

Chapitre IX - Arithmétique sur $K[X]$

Dans ce chapitre, la lettre K désigne un corps commutatif, par exemple \mathbb{Q} , \mathbb{R} , \mathbb{C} , ou $\mathbb{Z}/p\mathbb{Z}$, où p est un nombre premier. On va définir l'anneau $K[X]$ des polynômes à une indéterminée à coefficients dans K . On constatera que les propriétés arithmétiques de cet anneau sont essentiellement les mêmes que celles de l'anneau \mathbb{Z} , ce qui s'explique par le fait que ce sont des anneaux euclidiens, autrement dit, qu'il existe une «division euclidienne» sur chacun d'eux. Cela étant, contrairement à ce que l'on pourrait penser au départ, l'étude de l'arithmétique de \mathbb{Z} est plus difficile en général que celle de $K[X]$. Par exemple, il est assez facile de démontrer que pour tout entier $n \geq 3$, il n'existe pas de polynômes A, B, C dans $\mathbb{C}[X]$, premiers entre eux, dont l'un au moins soit non constant, tels que l'on ait

$$A^n + B^n + C^n = 0.$$

On donnera une démonstration de ce résultat à la fin du chapitre. L'analogue de cet énoncé sur \mathbb{Z} est «le grand théorème de Fermat», qui n'est devenu un théorème qu'en 1994, et dont la preuve nécessite un arsenal mathématique considérable. De nombreux résultats sont aujourd'hui démontrés dans $K[X]$ et leurs analogues sur \mathbb{Z} restent à l'état de conjectures.

Table des matières

| | |
|--|----|
| 1. L'anneau $K[X]$ | 1 |
| 2. Degré - Division euclidienne | 2 |
| 3. Plus grand commun diviseur | 5 |
| 4. Plus petit commun multiple | 7 |
| 5. Polynômes irréductibles | 8 |
| 6. Racines d'un polynôme | 10 |
| 7. Relations entre les coefficients et les racines d'un polynôme | 15 |
| 8. Théorème de Mason | 16 |

1. L'anneau $K[X]$

Un polynôme à une indéterminée à coefficients dans K est par définition une suite $(a_n)_{n \in \mathbb{N}}$ d'éléments de K qui est nulle à partir d'un certain rang. Les a_n sont appelés les

coefficients du polynôme. Sur cet ensemble de polynômes, on définit deux lois de composition, une addition et une multiplication. Si $P = (p_0, p_1, \dots)$ et $Q = (q_0, q_1, \dots)$ sont des polynômes à coefficients dans K , on pose

$$P + Q = (p_0 + q_0, p_1 + q_1, \dots) \quad \text{et} \quad PQ = (s_0, s_1, \dots) \quad \text{avec} \quad s_n = \sum_{i+j=n} p_i q_j.$$

On vérifie que cet ensemble est ainsi muni d'une structure d'anneau commutatif. Pour tout $a \in K$, on note a le polynôme $(a, 0, \dots, 0, \dots)$. Posons

$$X = (0, 1, 0, \dots, 0, \dots).$$

Pour tout entier $n \geq 1$, et tout $a \in K$, on vérifie alors que l'on a

$$aX^n = (0, \dots, 0, a, 0, \dots),$$

où le $n + 1$ -ième terme de la suite est a et où tous les autres sont nuls. Avec ces notations, tout polynôme $P = (p_0, p_1, \dots, p_n, 0, \dots)$, dont les coefficients d'indices strictement plus grands que n sont nuls, s'écrit

$$P = p_0 + p_1X + \dots + p_nX^n,$$

qui est la notation polynômiale de P et que l'on utilise exclusivement. On note $K[X]$ l'anneau ainsi obtenu. Bien entendu, on peut désigner le polynôme $(0, 1, 0, \dots)$ par d'autres lettres que X , par exemple Y , Z ou T , pourvu que la lettre choisie n'ait pas été utilisée par ailleurs. Signalons que ces définitions s'étendent directement si K est un anneau commutatif, pas nécessairement un corps.

2. Degré - Division euclidienne

Définissons ce que l'on appelle le degré d'un élément de $K[X]$. Considérons pour cela l'ensemble $\mathbb{N} \cup \{-\infty\}$ obtenu en adjoignant à \mathbb{N} un élément noté $-\infty$, que l'on munit de la structure d'ensemble ordonné qui induit l'ordre usuel sur \mathbb{N} et telle que $-\infty \leq n$ pour tout entier naturel n . Tout ensemble non vide de $\mathbb{N} \cup \{-\infty\}$ possède ainsi un plus petit élément. On prolonge par ailleurs la loi additive de \mathbb{N} à cet ensemble en posant $(-\infty) + n = n + (-\infty) = -\infty$ et $(-\infty) + (-\infty) = -\infty$. On définit alors l'application degré

$$\deg : K[X] \rightarrow \mathbb{N} \cup \{-\infty\},$$

de la façon suivante :

Définition 9.1. Soit $F = (a_i)_{i \geq 0}$ un polynôme à coefficients dans K .

- 1) Si $F = 0$ i.e. si tous les a_i sont nuls, on pose $\deg(F) = -\infty$.
- 2) Si F n'est pas nul, $\deg(F)$ est le plus grand entier $n \geq 0$ tel que $a_n \neq 0$.

On dit que $\deg(F)$ est le degré de F .

Si $F \in K[X]$ est non nul, le coefficient de $X^{\deg(F)}$ est appelé le coefficient dominant de F . C'est le coefficient du terme de plus haut degré de F . S'il vaut 1, le polynôme F est dit unitaire.

Lemme 9.1. Soient P et Q des éléments de $K[X]$.

- 1) On a $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$ avec égalité si $\deg(P) \neq \deg(Q)$.
- 2) On a $\deg(PQ) = \deg(P) + \deg(Q)$.

Démonstration : On vérifie que ces assertions sont vraies si l'un des polynômes P et Q est nul. Supposons P et Q non nuls. Posons

$$P = a_0 + \cdots + a_r X^r \quad \text{et} \quad Q = b_0 + \cdots + b_s X^s \quad \text{avec} \quad a_r \neq 0 \quad \text{et} \quad b_s \neq 0.$$

On a évidemment $\deg(P + Q) \leq \max(r, s)$ avec égalité si $r \neq s$. Par ailleurs, on a une égalité de la forme $PQ = a_r b_s X^{r+s} + R$ où $R \in K[X]$ est de degré $< r + s$. Puisque K est un anneau intègre (c'est un corps), on a $a_r b_s \neq 0$ de sorte que le degré de PQ est $r + s$.

Corollaire 9.1. L'anneau $K[X]$ est intègre et le groupe de ses éléments inversibles est K^* i.e. est l'ensemble des éléments non nuls de K ⁽¹⁾.

Démonstration : L'anneau $K[X]$ n'est pas nul et est commutatif. D'après l'assertion 2 du lemme 9.1, quels que soient P et Q dans $K[X]$, si $PQ = 0$ alors $\deg(P)$ ou bien $\deg(Q)$ vaut $-\infty$, autrement dit, on a $P = 0$ ou bien $Q = 0$, donc $K[X]$ est intègre. Par ailleurs, si $PQ = 1$, on a $\deg(P) + \deg(Q) = 0$, ce qui entraîne $\deg(P) = \deg(Q) = 0$, d'où le résultat.

Le théorème de division euclidienne est le suivant :

Théorème 9.1 (Division euclidienne). Soient A et B des polynômes de $K[X]$ tels que $B \neq 0$. Alors, il existe un unique couple (Q, R) de polynômes de $K[X]$ tel que

$$A = BQ + R \quad \text{avec} \quad \deg R < \deg B.$$

On dit que Q est le quotient et que R est le reste de la division euclidienne de A par B .

Démonstration : On prouve le lemme suivant :

⁽¹⁾ Ce résultat est faux si K est remplacé par un anneau non intègre. Par exemple, le polynôme $F = 2X + 1 \in (\mathbb{Z}/4\mathbb{Z})[X]$ vérifie l'égalité $F^2 = 1$ (on note ici 2 la classe de 2 et 1 la classe de 1 modulo 4 \mathbb{Z}). On a aussi dans cet anneau $(2X)^2 = 0$.

Lemme 9.2. Soient U et V des polynômes de $K[X]$ tels que $V \neq 0$ et $\deg(U) \geq \deg(V)$. Il existe $Q \in K[X]$ tel que l'on ait

$$\deg(U - VQ) < \deg(U).$$

Démonstration : Puisque V est non nul, il en est de même de U . Soient a_k le coefficient dominant de U et b_q celui de V , de sorte que $\deg(U) = k$ et $\deg(V) = q$. On a par hypothèse $k \geq q$. Posons

$$Q = \frac{a_k}{b_q} X^{k-q}.$$

On constate que l'on a $\deg(U - VQ) < \deg(U)$, d'où le lemme.

Le théorème 9.1 se déduit comme suit. Démontrons l'assertion d'existence. On considère l'ensemble

$$S = \{A - BQ \mid Q \in K[X]\}.$$

Le sous-ensemble de $\mathbb{N} \cup \{-\infty\}$ formé des degrés des éléments de S possède un plus petit élément r . Considérons un polynôme $Q \in K[X]$ tel que

$$\deg(A - BQ) = r.$$

Il s'agit de montrer que l'on a $r < \deg(B)$. Supposons le contraire i.e. que $r \geq \deg(B)$. On a $B \neq 0$. Compte tenu du lemme 9.2, il existe $H \in K[X]$ tel que le polynôme

$$A - BQ - HB = A - B(Q + H)$$

soit de degré strictement plus petit que r . Puisque ce polynôme est dans S , le caractère minimal de r conduit alors à une contradiction.

Prouvons l'assertion d'unicité. Soient Q et Q_1 des éléments de $K[X]$ tels que l'on ait

$$\deg(A - BQ) < \deg(B) \quad \text{et} \quad \deg(A - BQ_1) < \deg(B).$$

On déduit de l'assertion 1 du lemme 9.1 que l'on a

$$\deg((A - BQ) - (A - BQ_1)) = \deg(B(Q_1 - Q)) < \deg(B).$$

D'après l'assertion 2 de ce lemme, on a ainsi $\deg(Q_1 - Q) < 0$, ce qui entraîne $Q_1 = Q$ et le résultat⁽²⁾.

⁽²⁾ Cette démonstration montre que le théorème de division euclidienne est aussi valable si l'on remplace K par un anneau commutatif quelconque à condition de supposer que le coefficient dominant de B soit un élément inversible de K .

Exercice 1. Déterminer le quotient et le reste de la division euclidienne de $X^3 + X^2 + 1$ par $X^2 + X + 1$ dans $(\mathbb{Z}/2\mathbb{Z})[X]$.

Définition 9.2. Soient A et B des polynômes de $K[X]$. On dit que B divise A , ou que A est multiple de B , s'il existe $Q \in K[X]$ tel que $A = BQ$. Si $B \neq 0$ cela signifie que le reste de la division euclidienne de A par B est nul.

Lemme 9.3. Soient A et B des polynômes non nuls de $K[X]$ tels que A divise B et que B divise A . Il existe $\lambda \in K$ non nul tel que $A = \lambda B$. On dit alors que A et B sont associés.

Démonstration : Il existe Q et Q_1 dans $K[X]$ tels que $A = BQ$ et $B = AQ_1$, d'où $A(1 - QQ_1) = 0$. Par suite, on a $QQ_1 = 1$, autrement dit Q est inversible, d'où l'assertion (cor. 9.1).

Notation. Étant donné un polynôme $P \in K[X]$, on notera désormais

$$(P) = \{PR \mid R \in K[X]\},$$

l'ensemble des multiples de P dans $K[X]$.

3. Plus grand commun diviseur

Considérons des polynômes A et B de $K[X]$ non tous les deux nuls. Posons

$$I = \{AU + BV \mid U, V \in K[X]\}.$$

Théorème 9.2. Il existe un unique polynôme unitaire $D \in K[X]$ tel que l'on ait

$$I = (D).$$

Démonstration : Il existe D non nul dans I de degré minimum (parmi les éléments non nuls de I). Quitte à multiplier D par un élément convenable de K , on peut supposer que D est unitaire. Vérifions que l'on a $I = (D)$. D'abord tout multiple de D appartient à I . Inversement, soit P un élément de I . D'après le théorème de division euclidienne, il existe Q et R dans $K[X]$ tels que l'on ait $P = QD + R$ avec $\deg(R) < \deg(D)$. Le polynôme $R = P - QD$ appartient à I . Le caractère minimal de D entraîne alors $R = 0$, d'où $P = QD \in (D)$. Cela établit l'assertion d'existence. Considérons alors des polynômes unitaires F et G de $K[X]$ tels que $I = (F) = (G)$. En exprimant le fait que F est dans (G) et que G est dans (F) , on constate que F et G sont associés (lemme 9.3). Puisqu'ils sont unitaires, ils sont égaux.

Définition 9.3. On dit que D est le plus grand commun diviseur de A et B , ou en abrégé, le pgcd de A et B .

Avec cette définition, on a de fait la propriété de Bézout dans $K[X]$, à savoir qu'il existe U et V dans $K[X]$ tels que l'on ait

$$(1) \quad D = AU + BV.$$

Cela étant, il convient de vérifier la propriété attendue du pgcd de deux polynômes :

Théorème 9.3. *Soit F un polynôme unitaire de $K[X]$. Alors, F est le pgcd de A et B si et seulement si les deux conditions suivantes sont vérifiées :*

- 1) *le polynôme F divise A et B .*
- 2) *Tout diviseur de A et B dans $K[X]$ divise F .*

Démonstration : En exprimant le fait que A et B appartiennent à I , on constate que D divise A et B . Par ailleurs, d'après (1), si un polynôme de $K[X]$ divise A et B , alors il divise D . Par suite, D vérifie les conditions 1 et 2. Inversement, soit $F \in K[X]$ réalisant ces conditions. L'égalité (1) et la condition 1 entraînent que F divise D . Puisque D est un diviseur de A et B , d'après la seconde condition D divise F . Les polynômes D et F étant unitaires, ils sont donc égaux.

Définition 9.4. *On dit que A et B sont premiers entre eux, ou que A est premier avec B , si l'on a $D = 1$.*

On a ainsi l'énoncé suivant (égalité (1) et th. 9.3) :

Corollaire 9.2. *Les polynômes A et B sont premiers entre eux si et seulement si il existe U et V dans $K[X]$ tels que $AU + BV = 1$.*

Théorème 9.4 (Gauss). *Soient F , G et H des polynômes de $K[X]$ tels que F divise GH et que F soit premier avec G . Alors, F divise H .*

Démonstration : Il existe $U, V \in K[X]$ tels que $UF + VG = 1$ (cor. 9.2), d'où l'égalité $(UH)F + V(GH) = H$, donc F divise H .

Remarque 9.1. Compte tenu du théorème de division euclidienne, afin de déterminer le pgcd de deux polynômes, et d'obtenir explicitement une relation de Bézout, on peut utiliser, comme dans le cas de l'anneau \mathbb{Z} , l'algorithme d'Euclide.

Exercice 2. Déterminer une relation de Bézout entre les polynômes $(X - 1)^3$ et $(X + 1)^3$ dans $\mathbb{Q}[X]$.

Exercice 3. Soient m et n des entiers naturels non nuls. Montrer que le pgcd des polynômes $X^m - 1$ et $X^n - 1$ est $X^d - 1$ où $d = \text{pgcd}(m, n)$.

4. Plus petit commun multiple

Considérons des polynômes non nuls A et B de $K[X]$. En recopiant la démonstration du théorème 9.2, on obtient :

Théorème 9.5. *Il existe un unique polynôme unitaire $M \in K[X]$ tel que l'on ait*

$$(A) \cap (B) = (M).$$

Remarque 9.2. La notion d'idéal d'un anneau commutatif permet d'expliquer pourquoi les démonstrations des théorèmes 9.2 et 9.5 sont les mêmes.

Définition 9.5. *On dit que M est le plus petit commun multiple de A et B , ou en abrégé, le ppcm de A et B .*

Théorème 9.6. *Soit F un polynôme unitaire de $K[X]$. Alors, F est le ppcm de A et B si et seulement si les deux conditions suivantes sont vérifiées :*

- 1) *le polynôme F est un multiple de A et B .*
- 2) *Tout multiple de A et B dans $K[X]$ est un multiple de F .*

Démonstration : Puisque M appartient à (A) et (B) , le polynôme M est un multiple de A et B . Par ailleurs, si un polynôme de $K[X]$ est multiple de A et B , il est dans (M) , c'est donc un multiple de M . Ainsi M vérifie les conditions 1 et 2. Inversement, soit $F \in K[X]$ un polynôme réalisant ces conditions. On déduit de la condition 1 que F est dans (M) . D'après la condition 2, M est dans (F) . Par suite, on a $(M) = (F)$, puis $F = M$ vu que F et M sont unitaires.

Proposition 9.1. *Soit D le pgcd de A et B . On a $(AB) = (DM)$.*

Démonstration : Il s'agit de démontrer que l'on a

$$\left(\frac{AB}{D^2}\right) = \left(\frac{M}{D}\right).$$

Le polynôme M/D est le ppcm de A/D et B/D (cf. th. 9.6). Par ailleurs, les polynômes A/D et B/D sont premiers entre eux (cor. 9.2). On se ramène ainsi à prouver l'assertion dans le cas où $D = 1$. Supposons donc A et B premiers entre eux et vérifions que l'on a $(AB) = (M)$. Le polynôme AB est un multiple de A et B . Par ailleurs, soit C un multiple de A et B . Compte tenu du théorème 9.6, tout revient à vérifier que C est un multiple de AB . Il existe R et S dans $K[X]$ tels que $C = RA$ et $C = SB$. On a $RA = SB$, donc A divise SB . Puisque A est par hypothèse premier avec B , on déduit du théorème de Gauss que A divise S , d'où le résultat.

5. Polynômes irréductibles

Définition 9.6. Un polynôme de $K[X]$ est dit irréductible (dans $K[X]$ ou sur K) si son degré est supérieur ou égal à 1 et si l'ensemble de ses diviseurs est formé des éléments non nuls de K et des polynômes qui lui sont associés⁽³⁾.

Autrement dit, un polynôme $P \in K[X]$ de degré ≥ 1 est irréductible s'il ne possède pas de diviseur $Q \in K[X]$ tel que $1 \leq \deg(Q) \leq \deg(P) - 1$. Tel est le cas des polynômes de degré 1. Rappelons que ce sont les seuls si K est le corps \mathbb{C} des nombres complexes. Deux polynômes irréductibles de $K[X]$ sont premiers entre eux ou sont associés. Un polynôme qui n'est pas irréductible est dit réductible.

Exercice 4. Montrer que le seul polynôme irréductible de degré 2 dans $(\mathbb{Z}/2\mathbb{Z})[X]$ est $X^2 + X + 1$.

Exercice 5. Soit p un nombre premier. Quel est le nombre de polynômes unitaires de degré 2 dans l'anneau $(\mathbb{Z}/p\mathbb{Z})[X]$? Montrer que le nombre de polynômes irréductibles unitaires de degré 2 dans cet anneau est $\frac{p(p-1)}{2}$.

Exercice 6. Montrer que le polynôme $X^2 - 2$ est irréductible dans $\mathbb{Q}[X]$.

Soit \mathbb{P} l'ensemble des polynômes irréductibles unitaires de $K[X]$. Comme dans le cas de l'anneau \mathbb{Z} , on a le résultat suivant, qui est le théorème fondamental de l'arithmétique de $K[X]$:

Théorème 9.7. Soit P un polynôme non nul de $K[X]$. Alors P s'écrit de manière unique sous la forme

$$(2) \quad P = \lambda \prod_{F \in \mathbb{P}} F^{n_F},$$

où $\lambda \in K$, et où les n_F sont des entiers naturels nuls sauf un nombre fini d'entre eux.

Démonstration : Cet énoncé est vrai si le degré de P est nul, auquel cas on prend $\lambda = P$ et tous les n_F nuls. Considérons alors un entier $n \geq 1$. Supposons que le résultat soit vrai pour tous les polynômes de degré $\leq n - 1$ et que l'on ait $\deg(P) = n$. Soit E l'ensemble de tous les diviseurs de P de degré ≥ 1 . Cet ensemble n'est pas vide car P est dans E . Il existe donc un élément $Q \in E$ de degré minimum. Ce polynôme est irréductible. Il existe $R \in K[X]$ tel que $P = QR$. On a $\deg(R) \leq n - 1$. D'après l'hypothèse de

⁽³⁾ Cette définition est un cas particulier de la notion générale d'élément irréductible dans un anneau commutatif. Si A est un tel anneau, un élément $a \in A$ est dit irréductible s'il n'est pas inversible et si ses seuls diviseurs sont les éléments inversibles et les ua où u est inversible. Les nombres premiers et leurs opposés sont les éléments irréductibles de \mathbb{Z} . À titre indicatif, $2X$ n'est pas irréductible dans $\mathbb{Z}[X]$.

réurrence, R possède une décomposition de la forme (2), et il en est donc de même de P . Cela établit l'assertion d'existence. Vérifions l'assertion d'unicité. Prouvons pour cela le résultat suivant :

Lemme 9.3. *Soit A un polynôme irréductible divisant un produit de polynômes $A_1 \cdots A_r$ dans $K[X]$. Alors, A divise l'un des A_i .*

Démonstration : Supposons le contraire. Puisque A est irréductible, cela signifie que pour tout $i = 1, \dots, r$, les polynômes A et A_i sont premiers entre eux. Il existe donc des polynômes U_i et V_i dans $K[X]$ tels que l'on ait

$$U_i A + V_i A_i = 1 \quad \text{pour } i = 1, \dots, r.$$

Par ailleurs, il existe $R \in K[X]$ tel que l'on ait

$$1 = \prod_{i=1}^r (U_i A + V_i A_i) = RA + \prod_{i=1}^r V_i A_i,$$

ce qui entraîne que A divise 1, et conduit à une contradiction.

Le théorème se déduit comme suit. Supposons que l'on ait deux décompositions de P de la forme (2) :

$$(3) \quad \lambda \prod_{F \in \mathbb{P}} F^{n_F} = \mu \prod_{F \in \mathbb{P}} F^{m_F}.$$

Il résulte du lemme 9.3 que pour tout $F \in \mathbb{P}$, n_F est nul si et seulement si m_F l'est aussi. Considérons alors $F \in \mathbb{P}$ tel que $n_F > 0$. On a donc $m_F > 0$. En divisant les deux membres de (3) par F , on obtient une égalité analogue avec un polynôme de degré $\leq n - 1$. D'après l'hypothèse de récurrence, on a donc $\lambda = \mu$, $n_G = m_G$ pour tout $G \neq F$, et $n_F - 1 = m_F - 1$ i.e. $n_F = m_F$, d'où le théorème.

Comme conséquence des théorèmes 9.3, 9.6 et 9.7, on obtient l'énoncé suivant :

Corollaire 9.3. *Soient P et Q deux polynômes non nuls de $K[X]$. Soient*

$$P = \lambda \prod_{F \in \mathbb{P}} F^{n_F} \quad \text{et} \quad Q = \mu \prod_{F \in \mathbb{P}} F^{m_F},$$

les décompositions de P et Q en produit d'éléments de \mathbb{P} . Soient D et M respectivement le pgcd et le ppcm de P et Q . On a alors

$$D = \prod_{F \in \mathbb{P}} F^{\min(n_F, m_F)} \quad \text{et} \quad M = \prod_{F \in \mathbb{P}} F^{\max(n_F, m_F)}.$$

Pour tout $F \in \mathbb{P}$, on a

$$\text{Min}(n_F, m_F) + \text{Max}(n_F, m_F) = n_F + m_F.$$

On en déduit l'égalité

$$(DM) = (PQ),$$

déjà démontrée (prop. 9.1).

Exercice 7. Déterminer la décomposition en produit de facteurs irréductibles du polynôme $X^4 + 1$ dans $\mathbb{R}[X]$, $(\mathbb{Z}/2\mathbb{Z})[X]$, $(\mathbb{Z}/3\mathbb{Z})[X]$ et $(\mathbb{Z}/5\mathbb{Z})[X]$. On peut en fait démontrer que le polynôme $X^4 + 1$ est réductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$ pour tout nombre premier p , tout en étant irréductible dans l'anneau $\mathbb{Z}[X]$.

6. Racines d'un polynôme

Définition 9.7. Soit $P = a_0 + \dots + a_n X^n$ un polynôme de $K[X]$. On appelle fonction polynôme associée à P l'application $\tilde{P} : K \rightarrow K$ définie par

$$\tilde{P}(x) = \sum_{i=0}^n a_i x^i \quad \text{quel que soit } x \in K^{(4)}.$$

Pour tout $a \in K$ fixé, l'application $K[X] \rightarrow K$ qui à $P \in K[X]$ associe $\tilde{P}(a)$ est un homomorphisme d'anneaux. C'est le morphisme d'évaluation en a . Étant donnés $P \in K[X]$ et $a \in K$, on notera par abus $P(a)$ l'élément $\tilde{P}(a)$.

Définition 9.8. Soient P un polynôme de $K[X]$ et a un élément de K . On dit que a est une racine de P si l'on a $P(a) = 0$.

Lemme 9.4. Soient P un polynôme de $K[X]$ et a un élément de K . On a $P(a) = 0$ si et seulement si $X - a$ divise $P^{(5)}$.

Démonstration : Supposons $P(a) = 0$. D'après le théorème de division euclidienne, il existe Q et R dans $K[X]$ tels que $P = (X - a)Q + R$ avec $\deg(R) < 1$. On a $P(a) = 0$, d'où $R(a) = 0$. Puisque R est un élément de K , on a donc $R = 0$. La réciproque est immédiate.

⁽⁴⁾ On obtient ainsi une application Φ de $K[X]$ à valeurs dans l'ensemble des applications de K dans K , définie par $\Phi(P) = \tilde{P}$. C'est un homomorphisme d'anneaux. Si K est un corps fini, cette application n'est pas injective : par exemple si $K = \mathbb{Z}/p\mathbb{Z}$ où p est premier, pour tout $x \in K$ on a

$$x^p - x = 0,$$

pour autant le polynôme $X^p - X$ n'est pas nul. Si K est infini, on constatera plus loin que Φ est injective.

Remarques 9.3.

1) Un polynôme de $K[X]$ de degré ≥ 2 qui possède une racine dans K est réductible (lemme 9.4). Par ailleurs, les polynômes de $K[X]$ de degré 1 sont irréductibles et cependant ils ont une racine dans K .

2) Soit P un polynôme de $K[X]$ de degré 2 ou 3. Alors, P est irréductible si et seulement si P n'a pas de racines dans K . C'est une conséquence de la remarque ci-dessus et du fait que si $P = AB$ où $A, B \in K[X]$ sont non inversibles, alors le degré de P étant 2 ou 3, on a $\deg(A) = 1$ ou bien $\deg(B) = 1$, de sorte que P a une racine dans K .

3) Il est faux en général que la condition « P n'a pas de racines dans K » entraîne que P soit irréductible, comme le montre le polynôme $(X^2 + 1)^2 \in \mathbb{R}[X]$: il est réductible dans $\mathbb{R}[X]$ et sans racines dans \mathbb{R} .

Exercice 8. Démontrer que les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 ayant un discriminant négatif (on utilisera le fait que tout polynôme à coefficients dans \mathbb{R} possède une racine dans \mathbb{C}).

Si $a \in K$ est une racine de $P \in K[X]$, il importe souvent de connaître la plus grande puissance de $X - a$ qui divise P . Cela conduit à la notion d'ordre de multiplicité.

Définition 9.9 (Ordre de multiplicité d'une racine). Soient P un polynôme non nul de $K[X]$ et $a \in K$ une racine de P . On appelle ordre de multiplicité de a (dans P) le plus grand entier naturel r tel que P soit divisible par $(X - a)^r$. Si $r = 1$, on dit que a est racine simple de P , et si $r \geq 2$, on dit que a est une racine multiple de P .

Afin de calculer r , il convient de définir la notion de polynôme dérivé :

Définition 9.10 (Polynôme dérivé). Soit $P = a_0 + a_1X + \cdots + a_nX^n$ un polynôme de $K[X]$. On appelle polynôme dérivé de P , et on le note P' , le polynôme

$$P' = \sum_{i=1}^n i a_i X^{i-1}.$$

⁽⁵⁾ On peut aussi définir, comme ci-dessus, la notion de racine d'un polynôme à coefficients dans un anneau commutatif K quelconque. Vérifions que cet énoncé est encore valable dans ce cas. Soient P un élément de $K[X]$, a un élément de K , et Y une autre indéterminée. En substituant à X le polynôme $a + Y \in K[Y]$, on obtient dans cet anneau le polynôme

$$P(a + Y) = a_0 + a_1Y + \cdots + a_nY^n$$

avec des $a_i \in K$. On a $P(a) = a_0$, d'où $P(a + Y) = P(a) + YQ(Y)$ où $Q \in K[Y]$. En substituant Y par $X - a$, on a ainsi l'égalité

$$P(X) = P(a) + (X - a)H(X),$$

où $H \in K[X]$. Par suite, si $P(a) = 0$ alors $X - a$ divise P .

En particulier, si $\deg(P) = 0$, on a $P' = 0$. On vérifie que toutes les règles de dérivation usuelles sur les fonctions d'une variable réelle restent valables dans ce contexte. En effet, pour tous P et Q dans $K[X]$, $\lambda \in K$ et $n \geq 1$, on a les relations

$$(P + Q)' = P' + Q', \quad (\lambda P)' = \lambda P', \quad (PQ)' = P'Q + PQ', \quad P^n = nP^{n-1}P'.$$

Proposition 9.2. *Soit P un polynôme de $K[X]$. Pour qu'un élément $a \in K$ soit racine simple de P , il faut et il suffit que l'on ait*

$$P(a) = 0 \quad \text{et} \quad P'(a) \neq 0.$$

Démonstration : Soit a une racine de P . On a $P = (X - a)Q$ où $Q \in K[X]$. Par ailleurs, on a $P' = Q + (X - a)Q'$, d'où $Q(a) = P'(a)$. Si a est une racine simple, on a $Q(a) \neq 0$, d'où $P'(a) \neq 0$. Inversement, si $P'(a) \neq 0$, il en est de même de $Q(a)$. Par suite, $X - a$ ne divise pas Q , ce qui entraîne que $(X - a)^2$ ne divise pas P i.e. que a est racine simple de P .

Exemple 9.1. Soient P un polynôme de $\mathbb{Q}[X]$ de degré n et a une racine de P dans \mathbb{C} d'ordre de multiplicité strictement supérieure à $n/2$. Démontrons que a appartient à \mathbb{Q} . On procède par récurrence sur le degré de P . L'assertion est vérifiée si l'on a $n \leq 1$. Supposons $n \geq 2$ et le résultat vrai pour tous les polynômes de degré au plus $n - 1$. Puisque l'on a $n \geq 2$, la multiplicité de la racine a de P est au moins 2, donc le pgcd de P et de son polynôme dérivé est de degré ≥ 1 . En particulier, P n'est pas irréductible sur \mathbb{Q} . Il existe donc des polynômes Q et R de degrés $\leq n - 1$ tels que $P = QR$. Notons $\nu_P(a)$, $\nu_Q(a)$ et $\nu_R(a)$ les multiplicités de a dans P , Q et R . On a $\nu_P(a) = \nu_Q(a) + \nu_R(a)$ et par hypothèse on a $\nu_P(a) > n/2$. L'égalité $n = \deg(Q) + \deg(R)$ entraîne ainsi $\nu_Q(a) > \deg(Q)/2$ ou bien $\nu_R(a) > \deg(R)/2$. On déduit alors de l'hypothèse de récurrence que a est dans \mathbb{Q} .

Théorème 9.8. *Soient P un polynôme de $K[X]$ et a_1, \dots, a_k des éléments de K , distincts deux à deux, qui sont racines de P d'ordres de multiplicité n_1, \dots, n_k respectivement. Alors, il existe un polynôme $Q \in K[X]$, tel que l'on ait*

$$P = Q \prod_{i=1}^k (X - a_i)^{n_i},$$

et que $Q(a_i)$ soit non nul pour tout $i = 1, \dots, k$.

Démonstration : Procédons par récurrence sur k . L'énoncé est vrai si $k = 1$. Considérons un entier $k \geq 2$ tel que cet énoncé soit vrai pour l'entier $k - 1$. Il existe donc $R \in K[X]$ tel que l'on ait

$$P = R \prod_{i=1}^{k-1} (X - a_i)^{n_i}.$$

Par ailleurs, $(X - a_k)^{n_k}$ divise P et est premier avec le produit des $(X - a_i)^{n_i}$ pour i compris entre 1 et $k - 1$. En effet dans le cas contraire, d'après le lemme 9.3, $X - a_k$ devrait diviser l'un des facteurs $(X - a_i)^{n_i}$ ce qui conduit à une contradiction vu que $a_k \neq a_i$ pour $i = 1, \dots, k - 1$. D'après le théorème de Gauss (th. 9.4), $(X - a_k)^{n_k}$ divise donc R , ce qui entraîne le résultat.

Corollaire 9.4. *Soit P un polynôme non nul de degré n dans $K[X]$. Alors P possède au plus n racines distinctes dans K ⁽⁶⁾.*

Démonstration : Si P possédait (au moins) $n + 1$ racines dans K il serait divisible par un polynôme de $K[X]$ de degré $n + 1$, ce qui contredit le fait que P soit de degré n .

Ce résultat entraîne que l'application Φ de $K[X]$ à valeurs dans l'ensemble des applications de K dans K , définie par l'égalité

$$\Phi(P) = \tilde{P},$$

est injective si K est infini. En effet, si la fonction polynôme \tilde{P} associée à P est nulle sur K , cela signifie que P a une infinité de racines (car K est infini), et d'après le résultat précédent, P doit être le polynôme nul. Par suite, sur un corps infini, on peut identifier $K[X]$ et l'anneau des fonctions polynômes sur K i.e. l'image de Φ .

Comme application de ce qui précède, démontrons le théorème de Wilson (1741-1793), qui est une caractérisation des nombres premiers :

⁽⁶⁾ En fait, ce résultat est encore vrai si l'anneau de base est un anneau intègre quelconque : soit F un polynôme de degré $n \geq 0$ à coefficients dans un anneau intègre A . Alors, F possède au plus n racines dans A . Pour le démontrer, on procède par récurrence sur n . Si $n = 0$, alors F est un élément non nul de A , donc ne possède aucune racine et le résultat est démontré dans ce cas. Supposons F de degré $n \geq 1$ et le résultat démontré pour tous les polynômes de degré $\leq n - 1$. Soit $a \in A$ une racine de F . Il existe $Q \in A[X]$ tel que $F = (X - a)Q$. Le degré de Q est $n - 1$. Par ailleurs, si $b \in A$ est une racine de F distincte de a , on a $(b - a)Q(b) = 0$, d'où $Q(b) = 0$ car A est intègre. Ainsi les racines de F autres que a sont celles de Q . D'après l'hypothèse de récurrence, Q possède au plus $n - 1$ racines dans A , donc F en possède au plus n , d'où le résultat.

En revanche, ce résultat est faux en général si A n'est pas un anneau intègre. On le constate par exemple en considérant le polynôme $(X - 2)(X - 3) \in (\mathbb{Z}/6\mathbb{Z})[X]$, qui est de degré 2, et qui possède quatre racines dans $\mathbb{Z}/6\mathbb{Z}$, à savoir les classes de 0, 2, 3 et 5. Tel est aussi le cas du polynôme $2X \in (\mathbb{Z}/4\mathbb{Z})[X]$ qui possède comme racines les classes de 0 et de 2 modulo 4 \mathbb{Z} . Il existe aussi des anneaux non intègres sur lesquels il existe des polynômes de degré 2 ayant une infinité de racines. En effet, soient E un ensemble infini et A l'anneau formé de l'ensemble des parties de E muni de la différence symétrique Δ et de l'intersection \cap comme addition et multiplication. Rappelons que si U et V sont deux parties de E , on a par définition $U \Delta V = U \cup V - U \cap V$. L'élément neutre additif est l'ensemble vide et l'élément neutre multiplicatif est l'ensemble E . Toute partie U de E est alors racine du polynôme $X^2 + X \in A[X]$, qui a donc une infinité de racines si E est infini : on a ici $U^2 + U = (U \cap U) \Delta U = U \Delta U = \emptyset$.

Théorème 9.9 (Wilson). Soit p un entier ≥ 2 . Alors, p est premier si et seulement si $(p-1)! + 1$ est divisible par p .

Démonstration : Supposons que p soit un nombre premier. Il résulte du petit théorème de Fermat que pour tout a compris entre 1 et $p-1$, l'élément $\bar{a} = a + p\mathbb{Z}$ est racine du polynôme $X^{p-1} - 1 \in (\mathbb{Z}/p\mathbb{Z})[X]$. D'après le théorème 9.8, on en déduit que l'on a dans cet anneau

$$X^{p-1} - 1 = \prod_{a=1}^{p-1} (X - \bar{a}).$$

En exprimant le fait que les termes constants sont les mêmes, on obtient l'égalité dans le corps $\mathbb{Z}/p\mathbb{Z}$

$$-1 = (-1)^{p-1} \prod_{a=1}^{p-1} \bar{a}.$$

Autrement dit, on a la congruence

$$-1 \equiv (-1)^{p-1} (p-1)! \pmod{p},$$

par suite p divise $(p-1)! + 1$. Inversement, supposons $(p-1)! + 1$ divisible par p . Si ℓ est un diviseur positif de p autre que p , alors ℓ divise $(p-1)!$, d'où $\ell = 1$ et le fait que p soit un nombre premier.

Remarques 9.4.

1) Pour démontrer le théorème 9.9 on peut aussi utiliser l'argument suivant. Supposons p premier. Dans le corps $\mathbb{Z}/p\mathbb{Z}$, les seuls éléments égaux à leur inverse sont ± 1 . Il en résulte que l'on a (en regroupant chaque terme du produit avec son inverse modulo p)

$$\prod_{k=2}^{p-2} k \equiv 1 \pmod{p}.$$

Par suite, on a $(p-1)! \equiv p-1 \pmod{p}$ i.e. $(p-1)! + 1 \equiv 0 \pmod{p}$.

2) Le théorème de Wilson est un test de primalité, mais il n'est pas efficace car le calcul de $(p-1)!$ nécessite beaucoup d'opérations. Signalons que si p est un nombre premier, on définit le quotient de Wilson

$$W(p) = \frac{(p-1)! + 1}{p},$$

qui est donc un entier. On dit que p est un nombre premier de Wilson si p divise $W(p)$, autrement dit, si l'on a $(p-1)! + 1 \equiv 0 \pmod{p^2}$. Par exemple, 5 et 13 sont des nombres premiers de Wilson. La question de savoir s'il existe une infinité de tels nombres premiers est ouverte. En dehors de 5 et 13, on ne connaît qu'un seul autre nombre premier de Wilson, à savoir 563 (découvert en 1953). Il n'y en a pas d'autres plus petits que 5.10^8 .

7. Relations entre les coefficients et les racines d'un polynôme

Considérons un polynôme

$$F = u_n X^n + u_{n-1} X^{n-1} + \cdots + u_0$$

de degré $n \geq 1$ à coefficients dans \mathbb{C} . Il possède n racines

$$a_1, \dots, a_n,$$

dans \mathbb{C} , comptées avec leurs ordres de multiplicité. Les relations entre les coefficients et les racines de F sont les suivantes :

Théorème 9.10. *Pour tout $k = 1, \dots, n$, on a l'égalité*

$$\sum_{\{i_1, \dots, i_k\}} a_{i_1} a_{i_2} \cdots a_{i_k} = (-1)^k \frac{u_{n-k}}{u_n},$$

où la somme parcourt toutes les parties à k éléments $\{i_1, \dots, i_k\}$ de l'ensemble $\{1, \dots, n\}$.

Démonstration : On a l'égalité (th. 9.8)

$$F = u_n \prod_{j=1}^n (X - a_j).$$

Dans $\mathbb{C}[X]$, posons

$$(4) \quad \prod_{j=1}^n (X - a_j) = X^n + v_{n-1} X^{n-1} + \cdots + v_0.$$

Le second membre de (4) s'obtient en choisissant dans chaque somme $X - a_j$ l'un des termes X et $-a_j$, en multipliant les termes ainsi choisis, et en effectuant la somme des produits obtenus pour tous les choix possibles. Par suite, le coefficient de X^{n-k} s'obtient en additionnant tous les produits de k éléments parmi les $-a_j$. On a donc

$$v_{n-k} = (-1)^k \sum a_{i_1} a_{i_2} \cdots a_{i_k},$$

où la somme est étendue à toutes les parties à k éléments $\{i_1, \dots, i_k\}$ de $\{1, \dots, n\}$. Le fait que l'on ait $u_{n-k} = u_n v_{n-k}$ entraîne alors le résultat.

Par exemple, avec $k = 1$ et $k = n$, on obtient respectivement les relations

$$\frac{u_{n-1}}{u_n} = - \sum_{j=1}^n a_j \quad \text{et} \quad \frac{u_0}{u_n} = (-1)^n \prod_{j=1}^n a_j.$$

8. Théorème de Mason

Il s'agit de l'énoncé suivant :

Théorème 9.11 (Mason). *Soient P , Q et R des polynômes non nuls dans $\mathbb{C}[X]$, premiers entre eux, dont l'un au moins n'est pas constant, tels que*

$$P + Q + R = 0.$$

Soit s le nombre de racines distinctes de PQR dans \mathbb{C} . Alors, on a

$$\text{Max}(\deg(P), \deg(Q), \deg(R)) < s.$$

Démonstration : Soient P' , Q' et R' les polynômes dérivés de P , Q et R . Posons

$$(5) \quad D = PQ' - P'Q.$$

Vérifions que l'on a $D \neq 0$. Supposons $D = 0$. On a alors $PQ' = P'Q$. Puisque P et Q sont premiers entre eux, il en résulte que P divise P' . Cela entraîne $P' = 0$, puis $Q' = 0$ (car $P \neq 0$) et $R' = 0$, d'où une contradiction. Par ailleurs, on a

$$(6) \quad D = RP' - R'P.$$

On déduit alors de (5) et (6) que si z est une racine d'ordre de multiplicité m de P , de Q ou de R , alors $(X - z)^{m-1}$ divise D . Les polynômes P , Q et R étant premiers entre eux deux à deux, et D étant non nul, on obtient

$$\deg(D) \geq \deg(P) + \deg(Q) + \deg(R) - s.$$

L'inégalité

$$\deg(D) < \deg(P) + \deg(Q),$$

implique alors $\deg(R) < s$. De même, on a $\deg(P) < s$ et $\deg(Q) < s$, d'où le résultat.

Remarque 9.5. L'analogue du théorème de Mason sur \mathbb{Z} n'est pas un théorème, mais une conjecture, appelée la conjecture abc. Elle affirme que pour tout $\varepsilon > 0$, il existe une constante $C(\varepsilon) > 0$ telle que pour tout triplet (a, b, c) d'entiers non nuls, premiers entre eux, vérifiant l'égalité $a + b + c = 0$, on ait

$$\text{Max}(|a|, |b|, |c|) \leq C(\varepsilon) (\text{rad}(abc))^{1+\varepsilon},$$

où $\text{rad}(abc)$ est le produit des nombres premiers divisant abc . Elle entraîne le grand théorème de Fermat (sur \mathbb{Z}) pour les exposants assez grands.

Corollaire 9.5 (Théorème de Fermat sur $\mathbb{C}[X]$). Soit n un entier ≥ 3 . Il n'existe pas de polynômes A, B, C dans $\mathbb{C}[X]$, premiers entre eux, dont l'un au moins soit non constant, vérifiant l'égalité

$$A^n + B^n + C^n = 0.$$

Démonstration : Supposons qu'il existe A, B, C dans $\mathbb{C}[X]$, premiers entre eux, dont l'un au moins soit non constant, tels que $A^n + B^n + C^n = 0$. On a $ABC \neq 0$. Soit s le nombre de racines distinctes de $(ABC)^n$ dans \mathbb{C} i.e. celui de ABC . On a

$$s \leq \deg(A) + \deg(B) + \deg(C) \leq 3 \max(\deg(A), \deg(B), \deg(C)).$$

On déduit alors du théorème de Mason l'inégalité

$$n \max(\deg(A), \deg(B), \deg(C)) < 3 \max(\deg(A), \deg(B), \deg(C)),$$

d'où $n < 3$ et le résultat.

Remarque 9.6. Pour tout polynôme $P \in \mathbb{C}[X]$, en posant

$$A = 1 - P^2, \quad B = 2P \quad \text{et} \quad C = i(1 + P^2),$$

on a $A^2 + B^2 + C^2 = 0$.