tilde{S} avec $\deg \tilde{S} < n$.

On pose $M = \text{dom}(P)^{-1} \text{dom}(S) \cdot X^{\deg S - \deg P}$ et $\tilde{S} = S - PM$.

On voit que $\deg(PM) = \deg S$ et $\text{dom}(PM) = \text{dom } S$, donc $\deg \tilde{S} < \deg S$.

Par hypothèse il existe $\tilde{Q}, R \in \mathbb{K}[X]$ tels que $\tilde{S} = \tilde{P}\tilde{Q} + R$ et $\deg R < \deg P$.

Ainsi $S = \tilde{S} + PM = \tilde{P}\tilde{Q} + R + PM$ en posant $Q = \tilde{Q} + M$. \square

12.2

17/32

Application aux anneaux quotients

Corollaire

Soit $P \in \mathbb{K}[X]$ un polynôme tel que $\text{dom } P \in \mathbb{K}^\times$. 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 $\deg R < \deg P$.

Démonstration. Existence. — On sait que $x = \text{cl}(S)$ pour un $S \in \mathbb{K}[X]$.

Il existe $Q, R \in \mathbb{K}[X]$ tels que $S = PQ + R$ et $\deg R < \deg P$.

On obtient ainsi $x = \text{cl}(S) = \text{cl}(PQ + R) = \text{cl}(R)$ comme souhaité.

Unicité. — Supposons que $x = \text{cl}(R) = \text{cl}(R')$ où $\deg R, \deg R' < \deg P$.

On a alors $R - R' = PQ$ avec $Q \in \mathbb{K}[X]$. Ainsi

$$\deg P > \deg(R - R') = \deg(PQ) = \deg P + \deg Q.$$

On conclut que $Q = 0$, donc $R = R'$, comme énoncé. \square

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.

$$\mathbb{Z}_m = \{\bar{r} \mid r \in \mathbb{N}, r < m\} = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$$

$$\mathbb{K}[X]/(P) = \{\bar{R} \mid R \in \mathbb{K}[X], \deg R < \deg P\}$$

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).

12.3

19/32

La division euclidienne : algorithme

Algorithme 9.4 division euclidienne de deux polynômes

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

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

$Q \leftarrow 0; R \leftarrow S$

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

$M \leftarrow \text{dom}(P)^{-1} \text{dom}(R) \cdot X^{\deg R - \deg P}$

$Q \leftarrow Q + M; R \leftarrow R - PM$

fin tant que

retourner (Q, R)

Proposition

L'algorithme 9.4 ci-dessus est correct.

Démonstration. Terminaison. — Le monôme M est choisi tel que R et PM aient le même degré et coefficient dominant. Ainsi $\deg(R - PM) < \deg R$. L'algorithme se termine après au plus $1 + \deg S - \deg P$ itérations.

Validité. — L'initialisation $Q \leftarrow 0, R \leftarrow S$ assure que $S = PQ + R$. Chaque itération $Q \leftarrow Q + M, R \leftarrow R - PM$ conserve cette égalité. À la fin nous avons $S = PQ + R$ et $\deg R < \deg P$, comme souhaité. \square

18/32

Exercices

Exercice

Soit $\mathbb{F}_4 := \mathbb{Z}_2[X]/(X^2 + X + 1)$. On pose $x := \bar{X} \in \mathbb{F}_4$.

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

Exercice

Soit $P \in \mathbb{Z}_m[X]$ un polynôme avec $\deg P = d$ et $\text{dom } P = 1$.

- Déterminer le cardinal de l'anneau quotient $\mathbb{Z}_m[X]/(P)$.
- 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.)

20/32

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.

Démonstration. Il existe une unique paire de polynômes $Q, R \in \mathbb{K}[X]$ telle que $P = (X - a)Q + R$ et $\deg R < \deg(X - a) = 1$, donc $R \in \mathbb{K}$.
Ainsi $P(a) = R$ s'annule si et seulement si $R = 0$.
Dans ce cas $P = (X - a)Q$, comme souhaité. □

Corollaire

Pour tout $P \in \mathbb{K}[X]^*$ et tout $a \in \mathbb{K}$ il existe un unique entier $m \geq 0$ et une 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 $m \geq 2$. □

§3.1

21/32

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 $a_1, \dots, a_k \in \mathbb{K}$ sont des racines distinctes, de multiplicité $m_1, \dots, m_k \geq 1$,
et le polynôme $Q \in \mathbb{K}[X]$ n'a pas de racine dans \mathbb{K} .

Démonstration. On procède par récurrence sur $\deg(P) \geq 0$.

Si $\deg(P) = 0$ alors P n'a pas de racines et $P = Q$ convient.

Si $\deg(P) \geq 1$ on distingue deux cas : si P n'a pas de racines alors $P = Q$.

Si $a_1 \in \mathbb{K}$ est une racine de P , alors $P = (X - a_1)^{m_1} P^*$ où $m_1 \geq 1$
et $P^* \in \mathbb{K}[X]$ vérifie $P^*(a_1) \neq 0$ et $0 \leq \deg(P^*) < \deg(P)$.

Par récurrence, on sait déjà que $P^* = (X - a_2)^{m_2} \cdots (X - a_k)^{m_k} Q$
où $a_2, \dots, a_k \in \mathbb{K}$ sont des racines distinctes, de multiplicité $m_1, \dots, m_k \geq 1$,
et le polynôme $Q \in \mathbb{K}[X]$ n'a pas de racine dans \mathbb{K} .
On conclut que $P = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k} Q$ comme souhaité. □

⚠ 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 $P = (X - \bar{1})(X + \bar{1}) = (X - \bar{3})(X + \bar{3})$.

§3.1

21/32

22/32

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).

Démonstration. On peut écrire $P = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k} Q$
où $a_1, \dots, a_k \in \mathbb{K}$ sont des racines distinctes, de multiplicité $m_1, \dots, m_k \geq 1$,
et le polynôme $Q \in \mathbb{K}[X]$ n'a pas de racine dans \mathbb{K} .

Si $P(a) = 0$ pour un $a \in \mathbb{K}$, alors l'intégrité de \mathbb{K} entraîne qu'un des facteurs ci-dessus s'annule : ce ne peut être $Q(a)$, on a donc $(a - a_i) = 0$ pour un i .
Ainsi a est forcément une des racines a_1, \dots, a_k déjà exhibées,
et l'égalité $\deg P = m_1 + \cdots + m_k + \deg Q$ prouve l'énoncé. □

Remarque

Nous ne regardons ici que des anneaux commutatifs.

Dans l'anneau non commutatif $\text{Mat}(2 \times 2, \mathbb{C})$ 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 $M = \begin{pmatrix} ix & y+iz \\ -y+iz & -ix \end{pmatrix}$ vérifie $M^2 = -1$.

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

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

§3.1

23/32

Racines multiples et dérivée

Proposition

La **dérivation** $\partial: \mathbb{K}[X] \rightarrow \mathbb{K}[X]$ 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 : $\partial(PQ) = (\partial P) \cdot Q + P \cdot (\partial Q)$.

Démonstration. Évidemment $\partial(P+Q) = \partial P + \partial Q$ et $\partial(aP) = a(\partial P)$ pour tout $a \in \mathbb{K}$. La règle de Leibniz est vérifiée pour $P = X^m$ et $Q = X^n$ car

$$\begin{aligned} \partial(PQ) &= \partial X^{m+n} = (m+n)X^{m+n-1} \\ &= mX^{m-1} \cdot X^n + X^m \cdot nX^{n-1} = (\partial P) \cdot Q + P \cdot (\partial Q). \end{aligned}$$

Cette formule est linéaire en P et en Q , elle s'étend donc à toute paire de polynômes. (Exercice !)

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 .

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

D'après Leibniz on a $P' = \partial P = m(X - a)^{m-1} Q + (X - a)^m (\partial Q)$.

Si a est une racine multiple, c'est-à-dire $m \geq 2$, alors $P(a) = 0$ et $P'(a) = 0$.

Réciproquement $P'(a) = 0$ implique $m \geq 1$, puis $P'(a) = 0$ entraîne $m \geq 2$, car pour $m = 1$ on aurait $P'(a) = Q(a) \neq 0$. □

§3.1

23/32

24/32

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' . \odot

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 $0, 1, 2, \dots, p-1$ nous avons donc trouvé p racines distinctes. Ainsi $X^p - X = \prod_{a \in \mathbb{Z}_p} (X - a) = X(X-1)(X-2) \cdots (X-p+1)$. \odot

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 $X^n - 1 = (X^m - 1)^p$. \odot

◆ 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 $\text{pgcd}(P, P')$.

3.2

25.32

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 $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ 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

$$\langle e^{2\pi i/n} \rangle = \{e^{2\pi i k/n} \mid k = 0, \dots, n-1\}$$

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 $\text{Mat}(n \times n, \mathbb{K})^\times = \text{GL}(n, \mathbb{K})$. Effectivement, on a d'abord $G \hookrightarrow S_n$ puis $S_n \hookrightarrow \text{GL}(n, \mathbb{K})$.

26.32

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.

Démonstration. Soit $G \subset \mathbb{K}^\times$ un sous-groupe d'ordre n .

D'après Lagrange, tout élément $x \in G$ vérifie $x^n = 1$.

Ceci fournit n racines distinctes du polynôme $X^n - 1$.

On en déduit que $G = \{x \in \mathbb{K} \mid x^n - 1 = 0\}$, car $X^n - 1$ ne peut avoir plus de racines que les n racines déjà exhibées.

Si $H \subset \mathbb{K}^\times$ est un autre sous-groupe d'ordre n , alors cet argument montre que $H = \{x \in \mathbb{K} \mid x^n - 1 = 0\} = G$. \square

Exemple

Cet énoncé ne tient plus si \mathbb{K} n'est pas intègre. Le groupe $\mathbb{Z}_6^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ admet trois sous-groupes d'ordre 2, à savoir $\{\bar{1}, \bar{3}\}$ et $\{\bar{1}, \bar{5}\}$ et $\{\bar{1}, \bar{7}\}$.

3.3

27.32

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 $G = \langle g \rangle$.

Démonstration. Soit $n = |G|$ l'ordre du groupe et soit $n = p_1^{e_1} \cdots p_k^{e_k}$ sa décomposition en facteurs premiers $p_1 < \cdots < p_k$ où $e_1, \dots, e_k \geq 1$.

Tout $x \in G$ vérifie $x^n = 1$ par le théorème de Lagrange.

Pour $m_1 = p_1^{e_1-1} p_2^{e_2} \cdots p_k^{e_k}$ le polynôme $P_1 = X^{m_1} - 1$ admet au plus m_1 racines dans \mathbb{K} , il existe donc $x_1 \in G$ tel que $P_1(x_1) \neq 0$. Alors

$$g_1 := x_1^{p_2^{e_2} \cdots p_k^{e_k}} \text{ vérifie } g_1^{p_1} = x_1^{m_1} = 1 \text{ mais } g_1^{p_1-1} = x_1^{m_1-1} \neq 1.$$

Ceci veut dire que g_1 est d'ordre $p_1^{e_1}$ exactement.

De la même manière il existe g_2, \dots, g_k tels que $\text{ord}(g_i) = p_i^{e_i}$.

Leur produit $g = g_1 \cdots g_k$ est d'ordre $p_1^{e_1} \cdots p_k^{e_k}$, donc $G = \langle g \rangle$. \square

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 $\text{ord}(2) = 3$ puis $\text{ord}(3) = 6$, donc $\mathbb{Z}_7^\times = \langle 3 \rangle$.

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.

28.32

L'ordre d'un produit dans un groupe abélien

Lemme

Soit G un groupe abélien et soient $x, y \in G$ deux éléments tels que $m = \text{ord}(x)$ et $n = \text{ord}(y)$ soient premiers entre eux. Alors $\text{ord}(xy) = mn$.

Démonstration. On a $(xy)^{mn} = x^{mn}y^{mn} = 1$, donc $\text{ord}(xy)$ divise mn .

Il existe des coefficients de Bézout $u, v \in \mathbb{Z}$ tels que $um + vn = 1$.

On obtient ainsi $(xy)^{um} = x^{1-vn}y^{um} = x$, par conséquent $\langle x \rangle \subset \langle xy \rangle$.

Ainsi $\text{ord}(x)$ divise $\text{ord}(xy)$ par le théorème Lagrange.

De même $(xy)^{vn} = x^{vn}y^{1-um} = y$, donc $\text{ord}(y)$ divise $\text{ord}(xy)$.

Ainsi $\text{ppcm}(m, n) = mn$ divise $\text{ord}(xy)$. On conclut que $\text{ord}(xy) = mn$. \square

! Si m et n ne sont pas premiers entre eux, alors $\text{ord}(xy)$ divise $\text{ppcm}(m, n)$ mais en général on ne sait pas dire plus.

§3.3

29/32

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 2 puis de 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 ?

§4.0

31/32

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} . \square

Algorithme 9.5 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 $x^m = 1$.

§3/32

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 $\mathbb{K}[X] \rightarrow \mathbb{K}^\mathbb{K}$ donnée par $P \mapsto f_P$ est un morphisme d'anneaux injectif.

Si \mathbb{K} est intègre de cardinal $q \in \mathbb{N}$, alors $\mathbb{K}[X]_{<q} \rightarrow \mathbb{K}^\mathbb{K}$ 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 $R = X^{p^d} - X$ où $r = m \bmod n$.

(Indication : calculer modulo $X^{p^n} - X$, ce qui veut dire que $X^{p^n} \equiv X$.)

En déduire par récurrence que $\text{pgcd}(M, N) = X^{p^d} - X$ où $d = \text{pgcd}(m, n)$.

En particulier, $X^{p^m} - X$ divise $X^{p^n} - X$ si et seulement si m divise n .

§2/32