UNIVERSITÉ MOHAMMED V
FACULTÉ DES SCIENCES DE RABAT
Département de Mathématiques

Licence 1 – Sciences Mathématiques

Algèbre II

CHAPITRE 2

Polynômes

Définitions, arithmétique, racines et factorisation

Prof. Mohamed Najib LAATABI

Toute remarque de votre part est la bienvenue.
Si vous identifiez une erreur, veuillez la signaler.

najib.laatabi@um5r.ac.ma

mohamednajiblaatabi.com

Année universitaire : **2025–2026**

Table des matières

Notations et mode d'emploi **ii**

2 Polynômes **1**

2.1 L'anneau des polynômes à une indéterminée 1
2.2 Évaluation, fonctions polynomiales et composition 4
2.3 Division euclidienne dans $K[X]$ 5
2.4 Racines d'un polynôme 7
2.5 Multiplicité des racines et dérivation formelle 8
2.6 Divisibilité et PGCD des polynômes 10
2.7 Polynômes irréductibles et décomposition en facteurs 13
2.8 Factorisation suivant le corps de coefficients 15
2.9 Relations entre racines et coefficients 17
2.10 Interpolation polynomiale 18

Bibliographie **20**

Notations et mode d'emploi

Notation	Signification
$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	Entiers naturels (avec 0), entiers relatifs, rationnels, réels et complexes.
K, $K^\times$	Corps commutatif de coefficients ; groupe des scalaires non nuls.
$K[X]$, $K(X)$	Anneau des polynômes en X sur K ; corps des fractions rationnelles.
$P = \sum_{k=0}^{n} a_k X^k$	Polynôme à coefficients $a_k \in K$; X est une indéterminée.
$\deg P$, $\mathrm{cd}(P)$	Degré et coefficient dominant de $P \neq 0$; convention $\deg 0 = -\infty$.
$P(a)$, $\mathcal{Z}_K(P)$	Évaluation de P en a ; ensemble de ses racines dans K.
$P \circ Q$, P'	Composition de polynômes ; dérivée formelle.
$P^{(j)}$, $m_a(P)$	Dérivée d'ordre j ; multiplicité de a comme racine de $P \neq 0$.
$A \mid B$	A divise B dans $K[X]$.
$\mathrm{pgcd}(A, B)$, $\mathrm{ppcm}(A, B)$	PGCD et PPCM unitaires de polynômes.
$K_n[X]$	Espace vectoriel des polynômes de degré au plus n.
$\mathbb{F}_p$	Corps fini $\mathbb{Z}/p\mathbb{Z}$ pour p premier.
$\mathrm{car}(K)$	Caractéristique du corps K.

Conventions de lecture

Dans tout le chapitre, K désigne un **corps commutatif**. Les démonstrations sont données sauf mention explicite « admis » ; Les symboles pgcd et ppcm désignent des polynômes **unitaires**, afin de fixer leur unicité.

Chapitre

2 Polynômes

Les polynômes interviennent dans la résolution des équations, le calcul algébrique, l'interpolation et la construction de nouveaux corps. Leur étude offre un exemple central d'**anneau commutatif intègre** au sens du chapitre 1 : l'anneau $K[X]$ des polynômes à coefficients dans un corps K. Sa division euclidienne permet de transposer une grande partie de l'arithmétique des entiers aux polynômes.

Les notions de ce chapitre sont présentées dans l'esprit du cours Exo7 [1], avec les prolongements algébriques suggérés par Godement [2] et Perrin [3].

2.1 L'anneau des polynômes à une indéterminée

2.1.1 Définition formelle et égalité

Définition 2.1.1: Polynôme sur un corps

Soit K un corps commutatif. Un **polynôme à une indéterminée** X et à coefficients dans K est une écriture formelle

$$P = \sum_{k=0}^{n} a_k X^k = a_0 + a_1 X + \cdots + a_n X^n, \qquad a_k \in K.$$

Les coefficients au-delà de n sont supposés nuls. Deux polynômes sont égaux si et seulement si tous leurs coefficients de même indice sont égaux. L'ensemble des polynômes est noté $K[X]$; ses éléments constants s'identifient naturellement aux éléments de K.

L'indéterminée X est un symbole formel, et non un nombre choisi dans K. En particulier, la notion de polynôme est distincte de celle de fonction polynomiale, qui sera introduite plus loin.

Exemple 1: Écritures d'un même polynôme

Dans $\mathbb{Q}[X]$, les écritures $2+3X^2$ et $2+0X+3X^2+0X^4$ représentent le même polynôme. En revanche, $X^2+1 \neq X+1$ car leurs coefficients de X^2 diffèrent. Dans $\mathbb{F}_2[X]$, on a $X+X=0$ puisque $1+1=0$ dans $\mathbb{F}_2$.

Définition 2.1.2: Somme et produit

Pour $P = \sum_{k\geq 0} a_k X^k$ et $Q = \sum_{k\geq 0} b_k X^k$, on pose

$$P + Q = \sum_{k\geq 0} (a_k + b_k) X^k, \qquad PQ = \sum_{n\geq 0} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) X^n.$$

Ces sommes sont finies puisque les coefficients sont nuls à partir d'un certain rang. Le produit est appelé **produit de Cauchy**.

Proposition 2.1.1: Structure de $K[X]$

L'ensemble $K[X]$, muni de l'addition et de la multiplication précédentes, est un anneau commutatif unitaire, de neutres 0 et 1. Le corps K s'identifie à un sous-anneau de $K[X]$ par l'inclusion des constantes.

Démonstration. L'addition des coefficients hérite de l'associativité, de la commutativité, du neutre 0 et des opposés dans K. Pour le produit, le coefficient de X^n dans $(PQ)R$ vaut

$$\sum_{i+j+k=n} a_i b_j c_k,$$

qui est également le coefficient de X^n dans $P(QR)$: le produit est associatif. La formule des coefficients et la commutativité de K donnent $PQ = QP$. Le polynôme constant 1 est neutre pour le produit. Enfin, la distributivité résulte de celle de K coefficient par coefficient. ■

Exemple 2: Calcul du produit

Si $P = 1 + 2X + X^2$ et $Q = 1 - X$, alors

$$PQ = 1 + X - X^2 - X^3.$$

Il est important de regrouper les termes de même degré avant de conclure.

2.1.2 Degré, coefficient dominant et polynômes unitaires

Définition 2.1.3: Degré et coefficient dominant

Soit $P = \sum_{k\geq 0} a_k X^k \neq 0$. Son **degré** est

$$\deg P = \max\{k \in \mathbb{N} : a_k \neq 0\}.$$

Si $n = \deg P$, le coefficient a_n est le **coefficient dominant**, noté $\mathrm{cd}(P)$. Le polynôme P est **unitaire** si $a_n = 1$. On convient que $\deg 0 = -\infty$; un polynôme constant non nul est de degré 0.

Proposition 2.1.2: Règles sur les degrés

Pour tous $P, Q \in K[X]$:

1. $\deg(P+Q) \leq \max(\deg P, \deg Q)$; il y a égalité si $\deg P \neq \deg Q$;
2. si $P, Q \neq 0$, alors $\deg(PQ) = \deg P + \deg Q$ et $\mathrm{cd}(PQ) = \mathrm{cd}(P)\,\mathrm{cd}(Q)$;
3. si $P \neq 0$ et $n \geq 1$, $\deg(P^n) = n \deg P$.

Démonstration. Au-delà de $\max(\deg P, \deg Q)$, les deux coefficients sont nuls ; d'où la première inégalité. Si, par exemple, $\deg P > \deg Q$, le coefficient dominant de P ne peut pas être annulé par celui de Q. Si $P, Q \neq 0$, écrivons leurs termes dominants $a_m X^m$ et $b_n X^n$. Le coefficient de X^{m+n} dans PQ est $a_m b_n \neq 0$, car K est un corps, donc intègre, et il n'y a aucun terme de degré supérieur. La dernière formule découle par récurrence de la deuxième. ■

Corollaire 2.1.1: Intégrité et éléments inversibles

L'anneau $K[X]$ est intègre. Ses seuls éléments inversibles sont les polynômes constants non nuls :

$$K[X]^\times = K^\times.$$

Démonstration. Si $PQ = 0$ et $P, Q \neq 0$, on aurait $\deg(PQ) = \deg P + \deg Q \geq 0$, contradiction. Si $PQ = 1$, la formule des degrés entraîne $\deg P = \deg Q = 0$; P et Q sont donc des constantes non nulles. Réciproquement, toute constante non nulle est inversible dans K. ■

Remarque 1: L'hypothèse sur les coefficients

Sur un anneau possédant des diviseurs de zéro, la formule du degré du produit peut être fausse : dans $(\mathbb{Z}/6\mathbb{Z})[X]$, $(2X)(3X) = 0$ alors que les deux facteurs sont non nuls. Le caractère intègre de K est donc déterminant.

2.1.3 Identités remarquables et puissances

Pour $P, Q \in K[X]$, toutes les identités algébriques usuelles qui reposent sur la commutativité restent valables :

$$P^2 - Q^2 = (P-Q)(P+Q), \qquad P^n - Q^n = (P-Q)\sum_{j=0}^{n-1} P^{n-1-j}Q^j.$$

Proposition 2.1.3: Formule du binôme dans $K[X]$

Pour tous $P, Q \in K[X]$ et tout $n \in \mathbb{N}$,

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

Ici, $\binom{n}{k}$ est vu comme un élément de K via $\mathbb{Z} \longrightarrow K$.

Démonstration. Pour $n = 0$, les deux membres valent 1. Supposons la formule vraie au rang n ; en multipliant par $P+Q$ puis en regroupant les termes, la relation de Pascal $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ donne la formule au rang $n+1$. La preuve reste valable dans toute caractéristique. ■

2.2 Évaluation, fonctions polynomiales et composition

2.2.1 Substitution d'un scalaire

Définition 2.2.1: Valeur d'un polynôme

Pour $P = \sum_{k=0}^{n} a_k X^k \in K[X]$ et $x \in K$, on définit

$$P(x) = \sum_{k=0}^{n} a_k x^k.$$

L'application $\widetilde{P} : K \to K$, $x \mapsto P(x)$, est la **fonction polynomiale associée** à P.

Proposition 2.2.1: L'évaluation est un morphisme

Pour chaque $a \in K$, l'application

$$\mathrm{ev}_a : K[X] \longrightarrow K, \qquad P \longmapsto P(a)$$

est un morphisme d'anneaux unitaires :

$$(P+Q)(a) = P(a) + Q(a), \quad (PQ)(a) = P(a)Q(a), \quad 1(a) = 1.$$

Démonstration. La première formule résulte de l'addition coefficient par coefficient. Pour le produit, la distributivité et le regroupement selon les puissances montrent que

$$P(a)Q(a) = \sum_{i,j} a_i b_j a^{i+j} = \sum_{n} \left(\sum_{i+j=n} a_i b_j \right) a^n = (PQ)(a).$$

La valeur du polynôme constant 1 est 1. ■

Remarque 2: Polynôme versus fonction polynomiale

Sur un corps fini, deux polynômes distincts peuvent définir la même fonction. Ainsi, dans $\mathbb{F}_2[X]$, $X^2 - X \neq 0$, mais $x^2 - x = 0$ pour chaque $x \in \mathbb{F}_2$. Sur un corps infini, nous montrerons que l'application $P \mapsto \widetilde{P}$ est injective.

2.2.2 Composition et changement de variable

Définition 2.2.2: Composition de polynômes

Si $P = \sum_{k=0}^{n} a_k X^k$ et $Q \in K[X]$, on pose

$$P \circ Q = P(Q) = \sum_{k=0}^{n} a_k Q^k.$$

La composition est associative et X joue le rôle d'identité. En général, $P \circ Q \neq Q \circ P$.

Proposition 2.2.2: Degré d'une composée

Si P et Q sont non constants, alors

$$\deg(P \circ Q) = \deg P \deg Q.$$

Démonstration. Si $\deg P = m \geq 1$ et $\deg Q = n \geq 1$, le terme dominant de $P(Q)$ provient uniquement du terme $a_m Q^m$, de degré mn ; son coefficient dominant est $a_m \operatorname{cd}(Q)^m \neq 0$. Les autres puissances Q^k, pour $k < m$, ont un degré strictement inférieur. ■

Exemple 3: La composition n'est pas commutative

Pour $P = X + 1$ et $Q = X^2$, on obtient

$$P \circ Q = X^2 + 1, \qquad Q \circ P = (X+1)^2.$$

Dans $\mathbb{Q}[X]$, le second vaut $X^2 + 2X + 1$: les deux polynômes diffèrent.

2.3 Division euclidienne dans $K[X]$

2.3.1 Existence et unicité du quotient et du reste

Théorème 2.3.1: Division euclidienne des polynômes

Soient $A, B \in K[X]$, avec $B \neq 0$. Il existe un unique couple $(Q, R) \in K[X]^2$ tel que

$$\boxed{A = BQ + R, \qquad R = 0 \quad \text{ou} \quad \deg R < \deg B.}$$

Q est le **quotient** et R le **reste** de la division de A par B.

Démonstration. **Existence.** Si $A = 0$ ou $\deg A < \deg B$, on choisit $Q = 0$, $R = A$. Dans le cas contraire, écrivons $A = a_m X^m + \cdots$ et $B = b_n X^n + \cdots$, avec $m \geq n$ et $a_m b_n \neq 0$. Puisque K est un corps, b_n possède un inverse ; le polynôme

$$A_1 = A - \frac{a_m}{b_n} X^{m-n} B$$

a un degré strictement inférieur à m. En répétant l'opération, on abaisse strictement le degré à chaque étape. Après un nombre fini d'étapes, on trouve $A = BQ + R$ avec $\deg R < \deg B$ ou $R = 0$.

Unicité. Si $A = BQ + R = BQ' + R'$, alors $B(Q - Q') = R' - R$. Si $Q - Q' \neq 0$, le membre de gauche a un degré au moins égal à $\deg B$, alors que le membre de droite, s'il est non nul, a un degré strictement inférieur à $\deg B$. C'est impossible ; ainsi $Q = Q'$ et $R = R'$. ■

Exemple 4: Division posée

Dans $\mathbb{Q}[X]$, divisons $A = X^3 - 2X + 3$ par $B = X - 1$. On écrit successivement

$$\begin{aligned} A - X^2 B &= X^2 - 2X + 3, \\ (X^2 - 2X + 3) - XB &= -X + 3, \\ (-X + 3) - (-1)B &= 2. \end{aligned}$$

Ainsi

$$\boxed{X^3 - 2X + 3 = (X - 1)(X^2 + X - 1) + 2.}$$

Remarque 3: Pourquoi choisir un corps ?

Diviser dans $\mathbb{Q}[X]$ par $2X + 1$ est toujours possible, car 2 y est inversible. Dans $\mathbb{Z}[X]$, le quotient devrait parfois posséder des coefficients rationnels : la division euclidienne avec coefficients entiers n'y fonctionne pas sous cette forme.

2.3.2 Division par un polynôme de degré un

Théorème 2.3.2: Théorème du reste

Pour tout $P \in K[X]$ et tout $a \in K$, le reste de la division par $X - a$ est le polynôme constant $P(a)$. Il existe donc un unique $Q \in K[X]$ tel que

$$\boxed{P(X) = (X - a)Q(X) + P(a).}$$

Démonstration. Par la division euclidienne, on peut écrire $P = (X-a)Q+R$ avec $\deg R < 1$, donc R constant (éventuellement nul). L'évaluation en a fournit $P(a) = 0 \cdot Q(a) + R = R$. ■

Proposition 2.3.1: Schéma de Horner

Soit $P = a_n X^n + \cdots + a_1 X + a_0$. Pour calculer $P(a)$, on définit successivement

$$b_n = a_n, \qquad b_k = a_k + a\, b_{k+1} \quad (k = n-1, \ldots, 0).$$

Alors $P(a) = b_0$. De plus, $P = (X - a)(b_n X^{n-1} + \cdots + b_2 X + b_1) + b_0$.

Démonstration. On développe le membre de droite. Son coefficient de X^n est $b_n = a_n$ et celui de X^k, pour $1 \leq k \leq n-1$, est $b_k - a b_{k+1} = a_k$; le terme constant est $b_0 - a b_1 = a_0$. Le dernier terme b_0 est donc le reste ; le théorème du reste donne $b_0 = P(a)$. ■

Exemple 5: Horner en pratique

Pour $P = 2X^3 - 3X^2 + 4X - 5$ en $a = 2$, les coefficients successifs obtenus par Horner sont 2, 1, 6, 7. Ainsi $P(2) = 7$ et

$$P = (X - 2)(2X^2 + X + 6) + 7.$$

2.4 Racines d'un polynôme

2.4.1 Caractérisation et conséquences

Définition 2.4.1: Racine d'un polynôme

Soit $P \in K[X]$. Un élément $a \in K$ est une **racine** de P si $P(a) = 0$. L'ensemble des racines de P dans K est noté $\mathcal{Z}_K(P) = \{a \in K : P(a) = 0\}$.

Théorème 2.4.1: Critère de divisibilité par $X - a$

Pour tout $P \in K[X]$ et tout $a \in K$,

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

Démonstration. D'après le théorème du reste, $P = (X - a)Q + P(a)$. Si $P(a) = 0$, on a directement $P = (X - a)Q$. Inversement, si $P = (X - a)Q$, l'évaluation en a entraîne $P(a) = 0$. ■

Proposition 2.4.1: Produit de facteurs linéaires

Si $a_1, \ldots, a_r \in K$ sont des racines *deux à deux distinctes* de P, alors

$$\prod_{i=1}^{r}(X - a_i) \mid P.$$

Démonstration. Raisonnons par récurrence sur r. Le cas $r = 1$ vient du théorème précédent. Si $P = (X - a_1)Q$ et si $a_j \neq a_1$, alors $0 = P(a_j) = (a_j - a_1)Q(a_j)$. Comme $a_j - a_1 \neq 0$ et que K est un corps, on obtient $Q(a_j) = 0$ pour $j = 2, \ldots, r$. L'hypothèse de récurrence montre que $\prod_{i=2}^{r}(X - a_i)$ divise Q, et donc le produit voulu divise P. ■

Théorème 2.4.2: Nombre maximal de racines

Un polynôme non nul $P \in K[X]$ de degré n possède au plus n racines distinctes dans K.

Démonstration. Si P possédait $n+1$ racines distinctes, la proposition précédente impliquerait que le produit des $n + 1$ facteurs linéaires correspondants, de degré $n + 1$, divise P. Ainsi $P = QS$ avec $\deg Q = n + 1$ et $S \neq 0$, ce qui donne $\deg P \geq n + 1$, contradiction. ■

Corollaire 2.4.1: Égalité de polynômes sur un corps infini

Si K est infini et si $P, Q \in K[X]$ vérifient $P(x) = Q(x)$ pour tout $x \in K$, alors $P = Q$. Plus généralement, si $\deg P, \deg Q \leq n$ et si les deux polynômes coïncident en $n+1$ points distincts, alors $P = Q$.

Démonstration. Le polynôme $P - Q$ possède tous les points considérés comme racines. S'il était non nul, il serait de degré au plus n dans le second cas et ne pourrait avoir $n+1$ racines. Dans le premier cas, $P - Q$ aurait une infinité de racines, contredisant le théorème. ■

Exemple 6: Racines dans différents corps

Le polynôme $P = X^2 + 1$ n'a aucune racine dans $\mathbb{R}$, mais possède les deux racines i et $-i$ dans $\mathbb{C}$. Dans $\mathbb{F}_2$, le polynôme $X^2 - X$ est non nul et a les deux éléments du corps pour racines, ce qui est compatible avec son degré 2.

2.4.2 Polynômes scindés

Définition 2.4.2: Polynôme scindé

Un polynôme non constant $P \in K[X]$ est **scindé sur** K s'il s'écrit

$$P = a \prod_{j=1}^{n} (X - \alpha_j), \qquad a \in K^\times, \quad \alpha_j \in K,$$

avec $n = \deg P$. Les α_j ne sont pas nécessairement distincts.

Exemple 7: Scindage dépendant du corps

$X^2 - 2$ est scindé dans $\mathbb{R}[X]$, car $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$, mais il n'est pas scindé dans $\mathbb{Q}[X]$. Le polynôme $(X - 1)^3(X + 2)$ est scindé sur $\mathbb{Q}$.

2.5 Multiplicité des racines et dérivation formelle

2.5.1 Ordre d'une racine

Définition 2.5.1: Multiplicité d'une racine

Soit $P \in K[X]$ non nul et $a \in K$. La **multiplicité** de a est l'unique entier $m \geq 0$ tel que

$$P = (X - a)^m Q, \qquad Q(a) \neq 0.$$

On dit que a est racine **simple** si $m = 1$, **double** si $m = 2$, et ainsi de suite.

Proposition 2.5.1: Existence et additivité de la multiplicité

Pour tout $P \neq 0$, la multiplicité $m_a(P)$ existe et est unique. Pour tous $P, Q \neq 0$:

$$m_a(PQ) = m_a(P) + m_a(Q).$$

En outre, si $a_1, \ldots, a_r$ sont des racines distinctes de P de multiplicités $m_1, \ldots, m_r$, alors

$$\sum_{j=1}^{r} m_j \leq \deg P.$$

Démonstration. Les exposants m pour lesquels $(X - a)^m$ divise P sont compris entre 0 et $\deg P$: leur maximum existe. Si $P = (X - a)^m Q$ et $Q(a) = 0$, le théorème du reste montre que $(X - a)^{m+1}$ divise P, contradiction. L'unicité vient du caractère maximal de m. Si $P = (X - a)^m U$, $Q = (X - a)^n V$ avec $U(a)V(a) \neq 0$, alors $PQ = (X - a)^{m+n} UV$

et $(UV)(a) \neq 0$; d'où l'additivité. Pour des racines distinctes, le raisonnement successif du critère de factorisation montre que $\prod_j (X - a_j)^{m_j}$ divise P. La formule du degré donne la dernière inégalité. ■

Exemple 8: Racine multiple

Pour $P = (X-2)^3(X+1)^2$, le nombre 2 est racine triple et -1 est racine double. La somme des multiplicités vaut $5 = \deg P$.

2.5.2 Polynôme dérivé et règles de calcul

Définition 2.5.2: Dérivée formelle

La **dérivée formelle** de $P = \sum_{k=0}^{n} a_k X^k$ est

$$P' = \sum_{k=1}^{n} k a_k X^{k-1}.$$

Le coefficient k est interprété comme $k \cdot 1_K$. On note $P^{(j)}$ la dérivée formelle d'ordre j, avec $P^{(0)} = P$.

Proposition 2.5.2: Règles de dérivation

Pour $P, Q \in K[X]$ et $\lambda \in K$,

$$(P + \lambda Q)' = P' + \lambda Q', \qquad (PQ)' = P'Q + PQ', \qquad (P \circ Q)' = (P' \circ Q)Q'.$$

Démonstration. La linéarité résulte de la définition. Pour les monômes,

$$(X^i X^j)' = (i+j)X^{i+j-1} = iX^{i-1}X^j + jX^i X^{j-1}.$$

Par bilinéarité, la règle du produit s'étend aux polynômes quelconques. La règle de composition découle de $(Q^k)' = kQ^{k-1}Q'$, qui s'obtient par récurrence avec la règle du produit, puis de la linéarité de la dérivation. ■

Remarque 4: Attention à la caractéristique positive

Si K est de caractéristique $p > 0$, la dérivée de X^p est nulle bien que X^p soit non constant. La dérivation formelle ne se confond donc pas toujours avec les propriétés de dérivation en analyse réelle.

2.5.3 Détecter les racines multiples

Théorème 2.5.1: Critère de la racine multiple

Soit $P \in K[X]$ non nul et $a \in K$. Alors

$$\boxed{m_a(P) \geq 2 \iff P(a) = P'(a) = 0.}$$

En particulier, une racine a est simple si et seulement si $P(a) = 0$ et $P'(a) \neq 0$.

Démonstration. Si $P = (X-a)^m Q$ avec $m \geq 2$, sa dérivée est

$$P' = m(X-a)^{m-1}Q + (X-a)^m Q',$$

donc $P(a) = P'(a) = 0$. Réciproquement, si $P(a) = 0$, écrivons $P = (X-a)Q$. La règle du produit donne $P' = Q + (X-a)Q'$, d'où $P'(a) = Q(a)$. Si $P'(a) = 0$, le théorème du reste implique $(X-a) \mid Q$, et par suite $(X-a)^2 \mid P$. ■

Proposition 2.5.3: Dérivées successives en caractéristique nulle

Si $\mathrm{car}(K) = 0$, un élément $a \in K$ est racine d'ordre exactement $m \geq 1$ de P si et seulement si

$$P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0, \qquad P^{(m)}(a) \neq 0.$$

Démonstration. Pour $P = (X-a)^m Q$ avec $Q(a) \neq 0$, la règle de Leibniz, obtenue en dérivant m fois la règle du produit, montre que les m premières évaluations (ordres $0, \ldots, m-1$) sont nulles et que $P^{(m)}(a) = m!Q(a) \neq 0$ en caractéristique nulle. Inversement, si les dérivées des ordres $0, \ldots, m-1$ sont nulles, on applique successivement le critère du facteur $X-a$ et la relation $P'(a) = Q(a)$ pour obtenir $(X-a)^m \mid P$; la non-nullité de $P^{(m)}(a)$ exclut une puissance supplémentaire. ■

2.6 Divisibilité et PGCD des polynômes

2.6.1 Divisibilité et polynômes associés

Définition 2.6.1: Divisibilité dans $K[X]$

Pour $A, B \in K[X]$, on dit que A **divise** B, et on écrit $A \mid B$, s'il existe $Q \in K[X]$ tel que $B = AQ$. Deux polynômes non nuls sont **associés** s'ils diffèrent par multiplication par un scalaire non nul de K.

Proposition 2.6.1: Propriétés de la divisibilité

Soient $A, B, C \in K[X]$.

1. Si $A \mid B$ et $B \mid C$, alors $A \mid C$.
2. Si $A \mid B$ et $A \mid C$, alors $A \mid (UB + VC)$ pour tous $U, V \in K[X]$.
3. Si $A \mid B$ et $B \neq 0$, alors $\deg A \leq \deg B$.
4. Si $A, B \neq 0$, $A \mid B$ et $B \mid A$, alors A et B sont associés.

Démonstration. Les deux premières assertions découlent des identités $B = AU$ et $C = BV$, puis $UB + VC = A(UU_1 + VV_1)$ lorsque $B = AU_1, C = AV_1$. La troisième provient de $\deg B = \deg A + \deg Q$ si $B = AQ \neq 0$. Enfin, $B = AU$ et $A = BV$ donnent $A = AUV$. Par intégrité et $A \neq 0$, on déduit $UV = 1$, donc $U, V \in K^\times$. ■

Définition 2.6.2: Plus grand commun diviseur

Soient $A, B \in K[X]$, non tous deux nuls. Leur **PGCD**, noté $\mathrm{pgcd}(A, B)$, est le polynôme *unitaire* D qui divise A et B et que tout diviseur commun de A et B divise. On dit que A et B sont **premiers entre eux** si $\mathrm{pgcd}(A, B) = 1$.

2.6.2 Algorithme d'Euclide

Théorème 2.6.1: Algorithme d'Euclide dans $K[X]$

Pour $A, B \in K[X]$, non tous deux nuls, les divisions euclidiennes successives

$$\begin{aligned} A &= BQ_1 + R_1, \\ B &= R_1Q_2 + R_2, \\ R_1 &= R_2Q_3 + R_3, \quad \dots \end{aligned}$$

s'arrêtent après un nombre fini d'étapes. Le dernier reste non nul, rendu unitaire, est le PGCD de A et B.

Démonstration. Chaque reste non nul a un degré strictement inférieur au précédent. Comme une suite strictement décroissante d'entiers naturels est finie, l'algorithme s'arrête. Si $A = BQ + R$, tout diviseur commun de A et B divise $R = A - BQ$, et tout diviseur commun de B et R divise $A = BQ + R$. Les ensembles de diviseurs communs de (A, B) et (B, R) sont donc identiques. En itérant, ils sont ceux du dernier reste non nul. Celui-ci divise le reste précédent d'après la dernière division, puis tous les termes précédents en remontant les égalités. Le rendre unitaire conserve les diviseurs, et fournit le PGCD annoncé. ■

Exemple 9: Un PGCD calculé par Euclide

Sur $\mathbb{Q}[X]$, prenons $A = X^3 - 1$ et $B = X^2 - 1$. Alors

$$A = XB + (X - 1), \qquad B = (X + 1)(X - 1).$$

Le dernier reste non nul est $X - 1$, déjà unitaire :

$$\operatorname{pgcd}(X^3 - 1, X^2 - 1) = X - 1.$$

2.6.3 Identité de Bézout et théorème de Gauss

Théorème 2.6.2: Identité de Bézout

Si $D = \operatorname{pgcd}(A, B)$ pour deux polynômes A, B non tous deux nuls, il existe $U, V \in K[X]$ tels que

$$\boxed{AU + BV = D.}$$

En particulier, A et B sont premiers entre eux si et seulement si il existe $U, V \in K[X]$ tels que $AU + BV = 1$.

Démonstration. Dans l'algorithme d'Euclide, chaque nouveau reste est la différence des deux termes précédents, multipliés au besoin par un quotient. Par récurrence, tout reste est donc de la forme $AU + BV$. Le dernier reste non nul s'écrit ainsi ; en le multipliant par l'inverse de son coefficient dominant, on obtient le PGCD unitaire D. Si $AU + BV = 1$, tout diviseur commun de A, B divise 1, donc le PGCD unitaire vaut 1. La réciproque est l'identité précédente avec $D = 1$. ■

Exemple 10: Calcul explicite de Bézout

Pour $A = X^2 - 1$ et $B = X^2 + X$, on a

$$B - A = X + 1, \qquad A = (X - 1)(X + 1).$$

Le PGCD est $X + 1$; l'identité de Bézout s'écrit

$$\boxed{(X^2 + X) - (X^2 - 1) = X + 1.}$$

Il s'agit ici d'un exemple non premier entre eux.

Théorème 2.6.3: Lemme de Gauss pour la divisibilité

Si $A, B, C \in K[X]$ vérifient $\operatorname{pgcd}(A, B) = 1$ et $A \mid BC$, alors $A \mid C$.

Démonstration. Par Bézout, il existe U, V tels que $AU + BV = 1$. En multipliant par C,

$$C = A(UC) + (BC)V.$$

Le premier terme est multiple de A, et le second aussi puisque $A \mid BC$. Leur somme C est donc divisible par A. ■

Corollaire 2.6.1: Produit de polynômes premiers à A

Si $\operatorname{pgcd}(A, B) = \operatorname{pgcd}(A, C) = 1$, alors $\operatorname{pgcd}(A, BC) = 1$. Si $A \mid BC$ et si $\operatorname{pgcd}(A, B) = 1$, on peut simplifier le facteur B dans la condition de divisibilité.

Démonstration. Choisissons des identités de Bézout $AU + BV = 1$ et $AU' + CW = 1$. Leur produit donne

$$1 = A\big(AUU' + UCW + U'BV\big) + BCVW,$$

qui est une identité de Bézout pour A et BC. La seconde assertion est précisément le théorème précédent. ■

2.6.4 PPCM et relation avec le PGCD

Définition 2.6.3: Plus petit commun multiple

Pour $A, B \neq 0$, leur **PPCM** est l'unique polynôme unitaire M multiple de A et B qui divise tout multiple commun. On le note $\operatorname{ppcm}(A, B)$.

Proposition 2.6.2: Formule PGCD–PPCM

Si $A, B \neq 0$, en notant $D = \operatorname{pgcd}(A, B)$,

$$\boxed{\operatorname{ppcm}(A, B) = \frac{AB}{D \operatorname{cd}(AB/D)}.}$$

En particulier,

$$\deg \operatorname{pgcd}(A, B) + \deg \operatorname{ppcm}(A, B) = \deg A + \deg B.$$

Démonstration. Écrivons $A = DA_1$ et $B = DB_1$. Les polynômes A_1, B_1 sont premiers entre eux : un diviseur commun non constant conduirait, en le multipliant par D, à un diviseur commun de A, B de degré supérieur à celui de D. Le polynôme $AB/D = DA_1B_1$ est multiple de A et de B. Si N est un autre multiple commun, écrivons $N = DA_1U$. De $DB_1 \mid N$ on tire $B_1 \mid A_1U$; le théorème de Gauss donne $B_1 \mid U$. Ainsi $AB/D \mid N$. Sa normalisation unitaire est donc le PPCM ; l'égalité des degrés découle de $\deg(AB/D) = \deg A + \deg B - \deg D$. ■

2.7 Polynômes irréductibles et décomposition en facteurs

2.7.1 Irréductibilité

Définition 2.7.1: Polynôme irréductible

Un polynôme $P \in K[X]$ est **irréductible sur** K s'il est de degré au moins 1 et si, pour toute égalité $P = AB$ dans $K[X]$, l'un des facteurs A, B est constant non nul. Un polynôme de degré au moins 1 qui n'est pas irréductible est dit **réductible**.

Remarque 5: Le corps de base compte

Un même polynôme peut être irréductible sur un corps et réductible sur un autre. Par exemple, $X^2 + 1$ est irréductible sur $\mathbb{R}$, mais $X^2 + 1 = (X - i)(X + i)$ dans $\mathbb{C}[X]$.

Proposition 2.7.1: Critère pour les degrés deux et trois

Un polynôme $P \in K[X]$ de degré 2 ou 3 est irréductible sur K si et seulement s'il ne possède aucune racine dans K.

Démonstration. Si P possède une racine $a \in K$, alors $(X - a) \mid P$, donc $P = (X - a)Q$ avec $\deg Q = \deg P - 1 \geq 1$: il est réductible. Réciproquement, si $P = AB$ est une décomposition en facteurs non constants, $\deg A + \deg B \in \{2, 3\}$. Au moins l'un des degrés vaut 1. Ce facteur linéaire a une racine dans K, qui est également racine de P. ■

Exemple 11: Un polynôme irréductible de degré trois

Le polynôme $P = X^3 - X - 1$ est irréductible sur $\mathbb{Q}$. En effet, toute racine rationnelle de ce polynôme unitaire à coefficients entiers doit être un entier divisant 1 : nécessairement 1 ou -1. Or $P(1) = -1$ et $P(-1) = -1$. Le critère du degré trois conclut.

Proposition 2.7.2: Lemme d'Euclide pour les irréductibles

Si $P \in K[X]$ est irréductible et $P \mid AB$, alors $P \mid A$ ou $P \mid B$.

Démonstration. Si $P \nmid A$, tout diviseur commun de P et A est constant : en effet, un diviseur non constant de P lui serait associé, ce qui entraînerait $P \mid A$. Ainsi $\operatorname{pgcd}(P, A) = 1$. Le lemme de Gauss, appliqué à $P \mid AB$, donne $P \mid B$. ■

2.7.2 Décomposition en irréductibles

Théorème 2.7.1: Factorisation unique dans $K[X]$

Tout polynôme non nul $P \in K[X]$ s'écrit

$$\boxed{P = c\,P_1^{\alpha_1} \cdots P_r^{\alpha_r},}$$

où $c \in K^\times$, les P_j sont des polynômes irréductibles unitaires deux à deux distincts et $\alpha_j \geq 1$. Cette écriture est unique à l'ordre des facteurs près. Pour P constant non nul, le produit est vide et $P = c$.

Démonstration. **Existence.** On raisonne par récurrence sur le degré de P. Un polynôme de degré 0 est une unité. Si P est irréductible, sa normalisation unitaire donne la décomposition. Sinon, $P = AB$ avec $1 \leq \deg A, \deg B < \deg P$. L'hypothèse de récurrence fournit une factorisation en irréductibles de chaque facteur ; leur produit donne celle de P.

Unicité. Supposons $P = c\prod_i P_i^{\alpha_i} = d\prod_j Q_j^{\beta_j}$, avec les facteurs irréductibles unitaires. Alors P_1 divise le second produit. Le lemme d'Euclide, appliqué successivement, assure que $P_1 \mid Q_j$ pour un certain j. Comme Q_j est irréductible unitaire, $P_1 = Q_j$. On simplifie ce facteur dans l'anneau intègre $K[X]$ et on répète. Les facteurs et leurs multiplicités coïncident ; enfin, les coefficients dominants donnent $c = d$. ■

Corollaire 2.7.1: Lecture du PGCD sur les factorisations

Si A et B sont non nuls et si l'on regroupe tous les facteurs irréductibles unitaires présents dans leurs décompositions, en écrivant

$$A = a\prod_j P_j^{\alpha_j}, \qquad B = b\prod_j P_j^{\beta_j}, \qquad \alpha_j, \beta_j \geq 0,$$

alors

$$\operatorname{pgcd}(A,B) = \prod_j P_j^{\min(\alpha_j,\beta_j)}, \qquad \operatorname{ppcm}(A,B) = \prod_j P_j^{\max(\alpha_j,\beta_j)}.$$

Démonstration. Grâce à l'unicité de la factorisation, un polynôme unitaire divise A et B précisément lorsque chacun de ses exposants est au plus $\min(\alpha_j, \beta_j)$. Cette condition caractérise le PGCD. L'argument dual pour les multiples donne le PPCM. ■

Exemple 12: PGCD et PPCM directement

Dans $\mathbb{Q}[X]$, soient $A = (X-1)^3(X+2)$ et $B = (X-1)^2(X+3)^2$. Alors

$$\operatorname{pgcd}(A,B) = (X-1)^2, \qquad \operatorname{ppcm}(A,B) = (X-1)^3(X+2)(X+3)^2.$$

2.8 Factorisation suivant le corps de coefficients

2.8.1 Les polynômes complexes

Théorème 2.8.1: Théorème fondamental de l'algèbre (admis)

Tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine complexe. Par conséquent, tout polynôme $P \in \mathbb{C}[X]$ de degré $n \geq 1$ se décompose sous la forme

$$P(X) = a_n \prod_{j=1}^{n} (X - z_j), \qquad z_j \in \mathbb{C}.$$

Les racines sont comptées avec leurs multiplicités. Les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.

Démonstration. L'existence d'une racine complexe pour tout polynôme non constant constitue l'énoncé profond du théorème fondamental de l'algèbre, que nous *admettons* ici. La factorisation s'en déduit par récurrence : si z_1 est une racine, $P = (X - z_1)Q$ avec $\deg Q = n - 1$; on applique la même propriété à Q. Un polynôme de degré supérieur à 1 admet ainsi une décomposition non triviale, tandis qu'un polynôme de degré 1 est irréductible. ■

Remarque 6: Portée de la démonstration

La factorisation dans $\mathbb{C}[X]$ est ici une *conséquence démontrée* du théorème fondamental de l'algèbre ; l'existence initiale d'une racine complexe n'est pas démontrée dans ce cours élémentaire.

2.8.2 Polynômes réels et racines complexes conjuguées

Proposition 2.8.1: Conjugaison des racines

Soit $P \in \mathbb{R}[X]$ et $z \in \mathbb{C}$. Alors

$$P(\overline{z}) = \overline{P(z)}.$$

En particulier, si z est racine de P, son conjugué $\overline{z}$ est aussi racine, avec la même multiplicité.

Démonstration. Si $P = \sum a_k X^k$ avec $a_k \in \mathbb{R}$, la conjugaison donne

$$\overline{P(z)} = \sum a_k \overline{z}^k = P(\overline{z}).$$

Si $P = (X - z)^m Q$ avec $Q(z) \neq 0$, on conjugue les coefficients de cette égalité dans $\mathbb{C}[X]$. Comme P est réel, $P = (X - \overline{z})^m \overline{Q}$, avec $\overline{Q}(\overline{z}) = \overline{Q(z)} \neq 0$. Les multiplicités sont donc égales. ■

Théorème 2.8.2: Facteurs irréductibles sur $\mathbb{R}$

Tout polynôme non constant de $\mathbb{R}[X]$ est produit de facteurs de degré 1 et de polynômes quadratiques irréductibles. Les polynômes irréductibles de $\mathbb{R}[X]$ sont, à multiplication par une constante non nulle près :

— les polynômes $X - a$ avec $a \in \mathbb{R}$;

— les polynômes $X^2 + bX + c$, avec $b, c \in \mathbb{R}$ et $\Delta = b^2 - 4c < 0$.

Démonstration. Factorisons un polynôme réel dans $\mathbb{C}[X]$ à l'aide du théorème précédent. Les racines réelles donnent les facteurs $X - a$. Chaque paire de racines non réelles conjuguées $z, \overline{z}$ donne

$$(X - z)(X - \overline{z}) = X^2 - 2\,\mathrm{Re}(z)X + |z|^2,$$

polynôme réel de discriminant $-4\,\mathrm{Im}(z)^2 < 0$. Tout polynôme réel se décompose donc en facteurs des deux types. Un facteur linéaire est irréductible ; un facteur quadratique de discriminant négatif n'a aucune racine réelle et est irréductible par le critère du degré 2. Aucun facteur de degré supérieur n'est irréductible, puisqu'il possède une telle factorisation. ■

Exemple 13: Factoriser $X^4 + 4$ dans $\mathbb{R}[X]$

On utilise la différence de deux carrés :

$$X^4 + 4 = (X^2 + 2)^2 - (2X)^2 = (X^2 - 2X + 2)(X^2 + 2X + 2).$$

Chaque facteur quadratique a un discriminant négatif, égal à -4 ; la décomposition est donc irréductible sur $\mathbb{R}$. Sur $\mathbb{C}$, chaque facteur se décompose encore en deux facteurs linéaires.

2.8.3 Polynômes à coefficients rationnels et corps finis

Proposition 2.8.2: Critère des racines rationnelles

Soit $P = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$ avec $a_n a_0 \neq 0$. Si $r = u/v \in \mathbb{Q}$, écrit sous forme irréductible avec $u \in \mathbb{Z}$, $v \in \mathbb{N}^*$ et $\mathrm{pgcd}(u, v) = 1$, est une racine de P, alors

$$u \mid a_0, \qquad v \mid a_n.$$

En particulier, une racine rationnelle d'un polynôme unitaire à coefficients entiers est nécessairement entière.

Démonstration. L'égalité $P(u/v) = 0$, multipliée par v^n, donne

$$a_n u^n + a_{n-1} u^{n-1} v + \cdots + a_1 u v^{n-1} + a_0 v^n = 0.$$

Ainsi $u \mid a_0 v^n$ et $v \mid a_n u^n$. Puisque u et v sont premiers entre eux, u est premier à v^n et v est premier à u^n. Le lemme de Gauss dans $\mathbb{Z}$ donne $u \mid a_0$ et $v \mid a_n$. Si $a_n = 1$, $v = 1$. ■

Exemple 14: Un calcul sur $\mathbb{F}_2$

Dans $\mathbb{F}_2[X]$, le polynôme $P = X^2 + X + 1$ est irréductible : $P(0) = 1$ et $P(1) = 1 + 1 + 1 = 1$ dans $\mathbb{F}_2$. En revanche, $X^2 + X = X(X + 1)$ est réductible.

Remarque 7: Tester l'irréductibilité au-delà du degré trois

Pour un polynôme de degré au moins 4, l'absence de racines ne suffit plus. Ainsi X^4+4 n'a aucune racine réelle, mais se factorise dans $\mathbb{R}[X]$ en deux polynômes de degré 2. Il faut rechercher des facteurs de degrés plus élevés.

2.9 Relations entre racines et coefficients

2.9.1 Somme et produit des racines

Théorème 2.9.1: Relations de Viète

Soit $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$, avec $a_n \neq 0$. Supposons P scindé sur K et écrivons

$$P = a_n \prod_{j=1}^{n} (X - \alpha_j),$$

où les racines sont comptées avec leurs multiplicités. Alors, pour $1 \leq k \leq n$,

$$\boxed{\frac{a_{n-k}}{a_n} = (-1)^k \sum_{1 \leq i_1 < \cdots < i_k \leq n} \alpha_{i_1} \cdots \alpha_{i_k}.}$$

En particulier,

$$\sum_{j=1}^{n} \alpha_j = -\frac{a_{n-1}}{a_n}, \qquad \prod_{j=1}^{n} \alpha_j = (-1)^n \frac{a_0}{a_n}.$$

Démonstration. Dans le produit $\prod_j (X - \alpha_j)$, pour obtenir le terme X^{n-k}, il faut choisir le terme $-\alpha_j$ dans exactement k des n facteurs et le terme X dans les autres. La somme de ces contributions vaut $(-1)^k \sum_{i_1<\cdots<i_k} \alpha_{i_1} \cdots \alpha_{i_k}$. La comparaison des coefficients avec l'écriture initiale de P donne les formules. ■

Exemple 15: Trouver des relations sans résoudre l'équation

Si α, β, γ sont les racines complexes de $P = 2X^3 - 3X^2 + 5X - 7$, comptées avec leurs multiplicités, alors

$$\alpha + \beta + \gamma = \frac{3}{2}, \qquad \alpha\beta + \alpha\gamma + \beta\gamma = \frac{5}{2}, \qquad \alpha\beta\gamma = \frac{7}{2}.$$

Aucune résolution explicite du polynôme n'est nécessaire.

2.10 Interpolation polynomiale

2.10.1 Existence et unicité de l'interpolateur

Théorème 2.10.1: Interpolation de Lagrange

Soient $n \geq 0$, $x_0, \ldots, x_n \in K$ *deux à deux distincts* et $y_0, \ldots, y_n \in K$. Il existe un unique polynôme $P \in K[X]$ de degré au plus n tel que

$$P(x_i) = y_i \qquad (0 \leq i \leq n).$$

Il est donné par la **formule de Lagrange**

$$\boxed{P(X) = \sum_{i=0}^{n} y_i L_i(X), \qquad L_i(X) = \prod_{\substack{0 \leq j \leq n \\ j \neq i}} \frac{X - x_j}{x_i - x_j}.}$$

Pour $n = 0$, un produit vide vaut 1.

Démonstration. Les dénominateurs $x_i - x_j$ sont non nuls, donc inversibles dans K. Chaque polynôme L_i est de degré n au plus et satisfait

$$L_i(x_k) = \begin{cases} 1, & k = i, \\ 0, & k \neq i. \end{cases}$$

Ainsi, le polynôme $P = \sum_i y_i L_i$ est de degré au plus n et vérifie $P(x_k) = y_k$ pour chaque k : l'existence est établie. Si Q vérifie les mêmes conditions avec $\deg Q \leq n$, alors $P - Q$ s'annule aux $n + 1$ points distincts $x_0, \ldots, x_n$. Le théorème sur le nombre de racines impose $P - Q = 0$: unicité. ■

Exemple 16: Interpoler trois données

Cherchons le polynôme de degré au plus 2 tel que $P(0) = 1$, $P(1) = 2$ et $P(2) = 5$. La formule de Lagrange donne

$$P(X) = \frac{(X-1)(X-2)}{2} - 2X(X-2) + \frac{5}{2}X(X-1) = X^2 + 1.$$

On peut vérifier directement les trois valeurs demandées.

2.10.2 Applications et précautions

Remarque 8: Combien de points peut-on imposer ?

La construction de Lagrange utilise $n + 1$ abscisses distinctes de K. Sur un corps fini de cardinal q, on ne peut pas choisir plus de q points distincts. Les polynômes restent définis formellement, mais les fonctions polynomiales peuvent y être représentées par plusieurs polynômes différents.

Proposition 2.10.1: Différence de deux interpolateurs

Si deux polynômes $P, Q \in K[X]$ coïncident en des points distincts $x_0, \ldots, x_n$, alors

$$\prod_{i=0}^{n}(X - x_i) \mid (P - Q).$$

En particulier, le reste de la division de P par $\prod_{i=0}^{n}(X - x_i)$ est le polynôme interpolateur de degré au plus n prenant les valeurs $P(x_i)$.

Démonstration. Les x_i sont racines de $P - Q$, donc le produit des facteurs $(X - x_i)$ divise $P - Q$. Si l'on divise P par ce produit, $P = AB + R$ avec $\deg R \leq n$. Comme $B(x_i) = 0$, $R(x_i) = P(x_i)$; l'unicité de l'interpolateur donne le résultat. ■

Bibliographie

[1] **Collectif Exo7.** *Algèbre – Cours de mathématiques, première année*. Cours librement accessible sur la plateforme Exo7.

https://exo7.emath.fr/cours/livre-algebre-1.pdf.

Pour ce chapitre : calcul polynomial, divisions euclidiennes, racines, factorisation, PGCD et exercices de Licence.

[2] **Roger Godement.** *Cours d'algèbre*. Hermann, 3e édition.

https://www.editions-hermann.fr/livre/cours-d-algebre-roger-godement.

Pour ce chapitre : formulation rigoureuse des structures, polynômes, morphismes, propriétés de factorisation et corps.

[3] **Daniel Perrin.** *Cours d'algèbre*. Ellipses, 1996.

Pour ce chapitre : idéaux principaux, arithmétique de $K[X]$, irréductibilité, théorèmes d'isomorphisme et construction de corps.