17 | Arithmétique dans l'anneau $\mathbb{K}[X]$

Dans l'ensemble de ce chapitre, $\mathbb{K}$ désigne l'un des corps $\mathbb{R}$ ou $\mathbb{C}$.[†]

1 Divisibilité dans $\mathbb{K}[X]$

Les notions et résultats de cette section sont analogues à ceux que vous connaissez concernant les entiers relatifs.

1.1 Relation de divisibilité

Définition 1 – Divisibilité, diviseur, multiple

Soit A et B deux polynômes à coefficients dans $\mathbb{K}$.

- On dit que A *divise* B, ou que A *est un diviseur de* B, ou que B *est divisible par* A ou encore que B *est un multiple de* A lorsqu'il existe un polynôme $C \in \mathbb{K}[X]$ tel que $B = AC$. Cette relation se note $A \mid B$.
- Les polynômes A et B sont dits *associés* lorsque $A \mid B$ et $B \mid A$.

Exemple 2

- Le polynôme $X^2 + X - 6$ est divisible par $X + 3$ car $X^2 + X - 6 = (X + 3)(X - 2)$.
- Le polynôme nul est divisible par tous les polynômes mais il ne divise que lui-même.
- Les polynômes constants et non nuls divisent tous les polynômes.
- Si $A \mid B$ avec B non nul, alors $\deg B \geqslant \deg A$.

  En effet, il existe $C \in \mathbb{K}[X]\backslash\{0\}$ tel que $B = AC$, dont il découle $\deg B = \deg A + \deg C \geqslant \deg A$.

Théorème 3 – Propriétés de la relation de divisibilité

Soit $A, B, C, D \in \mathbb{K}[X]$

(i) Caractérisation des polynômes associés. $A \mid B$ et $B \mid A \iff \exists \lambda \in \mathbb{K}^*, \quad A = \lambda B.$

(ii) Réflexivité et transitivité. La relation de divisibilité $\mid$ est réflexive et transitive sur $\mathbb{K}[X]$.

(iii) Combinaison linéaire. $(D \mid A \text{ et } D \mid B) \implies (\forall U, V \in \mathbb{K}[X], \quad D \mid (AU + BV))$.

(iv) Produit. $(A \mid B \text{ et } C \mid D) \implies AC \mid BD$. En particulier, $A \mid B \implies \big(\forall k \in \mathbb{N}, \quad A^k \mid B^k\big)$.

Démonstration. ... ∎

Remarque 4 La relation de divisibilité restreinte à l'ensemble des polynômes unitaires est une relation d'ordre.

1.2 Division euclidienne

Théorème 5 – Division euclidienne

Soit $A, B \in \mathbb{K}[X]$ avec B NON NUL. Il existe un unique couple de polynômes $(Q, R) \in \mathbb{K}[X]^2$ pour lequel

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

On appelle A le *dividende* de la division euclidienne de A par B, B le *diviseur*, Q le *quotient* et R le *reste*.

Démonstration. ... ∎

†. L'essentiel des résultats de ce chapitre énoncé pour le corps $\mathbb{K}$ reste valable pour un corps quelconque, à l'exception notable du théorème 14, qui lui reste valable pour $\mathbb{K}$ un sous-corps de $\mathbb{C}$.

Remarque 6

- Le polynôme B divise A si et seulement si le reste de la division de A par B est nul.
- Soit $A, B \in \mathbb{R}[X]$ avec B non nul. La propriété d'unicité du quotient et du reste de la division euclidienne permet d'établir que B divise A dans $\mathbb{R}[X]$ si et seulement s'il divise A dans $\mathbb{C}[X]$.

Exemple 7 La division euclidienne de $7X^5 + 4X^4 + 2X^3 - X + 5$ par $X^2 + 2$ donne

$$7X^5 + 4X^4 + 2X^3 - X + 5 = (X^2 + 2)\underbrace{(7X^3 + 4X^2 - 12X - 8)}_{\text{quotient}} + \underbrace{23X + 21}_{\text{reste}}.$$

En particulier, $7X^5 + 4X^4 + 2X^3 - X + 5$ n'est pas divisible par $X^2 + 2$, puisque le reste de la division euclidienne entre ces deux polynômes n'est pas nul.

2 Racines d'un polynôme

2.1 Racines

Lemme 8 – Division euclidienne par $X - \lambda$

Soit $\lambda \in \mathbb{K}$ et $P \in \mathbb{K}[X]$. Le reste de la division euclidienne de P par $X - \lambda$ est $P(\lambda)$.

Démonstration. Par division euclidienne, il existe $Q, R \in \mathbb{K}[X]$ tels que $P = (X - \lambda)Q + R$ et $\deg R < 1$. Ainsi R est un polynôme constant. Il suffit alors d'évaluer en λ : $P(\lambda) = (\lambda - \lambda)Q(\lambda) + R(\lambda) = R$. ■

De ce résultat préliminaire découle la double définition suivante.

Définition 9 – Racine

Soit $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. On dit que λ est une *racine de P (dans $\mathbb{K}$)* lorsque l'une des deux assertions équivalentes suivantes est vérifiée :

(i) $P(\lambda) = 0$. **(ii)** P est divisible par $X - \lambda$.

✖ **Attention !** ✖ La précision « racine dans $\mathbb{K}$ » n'est pas superflue. Par exemple, le polynôme $X^2 + 1$ n'a pas de racine dans $\mathbb{R}$, alors qu'il en a deux dans $\mathbb{C}$, à savoir i et $-i$.

✎ **En pratique** ✎ Via la notion de racine, on ramène souvent les problèmes de divisibilité à des problèmes d'évaluation, et vice versa.

Exemple 10 Pour tout $n \in \mathbb{N}$, le reste de la division euclidienne de X^n par $X^2 - 3X + 2$ vaut $(2^n - 1)X - (2^n - 2)$.

Le résultat suivant permet de circonscrire la recherche d'éventuelles racines « évidentes » d'un polynôme.

Exemple 11 – Racines rationnelles d'un polynôme à coefficients entiers Soit $P = a_n X^n + \ldots + a_1 X + a_0 \in \mathbb{Z}[X]$ et $(p, q) \in \mathbb{Z} \times \mathbb{Z}^*$ avec $p \wedge q = 1$. Si le rationnel p/q est une racine de P, alors $q \mid a_n$ et $p \mid a_0$.

2.2 Multiplicité d'une racine

Définition-théorème 12 – Multiplicité d'une racine

Soit $P \in \mathbb{K}[X]$ non nul et $\lambda \in \mathbb{K}$.

- L'ensemble $\{k \in \mathbb{N} \mid (X - \lambda)^k \text{ divise } P\}$ possède un plus grand élément m appelé la *multiplicité de λ dans P* (on dit aussi que λ *est racine d'ordre m de P*), notée $\text{mult}(P, \lambda)$. En résumé, on dit souvent que m est la plus grande puissance de $X - \lambda$ qui divise P.

  En particulier, dire que λ n'est pas une racine de P revient à dire que λ a pour multiplicité 0 dans P. Une racine est dite *simple* lorsqu'elle est de multiplicité 1, *double* lorsqu'elle est de multiplicité 2, etc.
- Plus concrètement, l'entier m est caractérisé par chacune des deux assertions équivalentes suivantes :
  (i) P est divisible par $(X - \lambda)^m$ mais pas par $(X - \lambda)^{m+1}$.
  (ii) Il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - \lambda)^m Q$ et $Q(\lambda) \neq 0$.

Démonstration. $\mathscr{M} = \left\{k \in \mathbb{N} \mid (X-\lambda)^k \mid P\right\}$ possède un plus grand élément, en tant que partie non vide et majorée de $\mathbb{N}$. En effet, $\mathscr{M}$ est non vide d'une part, puisqu'il contient 0, et est majoré par $\deg P$ d'autre part (cf. exemple 2). ■

Remarque 13

- Si $(X-\lambda)^m$ divise P, alors la multiplicité de λ dans P est SUPÉRIEURE ou égale à m.
- La multiplicité de λ dans P est inférieure ou égale au degré de P (cf. dernier point de l'exemple 2).
- La notion de multiplicité $\text{mult}(P,\lambda)$ est analogue à la notion de valuation p-adique $v_p(n)$ d'un entier non nul n.

La formule de Taylor polynomiale (théorème 34 du chapitre 14) va nous permettre de caractériser la multiplicité d'une racine d'un polynôme par l'annulation des dérivées successives de ce polynôme en cette racine.

Théorème 14 – Multiplicité et dérivées successives

Soit $P \in \mathbb{K}[X]$ non nul (avec $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$), $\lambda \in \mathbb{K}$ et $m \in \mathbb{N}$. Les assertions suivantes sont équivalentes :

(i) λ est de multiplicité m dans P ; **(ii)** $\forall k \in [\![0\,, m-1]\!]$, $P^{(k)}(\lambda) = 0$ ET $P^{(m)}(\lambda) \neq 0$.

Démonstration. ... ■

Exemple 15 La multiplicité de 1 dans $P = X^4 + 3X^3 - 3X^2 - 7X + 6$ est égale à 2.

Exemple 16 Le trinôme du second degré $aX^2 + bX + c$, avec $a, b, c \in \mathbb{K}$ et $a \neq 0$, admet une racine double α si et seulement si $b^2 - 4ac = 0$ et, le cas échéant, $\alpha = -\frac{b}{2a}$.

Remarque 17 Soit $P \in \mathbb{K}[X]$ non nul, $\lambda \in \mathbb{K}$ et $m \in \mathbb{N}$. Si λ est de multiplicité m dans P, alors λ est de multiplicité $m - r$ dans $P^{(r)}$, pour tout $r \in [\![0\,, m]\!]$.

Théorème 18 – Racines complexes d'un polynôme réel

Soit $P \in \mathbb{R}[X]$ non nul – à coefficients RÉELS donc – et $\lambda \in \mathbb{C}$. Alors λ et $\overline{\lambda}$ ont même multiplicité dans P.

Démonstration. P étant à coefficients réels, pour tout $k \in \mathbb{N}$, $P^{(k)}(\overline{\lambda}) = \overline{P^{(k)}(\lambda)}$, la conclusion provient alors du théorème 14. ■

Exemple 19 À quelle condition nécessaire et suffisante sur $n \in \mathbb{N}$ le polynôme $X^2 + 1$ divise-t-il $X^n + 1$?

✎ **En pratique** ✎ Soit $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Nous avons déjà vu (cf. exemple 10) de quelle manière les racines de B peuvent être exploitées lorsque l'on veut déterminer le reste de la division euclidienne de A par B. Le théorème 14 permet de prendre en compte leurs multiplicités respectives.

- Si $B = X(X-1)(X+4)$, la division euclidienne de A par B s'écrit $A = X(X-1)(X+4)Q + aX^2 + bX + c$, avec $Q \in \mathbb{K}[X]$ et $a, b, c \in \mathbb{R}$, et l'évaluation de cette égalité en les racines 0, 1 et -4 fournit un système linéaire d'inconnue a, b, c aisé à résoudre.
- Si $B = (X-2)^3(X+1)$, la division euclidienne de A par B s'écrit $A = (X-2)^3(X+1)Q + aX^3 + bX^2 + cX + d$, avec $Q \in \mathbb{K}[X]$ et $a, b, c, d \in \mathbb{R}$. On n'obtient hélas que deux équations en évaluant en 2 et -1, mais on en obtient deux supplémentaires en exploitant la multiplicité de 2 dans B. En effet, $A'(2) = 12a + 4b + c$ et $A''(2) = 12a + 2b$.

Exemple 20 Pour tout $n \in \mathbb{N}^*$, le reste de la division euclidienne de X^n par $X(X-1)^2$ est $(n-1)X^2 - (n-2)X$.

2.3 Nombre maximal de racines

Lemme 21 – Additivité de la multiplicité d'une racine

Pour tous $P, Q \in \mathbb{K}[X]$ non nuls et $\lambda \in \mathbb{K}$, $\text{mult}(PQ, \lambda) = \text{mult}(P, \lambda) + \text{mult}(Q, \lambda)$.

Démonstration. ... ■

Remarque 22 Ce résultat d'additivité est analogue à celui obtenu pour les valuations p-adiques (théorème 53 du chapitre 13).

Théorème 23 – Factorisation « par les racines »

Soit $P \in \mathbb{K}[X]$ NON NUL et $\lambda_1, \dots, \lambda_r \in \mathbb{K}$ des racines distinctes de P de multiplicités respectives $m_1, \dots, m_r$. Alors $(X-\lambda_1)^{m_1} \cdots (X-\lambda_r)^{m_r}$ divise P. En particulier $\sum_{i=1}^{r} m_i \leqslant \deg P$.

Démonstration. ... ■

Exemple 24 Le polynôme $(X-1)^4X^2(X+2)$ possède en tout trois racines distinctes (1 de multiplicité 4, 0 de multiplicité 2 et -2 de multiplicité 1). On dit en revanche qu'il possède sept *racines comptées avec multiplicité*, puisque $4+2+1=7$.

✎ **En pratique** ✎ Le théorème précédent établit la caractérisation suivante de la divisibilité en termes de multiplicité des racines :

$$\prod_{i=1}^{r}(X-\lambda_i)^{m_i} \mid P \quad \Longleftrightarrow \quad \forall i \in [\![1\,,r]\!], \quad \mathrm{mult}(P,\lambda_i) \geqslant m_i,$$

où les λ_i sont des éléments de $\mathbb{K}$ DISTINCTS, les m_i des entiers naturels non nuls et $P \in \mathbb{K}[X]$ un polynôme non nul.

Le corollaire suivant est souvent utilisé pour montrer qu'un polynôme est nul.

Corollaire 25 – Nombre maximal de racines comptées avec multiplicité

- Un polynôme NON NUL P possède au plus $\deg P$ racines COMPTÉES AVEC MULTIPLICITÉ.
- En particulier, seul le polynôme nul possède une infinité de racines.

Un polynôme de degré n ne possède pas nécessairement n racines comptées avec multiplicité. Nous verrons à la section 4 que c'est le cas si $\mathbb{K}=\mathbb{C}$, mais pas si $\mathbb{K}=\mathbb{R}$. Par exemple, X^2+1 est réel de degré 2, mais n'a pas de racine réelle.

Ces diverses considérations sur le nombre maximal de racines d'un polynôme conduisent au résultat fondamental suivant, décliné sous trois formes équivalentes.

Théorème 26 – Rigidité des polynômes

1. Soit $P \in \mathbb{K}_n[X]$. Si P admet strictement plus de n racines, alors P est nul.
2. Soit $P, Q \in \mathbb{K}_n[X]$. Si P et Q coïncident en strictement plus de n valeurs distinctes, alors $P=Q$.
3. Soit $n \in \mathbb{N}^*$, $x_1, \dots, x_n$ des éléments DISTINCTS de $\mathbb{K}$ et $y_1, \dots, y_n$ des éléments de $\mathbb{K}$ non nécessairement distincts. Il existe au plus un polynôme $P \in \mathbb{K}_{n-1}[X]$ tel que $P(x_i)=y_i$, pour tout $i \in [\![1\,,n]\!]$. Ainsi, sous réserve d'existence, un polynôme de degré au plus $n-1$ est entièrement déterminé par ses valeurs en n points distincts.

Démonstration. Le point **1** est la contraposée du premier point du corollaire 25. Le point **2** est une conséquence de **1** appliqué à $P-Q$. Le point **3** n'est qu'une reformulation de **2**. ■

Remarque 27 Le dernier point du théorème précédent affirme l'unicité sous réserve d'existence d'un polynôme de degré au plus $n-1$ prenant des valeurs données en n points fixés. Il n'est pas difficile de construire explicitement un tel polynôme, fournissant ainsi l'existence, comme nous le verrons à la section 3.

Exemple 28 Soit $P \in \mathbb{R}[X]$. On suppose que, pour tout $n \in \mathbb{N}$, $P(n)=n^3-n^2+1$. Alors $P=X^3-X^2+1$ et, a fortiori, pour tout $z \in \mathbb{C}$, $P(z)=z^3-z^2+1$.

✎ **En pratique** ✎ Comme l'illustre l'exemple précédent, le théorème 26 est un théorème de DÉS-ÉVALUATION. Évaluer consiste à passer d'une égalité polynomiale à une égalité de nombres réels ou complexes. Dés-évaluer, c'est le contraire : remonter d'une collection d'égalités de nombres à une égalité polynomiale. En d'autres termes, lorsqu'un polynôme P est défini par certaines de ses valeurs, il est souvent fructueux d'interpréter cette hypothèse sur les valeurs de P en termes de racines d'un nouveau polynôme Q. Quand ce polynôme Q a trop de racines, il est nécessairement nul et on en tire souvent de précieux renseignement sur P.

Exemple 29 – Polynômes de Tchebychev (un grand classique)
Pour tout $n \in \mathbb{N}$, il existe un unique polynôme $T_n \in \mathbb{R}[X]$ tel que, pour tout $\theta \in \mathbb{R}$, $T_n(\cos\theta) = \cos(n\theta)$.

Exemple 30 Il n'existe pas de polynôme $P \in \mathbb{R}[X]$ tel que, pour tout $n \in \mathbb{N}$, $P(n) = \sqrt[3]{n^2+1}$.

Exemple 31 Soit $P \in \mathbb{R}[X]$ de degré n et tel que, pour tout $k \in [\![1, n+1]\!]$, $P(k) = \dfrac{1}{k}$. Alors $P(-1) = n+1$.

Théorème 32 – Identification polynôme/fonction polynomiale

L'application $P \longmapsto \widetilde{P}$ est un morphisme d'anneaux injectifs de $\mathbb{K}[X]$ dans $\mathbb{K}^{\mathbb{K}}$, dont l'image correspond à l'ensemble des fonctions polynomiales. Ainsi, deux polynômes sont égaux si et seulement si leurs fonctions polynomiales associées le sont.

Démonstration. Si $\widetilde{P} = \widetilde{Q}$, alors $\widetilde{P-Q}$ est nulle sur $\mathbb{K}$. Ainsi, tout élément de $\mathbb{K}$ est racine de $P-Q$, or $\mathbb{K}$ ($\mathbb{R}$ ou $\mathbb{C}$) est infini, $P-Q$ possède donc une infinité de racine et est par conséquent nul. ■

2.4 Polynômes scindés et relations entre coefficients et racines

Définition-théorème 33 – Polynôme scindé

Un polynôme $P \in \mathbb{K}[X]$ est dit *scindé (sur $\mathbb{K}$)* lorsqu'il n'est pas constant et possède exactement $\deg P$ racines (dans $\mathbb{K}$) comptées avec multiplicité, ce qui équivaut à dire que P est de la forme $\alpha \prod_{i=1}^{r} (X-\lambda_i)^{m_i}$, où $\lambda_1, \dots, \lambda_r$ sont les racines distinctes de P dans $\mathbb{K}$, de multiplicités respectives $m_1, \dots, m_r$, et où α est son coefficient dominant.

Démonstration. Si P est scindé sur $\mathbb{K}$, alors $\prod_{i=1}^{r}(X-\lambda_i)^{m_i}$ divise P (théorème 23). Ainsi $P = Q\prod_{i=1}^{r}(X-\lambda_i)^{m_i}$, avec $Q \in \mathbb{K}[X]$. Or $\deg Q = \deg P - \deg\left(\prod_{i=1}^{r}(X-\lambda_i)^{m_i}\right) = 0$, ainsi $Q \in \mathbb{K}$ et, comme $\prod_{i=1}^{r}(X-\lambda_i)^{m_i}$ est unitaire, Q est égal au coefficient dominant de P. ■

✖ **Attention !** ✖ La précision « scindé sur $\mathbb{K}$ » n'est pas superflue puisqu'un polynôme peut avoir des racines complexes mais aucune racine réelle, *e.g.* $X^2+1 = (X-i)(X+i)$ est scindé sur $\mathbb{C}$, mais pas sur $\mathbb{R}$.

Exemple 34 Les polynômes de degré 1 sont scindés.
En effet, P est non constant de la forme $aX+b$, avec $a, b \in \mathbb{K}$ et $a \neq 0$, et admet $-b/a$ pour racine dans $\mathbb{K}$.

Exemple 35 Pour tout $n \in \mathbb{N}^*$, le polynôme $X^n - 1$ est scindé sur $\mathbb{C}$. Précisément : $X^n - 1 = \prod_{k=0}^{n-1}\left(X - \mathrm{e}^{\frac{2ik\pi}{n}}\right)$.
En effet, le polynôme X^n-1 n'est pas constant et admet au plus n racines, étant de degré n. Or X^n-1 admet les n racines n^{es} de l'unité pour racines distinctes. Enfin, X^n-1 est unitaire.

Un polynôme possède-t-il toujours une racine ? Le théorème majeur suivant apporte une réponse affirmative à cette question en lien avec le corps $\mathbb{C}$.

Théorème 36 – Théorème de d'Alembert-Gauss[†]

Tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine complexe.[‡]

Démonstration. Admis, conformément au programme. Cf. annexe A pour une démonstration. ■

†. Jean Le Rond d'Alembert (1717 à Paris – 1783 à Paris) est un mathématicien, physicien, philosophe et encyclopédiste français qui a notamment dirigé avec Denis Diderot l'édition entre 1751 et 1772 de l'*Encyclopédie ou Dictionnaire raisonné des sciences, des arts et des métiers*, première encyclopédie française.
Johann Carl Friedrich Gauss (1777 à Brunswick – 1855 à Göttingen) est un mathématicien, astronome et physicien allemand, dont la contribution aux mathématiques est extraordinaire.
‡. Le corps $\mathbb{C}$ est dit *algébriquement clos*.

✖ **Attention !** ✖ Ce théorème est naturellement faux sur $\mathbb{R}$, *e.g.* le polynôme X^2+1 n'a pas de racine réelle.

Corollaire 37

Tout polynôme non constant de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$.

Démonstration. On procède par récurrence sur le degré des polynômes, en établissant pour $n \geqslant 1$ la propriété

$$\mathscr{P}(n) : \text{« } \forall P \in \mathbb{K}[X], \quad (\deg P = n \implies P \text{ est sindé) ».}$$

L'initialisation a été vue à l'exemple 34 et l'hérédité découle du théorème de d'Alembert-Gauss. ∎

Relations entre coefficients et racines Dans l'ensemble de ce paragraphe, on considère

$$P = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 = a_n \prod_{i=1}^{n} (X - x_i),$$

un polynôme de degré n scindé sur $\mathbb{K}$, en particulier $a_n \neq 0$.

Définition 38 – Fonctions symétriques élémentaires

Pour tout $r \in [\![1\,,n]\!]$, on définit la r^e *fonction symétrique élémentaire* en les racines du polynôme P par

$$\sigma_r = \sum_{1 \leqslant i_1 < \cdots < i_r \leqslant n} x_{i_1} \cdots x_{i_r}.$$

Exemple 39 $\sigma_1 = \sum_{i=1}^{n} x_i = x_1 + \ldots + x_n$, $\sigma_2 = \sum_{1 \leqslant i < j \leqslant n} x_i x_j = x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n$, et $\sigma_n = \prod_{i=1}^{n} x_i = x_1 x_2 \cdots x_n$.

Exemple 40

- Pour $n = 2$,
$$P = a_2X^2 + a_1X + a_0 = a_2(X - x_1)(X - x_2) = a_2X^2 - a_2(x_1 + x_2)X + a_2x_1x_2$$
et il y a deux fonctions symétriques élémentaires qui vérifient
$$\sigma_1 = x_1 + x_2 = -\frac{a_1}{a_2} \qquad \text{et} \qquad \sigma_2 = x_1x_2 = \frac{a_0}{a_2}.$$
Il s'agit des relations coefficients/racines pour le trinôme du second degré annoncées au chapitre 6.
- Pour $n = 3$,
$$\begin{aligned} P = a_3X^3 + a_2X^2 + a_1X + a_0 &= a_3(X - x_1)(X - x_2)(X - x_3) \\ &\ldots = a_3X^3 - a_3(x_1 + x_2 + x_3)X^2 + a_3(x_1x_2 + x_1x_3 + x_2x_3)X - a_3x_1x_2x_3 \end{aligned}$$
et il y a trois fonctions symétriques élémentaires qui vérifient
$$\sigma_1 = x_1 + x_2 + x_3 = -\frac{a_2}{a_3}, \qquad \sigma_2 = x_1x_2 + x_1x_3 + x_2x_3 = \frac{a_1}{a_3} \qquad \text{et} \qquad \sigma_3 = x_1x_2x_3 = -\frac{a_0}{a_3}.$$

En toute généralité, les formules de Viète† permettent d'exprimer les fonctions symétriques élémentaires en les racines d'un polynôme scindé en fonction de ses coefficients.

Théorème 41 – Formules de Viète

Pour tout $r \in [\![1\,,n]\!]$, $\sigma_r = (-1)^r \dfrac{a_{n-r}}{a_n}$. En particulier,

$$\sigma_1 = \sum_{i=1}^{n} x_i = -\frac{a_{n-1}}{a_n} \quad \text{(somme des racines)} \qquad \text{et} \qquad \sigma_n = \prod_{i=1}^{n} x_i = (-1)^n \frac{a_0}{a_n} \quad \text{(produit des racines).}$$

†. François Viète (1540 à Fontenay-le-Comte (Vendée) – 1603 à Paris) est un mathématicien français. Il mena ses recherches mathématiques en parallèle de ses charges publiques de maître des requêtes au parlement de Rennes, sous Charles IX, puis de maître des requêtes ordinaires de l'hôtel du roi, sous Henri III. Viète est l'un des premiers cryptologues à systématiser l'art de casser les codes.

Démonstration. On généralise la preuve des cas $n=2$ et $n=3$ de l'exemple 40 en remarquant que

$$P = a_n \prod_{i=1}^{n}(X-x_i) = a_n\big(X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \sigma_3 X^{n-3} + \ldots + (-1)^n \sigma_n\big),$$

ce qui mène au résultat par identification des coefficients. ∎

Remarque 42 Plus généralement, on peut démontrer que toute expression polynomiale symétrique en les racines d'un polynôme peut s'exprimer comme un polynôme à coefficients dans $\mathbb{K}$ en les fonctions symétriques élémentaires et donc en les coefficients du polynôme.

Exemple 43 Si x_1, x_2, x_3 sont les trois racines complexes de l'équation $x^3 + px + q = 0$, avec $p, q \in \mathbb{C}$, alors

$$x_1^2 + x_2^2 + x_3^2 = (x_1+x_2+x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3) = \sigma_1^2 - 2\sigma_2 = -2p.$$

Exemple 44 Pour tout $n \geqslant 2$, $\displaystyle\sum_{k=0}^{n-1} \mathrm{e}^{2ik\pi/n} = \sum_{\omega\in\mathbb{U}_n} \omega = 0$ et $\displaystyle\prod_{k=0}^{n-1} \mathrm{e}^{2ik\pi/n} = \prod_{\omega\in\mathbb{U}_n} \omega = (-1)^{n+1}$.

En effet, pour le polynôme scindé $X^n - 1$ (cf. exemple 35), $\sigma_1 = \displaystyle\sum_{\omega\in\mathbb{U}_n} \omega$ et $\sigma_n = \prod_{\omega\in\mathbb{U}_n} \omega$. Or les coefficients des termes de degré $n-1$ et 0 valent respectivement 0 et -1, d'où $\sigma_1 = (-1)^1 \dfrac{0}{1} = 0$ et $\sigma_n = (-1)^n \dfrac{-1}{1} = (-1)^{n+1}$.

3 Polynômes d'interpolation de Lagrange

Position du problème. On recherche un polynôme de degré au plus n coïncidant en $n+1$ points distincts avec une fonction f ou, de façon équivalente, prenant en $n+1$ points distincts $x_0, \ldots, x_{n+1}$, $n+1$ valeurs (non nécessairement distinctes) imposées $y_0, \ldots, y_n$.

La stratégie que nous allons développer consiste à commencer par le cas où les valeurs imposées sont toutes nulles, sauf une égale à 1. Le cas général s'en déduira par combinaison linéaire.

Définition-théorème 45 – Polynômes de Lagrange d'une famille de points

Soit $x_0, \ldots, x_n \in \mathbb{K}$ DISTINCTS. Pour tout $i \in [\![0, n]\!]$, on définit le i^e *polynôme de Lagrange*[‡] associé aux points $x_0, \ldots, x_n$ par

$$L_i = \prod_{\substack{0\leqslant j\leqslant n \\ j\neq i}} \frac{X - x_j}{x_i - x_j}.$$

Propriété fondamentale. Pour tous $i, j \in [\![0, n]\!]$, $L_i(x_j) = \delta_{i,j}$.

En particulier, L_i est de degré n et scindé sur $\mathbb{K}$ (ses racines sont $x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ (mais pas x_i)).

Démonstration. Simples vérifications. ∎

Exemple 46 Pour $n=2$, $L_0 = \dfrac{(X-x_1)(X-x_2)}{(x_0-x_1)(x_0-x_2)}$, $L_1 = \dfrac{(X-x_0)(X-x_2)}{(x_1-x_0)(x_1-x_2)}$ et $L_2 = \dfrac{(X-x_0)(X-x_1)}{(x_2-x_0)(x_2-x_1)}$.

Théorème 47 – Polynôme d'interpolation de Lagrange

Soit $x_0, \ldots, x_n \in \mathbb{K}$ DISTINCTS et $y_0, \ldots, y_n \in \mathbb{K}$ quelconques. Il existe alors un et un seul polynôme P dans $\mathbb{K}_n[X]$ tel que, pour tout $i \in [\![0, n]\!]$, $P(x_i) = y_i$, en l'occurrence $P = \displaystyle\sum_{i=0}^{n} y_i L_i$.

Démonstration. ... ∎

Exemple 48 Considérons $f : x \longmapsto \sin\dfrac{x\pi}{2}$ sur $[0\,,4]$, pour laquelle $f(0) = f(2) = f(4) = 0$, $f(1) = 1$ et $f(3) = -1$, et notons $L_0, \dots, L_4$ les cinq polynômes de Lagrange associés aux points $0, \dots, 4$. Le polynôme d'interpolation de Lagrange de f aux points $0, \dots, 4$ est donc le polynôme $\displaystyle\sum_{i=0}^{4} f(i)L_i = L_1 - L_3$. Or

$$L_1 = -\frac{X(X-2)(X-3)(X-4)}{6}, \quad L_3 = -\frac{X(X-1)(X-2)(X-4)}{6} \quad \text{et} \quad L_1 - L_3 = \frac{X(X-2)(X-4)}{3}.$$

Corollaire 49 – Description de l'ensemble des polynômes interpolateurs

Avec les notations du théorème 47, les polynômes $Q \in \mathbb{K}[X]$ tels que $Q(x_i) = y_i$, pour tout $i \in [\![0\,,n]\!]$, sont exactement les polynômes de la forme $\displaystyle\sum_{i=0}^{n} y_i L_i + R\prod_{i=0}^{n}(X - x_i)$, R décrivant $\mathbb{K}[X]$.

Démonstration. ... ■

4 Polynômes irréductibles dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$

Définition 50 – Polynôme irréductible

Un polynôme P de $\mathbb{K}[X]$ est dit *irréductible (sur $\mathbb{K}$)* lorsqu'il est non constant et lorsque ses seuls diviseurs sont les éléments de $\mathbb{K}^*$ et les associés de P, autrement dit P est non constant et vérifie

$$\forall A, B \in \mathbb{K}[X], \quad [P = AB \implies (\deg A = 0 \text{ ou } \deg B = 0)].$$

Exemple 51

- Tout polynôme de degré 1 est irréductible, le produit de deux polynômes non constants étant au moins de degré 2.
- Un polynôme irréductible dans $\mathbb{K}[X]$ possédant une racine $\alpha \in \mathbb{K}$ est de degré 1. En effet, il est divisible par le polynôme non constant $X - \alpha$ qui lui est donc associé.
- Un polynôme qui n'admet pas de racine dans $\mathbb{K}$ n'est pas nécessairement irréductible dans $\mathbb{K}[X]$, comme le prouve l'exemple de $\left(X^2+1\right)^2$ dans $\mathbb{R}[X]$.
- En revanche un polynôme de degré 2 ou 3 qui n'a pas de racine dans $\mathbb{K}$ est irréductible dans $\mathbb{K}[X]$, puisqu'une décomposition non triviale d'un tel polynôme utilise nécessairement un polynôme de degré 1 qui a donc une racine.
- Un polynôme de $\mathbb{R}[X]$ de degré 2 est donc irréductible dans $\mathbb{R}[X]$ si, et seulement si, son discriminant est strictement négatif.

Remarque 52 Soit $P, Q \in \mathbb{K}[X]$. Si P est irréductible et si Q est non constant et divise P, alors P et Q sont associés.

Définition 53 – Factorisation irréductible

On appelle *factorisation irréductible sur* $\mathbb{K}$ d'un polynôme non nul de $\mathbb{K}[X]$ toute écriture de P sous la forme d'un produit d'un élément de $\mathbb{K}^*$ et d'un nombre fini de polynômes irréductibles unitaires sur $\mathbb{K}$.

Remarque 54 Nous allons voir que tout polynôme non nul de $\mathbb{K}[X]$ admet une et une seule factorisation irréductible sur $\mathbb{K}$ (cf. théorèmes 56 et 58). Les polynômes irréductibles de l'anneau $\mathbb{K}[X]$ sont ainsi les analogues des nombres premiers dans l'anneau $\mathbb{Z}$.

‡. Joseph Louis de Lagrange (1736 à Turin – 1813 à Paris) est un mathématicien, mécanicien et astronome, originaire du royaume de Sardaigne et naturalisé français. À l'âge de trente ans, il quitte Turin et va séjourner à Berlin pendant vingt-et-un ans. Ensuite, il s'installe pour ses vingt-six dernières années à Paris où il prend la nationalité française en 1802. Fondateur du calcul des variations, avec Euler, et de la théorie des formes quadratiques, il démontre notamment la conjecture de Bachet : tout entier positif est somme de quatre carrés.

4.1 Factorisation irréductible dans $\mathbb{C}[X]$

Les théorèmes suivants sont des corollaires du théorème de d'Alembert-Gauss.

Théorème 55 – Irréductibles de $\mathbb{C}[X]$

Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Démonstration. Clair d'après les deux premiers points de l'exemple 51. ■

Théorème 56 – Factorisation irréductible dans $\mathbb{C}[X]$

Tout polynôme non constant de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$ et sa factorisation irréductible coïncide avec cette forme scindée, en particulier elle est unique à l'ordre près des facteurs. Précisément, tout polynôme P non constant de $\mathbb{C}[X]$ s'écrit

$$P = \alpha \prod_{k=1}^{r} (X - \lambda_k)^{m_k}$$

où les λ_k sont les racines distinctes de P de multiplicités respectives m_k et α son coefficient dominant.

Démonstration. L'existence d'une telle factorisation découle directement du corollaire 37 et son unicité de la notion de multiplicité d'une racine. ■

✎ **En pratique** ✎ Factoriser un polynôme de $\mathbb{C}[X]$ équivaut à déterminer ses racines dans $\mathbb{C}$.

4.2 Factorisation irréductible dans $\mathbb{R}[X]$

Théorème 57 – Irréductibles de $\mathbb{R}[X]$

Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant strictement négatif, *i.e.* sans racine réelle.

Démonstration. D'après l'exemple 51, les polynômes de $\mathbb{R}[X]$ de degré 1, ou de degré 2 et de discriminant strictement négatif sont irréductibles. Montrons qu'il s'agit des seuls.

Soit $P \in \mathbb{R}[X]$ un polynôme irréductible. En particulier, P est non constant et admet donc une racine $\lambda \in \mathbb{C}$ (théorème de d'Alembert-Gauss).

- Si $\lambda \in \mathbb{R}$, alors $X - \lambda$ divise P. Or P est irréductible, ainsi P et $X - \lambda$ sont associé et P est donc de degré 1.
- Si $\lambda \notin \mathbb{R}$, alors $\overline{\lambda}$ est aussi racine de P, car P est à coefficients réels (théorème 18). Ainsi $(X - \lambda)(X - \overline{\lambda})$ divise P, or

$$(X - \lambda)(X - \overline{\lambda}) = X^2 - 2\,\mathrm{Re}(\lambda)X + |\lambda|^2 \in \mathbb{R}[X].$$

  À nouveau, P étant irréductible, P et $X^2 - 2\,\mathrm{Re}(\lambda)X + |\lambda|^2$ sont associé et P est donc de degré 2 et sans racine réelle, *i.e.* de discriminant strictement négatif. ■

Théorème 58 – Factorisation irréductible dans $\mathbb{R}[X]$

La factorisation irréductible d'un polynôme non constant P de $\mathbb{R}[X]$ est unique, à l'ordre près des facteurs. Précisément, elle est de la forme

$$P = \alpha \prod_{i=1}^{r} (X - \lambda_i)^{m_i} \times \prod_{j=1}^{s} \left(X^2 + b_j X + c_j\right)^{n_j},$$

avec
- α le coefficient dominant de P ;
- $\lambda_1, \dots, \lambda_r$ les racines réelles distinctes de P, de multiplicités respectives $m_1, \dots, m_r$;
- $X^2 + b_j X + c_j$ des polynômes distincts et irréductibles sur $\mathbb{R}$ et $n_j \in \mathbb{N}^*$, pour tout $j \in [\![1\,,s]\!]$.

Démonstration. Soit $P \in \mathbb{R}[X]$ un polynôme non constant. Puisque P est à coefficients réels, ses racines non réelles peuvent être regroupées par paires de conjuguées de mêmes multiplicités (théorème 18). Ainsi, P étant scindé sur $\mathbb{C}$,

$$P = \alpha \prod_{i=1}^{r} (X - \lambda_i)^{m_i} \times \prod_{j=1}^{s} (X - \omega_j)^{n_j} (X - \overline{\omega}_j)^{n_j},$$

avec α le coefficient dominant de P, λ_k les racines réelles de P, et ω_k et $\overline{\omega}_k$ les racines complexes conjuguées. Or, pour tout $j \in [\![1\,,s]\!]$,

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

et ce trinôme à coefficients réels est de discriminant strictement négatif. Enfin cette factorisation sur $\mathbb{R}$ est unique, car dans le cas contraire P aurait plusieurs formes scindées sur $\mathbb{C}$, ce qui est exclu. ■

✎ **En pratique** ✎ La factorisation irréductible sur $\mathbb{R}$ d'un polynôme de $\mathbb{R}[X]$ se déduit de sa forme scindée sur $\mathbb{C}$ par regroupement des racines non réelles par paires de conjuguées.

Exemple 59 – Factorisation/développement classique Pour tout $\theta \in \mathbb{R}$, $\left(X-\mathrm{e}^{i\theta}\right)\left(X-\mathrm{e}^{-i\theta}\right) = X^2 - 2\cos(\theta)X + 1$. En particulier, le polynôme $X^2 - 2\cos(\theta)X + 1$ est irréductible sur $\mathbb{R}$ lorsque $\theta \not\equiv 0\,[\pi]$.

Exemple 60 Pour factoriser X^5+1 sur $\mathbb{R}$, on commence par le factoriser sur $\mathbb{C}$:

$$X^5+1 = \left(X-\mathrm{e}^{i\pi/5}\right)\left(X-\mathrm{e}^{3i\pi/5}\right)(X+1)\left(X-\mathrm{e}^{7i\pi/5}\right)\left(X-\mathrm{e}^{i9\pi/5}\right)$$

puis on regroupe les facteurs conjugués :

$$\begin{aligned} X^5+1 &= (X+1)\Big(\left(X-\mathrm{e}^{i\pi/5}\right)\left(X-\mathrm{e}^{i9\pi/5}\right)\Big)\Big(\left(X-\mathrm{e}^{3i\pi/5}\right)\left(X-\mathrm{e}^{7i\pi/5}\right)\Big) \\ &= (X+1)\Big(X^2-2\cos\frac{\pi}{5}X+1\Big)\Big(X^2-2\cos\frac{3\pi}{5}X+1\Big). \end{aligned}$$

✖ **Attention !** ✖ En dépit des apparences $(X+1)\left(X^2-3X+2\right)^2$ n'est pas la factorisation irréductible de ce polynôme sur $\mathbb{R}$, car $X^2-3X+2 = (X-1)(X-2)$ (ce trinôme n'est pas de discriminant strictement négatif).

5 PGCD et PPCM

Les énoncés de cette section sont largement analogues à ceux du chapitre *Arithmétique dans* $\mathbb{Z}$. Certaines démonstrations seront donc omises.

5.1 PGCD de deux polynômes, algorithme d'Euclide

Soit A et B deux polynômes dont l'un au moins est non nul. L'ensemble $\{\deg D \mid D \text{ divise } A \text{ et } B\}$ est une partie non vide (elle contient 0, car 1 divise A et B) et majorée de $\mathbb{N}$ (par le degré de A ou de B), il possède donc un plus grand élément. Ceci légitime la définition suivante.

Définition 61 – PGCD de deux polynômes

- Soit A et B deux polynômes dont l'un au moins est non nul. On appelle *plus grand commun diviseur (ou PGCD) de A et B* tout diviseur commun de A et B de degré maximal.
- Par convention, 0 est le seul PGCD de 0 et 0, et on note $0 \wedge 0 = 0$.

Exemple 62 Pour tout $A \in \mathbb{K}[X]$, les PGCD de A et 0 sont exactement les associés de A.

En effet, si A est non nul, les diviseurs communs de A et 0 sont les diviseurs de A, or les diviseurs de A de degré maximal sont ses associés.

Le principe à la base de l'algorithme d'Euclide subsiste.

Théorème 63 – Principe à la base de l'algorithme d'Euclide

Pour tous $A, B, K \in \mathbb{K}[X]$, $A+KB$ et B ont les mêmes diviseurs communs que A et B, et donc aussi les mêmes PGCD.

Algorithme d'Euclide L'*algorithme d'Euclide* s'adapte *mutatis mutandis* à deux polynômes de $\mathbb{K}[X]$ et fournit un algorithme de calcul effectif du PGCD. Précisément, étant donnés deux polynômes A et B de $\mathbb{K}[X]$, définissons une suite de polynômes R_k par

- $R_0 = A$ et $R_1 = B$;
- pour tout $k \in \mathbb{N}$, tant que $R_{k+1} \neq 0$, R_{k+2} est le reste de la division euclidienne de R_k par R_{k+1}.

Lors de la deuxième étape, si $R_{k+1} \neq 0$, on a par construction $\deg R_{k+2} < \deg R_{k+1}$. La suite des degrés des polynômes ainsi construite est strictement décroissante à partir du rang 1 et à valeurs dans $\mathbb{N}$, il existe donc un rang N tel que $R_N \neq 0$ et $R_{N+1} = 0$, ce qui assure la terminaison de l'algorithme.

Par ailleurs, d'après le théorème précédent, les diviseurs communs de A et B sont ceux de R_1 et R_2, puis de R_2 et R_3, ..., et enfin de R_N et R_{N+1}, donc les diviseurs de R_N, puisque $R_{N+1} = 0$. Ainsi les diviseurs communs de A et B sont exactement les diviseurs de R_N et leurs PGCD sont donc les associés de R_N (cf. exemple 62). En particulier, les PGCD de A et B sont associés.

Théorème 64 – « Unicité » du PGCD de deux polynômes, lien avec les diviseurs communs

Soit $A, B \in \mathbb{K}[X]$.

- Les PGCD de A et B sont associés. Si A ou B est non nul, un seul de ces PGCD est unitaire, on l'appelle *le PGCD de A et B* et on le note $A \wedge B$.
- Les diviseurs communs de A et B sont les diviseurs de $A \wedge B$.

Bilan : À une constante multiplicative près, $A \wedge B$ est le dernier reste non nul obtenu dans la suite des divisions successives des restes R_k de l'algorithme d'Euclide.

Algorithme d'Euclide étendu L'algorithme d'Euclide étendu s'adapte *mutatis mutandis* à deux polynômes de $\mathbb{K}[X]$. Précisément, étant donnés deux polynômes A et B de $\mathbb{K}[X]$, définissons des suites de polynômes R_k, U_k et V_k par

- $R_0 = A$, $U_0 = 1$ et $V_0 = 0$;
- $R_1 = B$, $U_1 = 0$ et $V_1 = 1$;
- pour tout $k \in \mathbb{N}$, tant que $R_{k+1} \neq 0$, on considère R_{k+2} et Q_{k+2} le reste et le quotient de la division euclidienne de R_k par R_{k+1}, ainsi $R_{k+2} = R_k - Q_{k+2}R_{k+1}$, et on pose

$$U_{k+2} = U_k - Q_{k+2}U_{k+1} \quad \text{et} \quad V_{k+2} = V_k - Q_{k+2}V_{k+1}.$$

Considérons le rang N tel que $R_N \neq 0$ et $R_{N+1} = 0$ (cf. algorithme d'Euclide), une récurrence double sur $k \in [\![0, N]\!]$ permet alors d'établir la propriété

$$\mathscr{P}(k) : \text{« } R_k = AU_k + BV_k \text{ ».}$$

En particulier, au rang N, $A \wedge B$ et $R_N = AU_N + BV_N$ sont associés, ce qui démontre le théorème fondamental suivant.

Théorème 65 – Relations de Bézout

Soit $A, B \in \mathbb{K}[X]$. Il existe deux polynômes $U, V \in \mathbb{K}[X]$ tels que $AU + BV = A \wedge B$. Une telle relation est appelée *une relation de Bézout de A et B de coefficients U et V*.

✖ ATTENTION ! ✖ Comme dans $\mathbb{Z}$, il n'y a pas unicité des polynômes U et V.

Exemple 66 Déterminons le PGCD et une relation de Bézout des polynômes $A = 6X^4 + 8X^3 - 7X^2 - 5X - 2$ et $B = 6X^3 - 4X^2 - X - 1$.

En effet, $A \wedge B = X - 1 = -(3X + 1)A + \big(3X^2 + 7X + 3\big)B$, puisque

k	R_k	Q_k	U_k	V_k
0	$6X^4 + 8X^3 - 7X^2 - 5X - 2$		1	0
1	$6X^3 - 4X^2 - X - 1$		0	1
2	$2X^2 - 2X$	$X + 2$	1	$-X - 2$
3	$X - 1$	$3X + 1$	$-3X - 1$	$3X^2 + 7X + 3$

$$A = \underbrace{(X+2)}_{q_2} \times B + \underbrace{2X^2 - 2X}_{r_2}$$
$$B = \underbrace{(3X+1)}_{q_3} \times \big(2X^2 - 2X\big) + \underbrace{X - 1}_{r_3}$$
$$2X^2 - 2X = \underbrace{2X}_{q_4} \times (X - 1) + \underbrace{0}_{r_4}$$

Théorème 67 – Propriétés du PGCD de deux polynômes

Soit A, B, C, K des polynômes à coefficients dans $\mathbb{K}$.

(i) Associativité. $(A \wedge B) \wedge C = A \wedge (B \wedge C)$.

(ii) Factorisation par un diviseur commun. $(KA) \wedge (KB)$ et $K(A \wedge B)$ sont associés.

✎ **En pratique** ✎ Si l'on connaît la factorisation irréductible de deux polynômes non nuls de $\mathbb{K}[X]$, on peut déterminer leur PGCD sans recourir à l'algorithme d'Euclide. Le principe est le même que dans $\mathbb{Z}$ (cf. théorème 58 du chapitre 13).

Exemple 68 $\big[2X(X+1)^2(X+2)^3\big] \wedge \big[X(X+2)^4\big(X^2+1\big)\big] = X(X+2)^3$.

5.2 PGCD d'une famille finie de polynômes

Définition-théorème 69 – PGCD d'une famille finie de polynômes

Soit $A_1, \dots, A_r \in \mathbb{K}[X]$ des polynômes dont l'un au moins est non nul.

- On appelle *plus grand commun diviseur (ou PGCD) de* $A_1, \dots, A_r$ tout diviseur commun de $A_1, \dots, A_r$ de degré maximal.
- Les PGCD de $A_1, \dots, A_r$ sont associés. Un seul d'entre eux est unitaire, il est appelé LE *PGCD de* $A_1, \dots, A_r$ et noté $A_1 \wedge \dots \wedge A_r$.
- Par convention, $0 \wedge \dots \wedge 0 = 0$.

Comme dans $\mathbb{Z}$, la propriété d'associativité du PGCD, permet de ramener le calcul du PGCD d'une famille finie de polynômes à des calculs successifs de PGCD de deux polynômes.

Exemple 70 $\big(X^3+4X^2+5X+2\big) \wedge \big(X^3+4X^2+4X\big) \wedge \big(X^2-4\big) = (X+2) \wedge \big(X^2-4\big) = X+2$.

Les résultats du paragraphe précédents s'étendent au PGCD d'une famille finie de polynômes.

Théorème 71

Soit $A_1, \dots, A_r \in \mathbb{K}[X]$.

- Les diviseurs communs de $A_1, \dots, A_r$ sont les diviseurs de $A_1 \wedge \dots \wedge A_r$.
- Pour tout $K \in \mathbb{K}[X]$, $(KA_1) \wedge \dots \wedge (KA_r)$ et $K(A_1 \wedge \dots \wedge A_r)$ sont associés.
- Il existe des polynômes $U_1, \dots, U_r \in \mathbb{K}[X]$ tels que $A_1 \wedge \dots \wedge A_r = A_1U_1 + \dots + A_rU_r$. Une telle relation est appelée UNE *relation de Bézout de* $A_1, \dots, A_r$ *de coefficients* $U_1, \dots, U_r$.

5.3 Polynômes premiers entre eux

Définition 72 – Polynômes premiers entre eux dans leur ensemble/deux à deux

Soit $A, B, A_1, \dots, A_r \in \mathbb{K}[X]$.

- A et B sont dits *premiers entre eux* lorsque 1 est leur seul diviseur commun unitaire, *i.e.* $A \wedge B = 1$.
- $A_1, \dots, A_r$ sont dits *premiers entre eux dans leur ensemble* lorsque 1 est leur seul diviseur commun unitaire, *i.e.* $A_1 \wedge \dots \wedge A_r = 1$.
- $A_1, \dots, A_r$ sont dits *premiers entre eux deux à deux* lorsque $A_i \wedge A_j = 1$, pour tous $i, j \in [\![1, r]\!]$ distincts.

✖ **Attention !** ✖ Premiers entre eux DEUX À DEUX $\implies$ Premiers entre eux DANS LEUR ENSEMBLE

mais la réciproque est bien sûr fausse, comme pour les entiers.

Exemple 73

- Soient a et b deux éléments distincts de $\mathbb{K}$. Si p et q sont deux entiers naturels, les polynômes $A = (X-a)^p$ et $B = (X-b)^q$ sont premiers entre eux puisque les diviseurs unitaires de A sont les polynômes $(X-a)^k$, avec $k \leqslant p$, et que parmi eux seul 1 divise B.
- Pour $(a_1, a_2, \dots, a_p) \in \mathbb{K}^p$, le polynôme $A = (X-a_1)(X-a_2)\dots(X-a_p)$ est premier avec tout polynôme n'admettant aucun a_i pour racine. En effet, les diviseurs unitaires de A sont les polynômes de la forme $\prod_{i\in I}(X-a_i)$, avec $I \subset [\![1, p]\!]$, et aucun d'eux hormis 1 ne divise B, puisque A et B n'ont pas de racine commune.
- En particulier, deux polynômes de $\mathbb{C}[X]$ sont premiers entre eux si et seulement s'ils n'ont pas de racine commune.

Théorème 74 – Théorèmes de Bézout et Gauss, conséquences

Soit $A, B, C, P, A_1, \dots, A_r \in \mathbb{K}[X]$.

- **Théorème de Bézout.** Les assertions suivantes sont équivalentes :
  (i) $A \wedge B = 1$ **(ii)** Il existe deux polynômes $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$.
- **Théorème de Gauss.** Si $A \mid BC$ et $A \wedge B = 1$, alors $A \mid C$.
- **Lemme d'Euclide.** Pour tout $P \in \mathbb{K}[X]$ IRRÉDUCTIBLE, $P \mid AB \iff P \mid A$ ou $P \mid B$.
- **Produits de polynômes.**
  × Si chacun des polynômes $A_1, \dots, A_r$ est premier avec P, alors leur produit $A_1 \cdots A_r$ l'est aussi.
  × Si $A_1, \dots, A_r$ divisent P et sont premiers entre eux DEUX À DEUX, alors leur produit $A_1 \cdots A_r$ divise P.

Exemple 75 On peut ainsi retrouver plus rapidement des résultats déjà connus.

- Si $a, b \in \mathbb{K}$ sont distincts, alors les polynômes $X - a$ et $X - b$ sont premiers entre eux, comme le prouve l'identité de Bézout $\frac{X-a}{b-a} + \frac{X-b}{a-b} = 1$. On en déduit, pour tous $p, q \in \mathbb{N}^2$, que $(X-a)^p$ et $(X-b)^q$ sont premiers entre eux.
- Soit A un polynôme admettant $\alpha_1, \alpha_2, \dots, \alpha_p$ pour racines distinctes d'ordres respectifs $r_1, r_2, \dots, r_p$.
  Par définition, les polynômes $(X - \alpha_i)^{r_i}$ divisent A et, comme ils sont premiers entre eux deux à deux, leur produit divise A (comme nous l'avions établi au théorème 23).

Corollaire 76 – Caractérisation de la divisibilité dans $\mathbb{C}[X]$

Soit $A, B \in \mathbb{C}[X]$ et $\alpha \prod_{k=1}^{r} (X - \lambda_k)^{m_k}$ la factorisation irréductible de A, les λ_k étant distincts. Le polynôme A divise B si et seulement si, pour tout $i \in [\![1, r]\!]$, λ_i est racine de B de multiplicité supérieure ou égale à m_i.

5.4 PPCM de deux polynômes

Définition-théorème 77 – PPCM de deux polynômes, lien avec le PGCD

Soit $A, B \in \mathbb{K}[X]$ non nuls. On appelle *plus petit commun multiple (ou PPCM) de A et B* tout multiple commun non nul de A et B de degré minimal.

- **Existence et unicité.** A et B possèdent un unique PPCM unitaire appelé LE *PPCM de A et B*, noté $A \vee B$. Leurs autres PPCM sont les associés de $A \vee B$.
- **Multiples communs et multiples du PPCM.** Les multiples communs de A et B sont les multiples de $A \vee B$, autrement dit $A\mathbb{K}[X] \cap B\mathbb{K}[X] = (A \vee B)\mathbb{K}[X]$.
- **Lien avec le PGCD.** Les polynômes AB et $(A \wedge B)(A \vee B)$ sont associés.

✎ **En pratique** ✎ Si l'on connaît la factorisation irréductible de deux polynômes non nuls de $\mathbb{K}[X]$, on peut déterminer leur PPCM sans calculer au préalable leur PGCD. Le principe est le même que dans $\mathbb{Z}$ (cf. théorème 58 du chapitre 13).

Exemple 78 $\big[2X(X+1)^2(X+2)^3\big] \vee \big[X(X+2)^4(X^2+1)\big] = X(X+1)^2(X+2)^4(X^2+1)$.

Quelques résultats classiques :

- Racines rationnelles d'un polynôme à coefficients entiers (exemple 11).
- Reste de la division euclidienne de X^k par $X^n - 1$ (exercice 7).
- Théorème des deux carrés dans $\mathbb{R}[X]$ (exercice 48).
- $(X^m - 1) \wedge (X^n - 1) = X^{m \wedge n} - 1$ (exercice 50).
- Polynômes P tels que $P' \mid P$ (exercice 54).

Compétences à acquérir

- Calculer le reste d'une division euclidienne : exercices 4, 5 et 7 à 9.
- Montrer qu'un polynôme est multiple d'un autre (via la division euclidienne) : exercices 2, 3 et 6.
- Déterminer la multiplicité d'une racine : exercices 10 et 16
- Montrer qu'un polynôme est multiple d'un autre (via la multiplicité des racines) : exercices 11 à 15.
- Utiliser la rigidité : exercices 19 à 24.
- Utiliser les formules de Viète : exercices 25 à 32.
- Utiliser les polynômes interpolateurs de Lagrange : exercices 33 à 36.
- Déterminer la factorisation irréductible sur $\mathbb{R}$ ou $\mathbb{C}$ d'un polynôme : exercices 38 à 43.
- Calculer le PGCD de deux polynômes : exercices 49 et 50.

A Annexe

Démonstration du théorème 36.

Soit P un polynôme à coefficients complexes de degré $p > 0$. Pour montrer que P possède une racine complexe, considérons $\alpha = \inf_{z\in\mathbb{C}} |P(z)|$, qui existe puisque $\{|P(z)| \mid z \in \mathbb{C}\}$ est une partie non vide de $\mathbb{R}_+$, et montrons que cette borne inférieure est atteinte, puis qu'elle est nulle.

Etape 1 - L'inf est atteint. Posons $P = \sum_{k=0}^{p} a_k X^k$ avec $a_p \neq 0$, alors, pour tout $z \in \mathbb{C}$ avec $r = |z|$,

$$|P(z)| \geqslant |a_p z^p| - \left|\sum_{k=0}^{p-1} a_k z^k\right| \geqslant |a_p| r^p - \sum_{k=0}^{p-1} |a_k| r^k,$$

d'après l'inégalité triangulaire. Ce minorant définit une fonction polynomiale réelle en la variable r, qui tend vers $+\infty$ quand r tend vers $+\infty$ (règle du plus haut degré). Elle est donc plus grande que $\alpha + 1$ au voisinage de $+\infty$, ce qui prouve qu'il existe un disque D centré en 0 en dehors duquel on a $|P(z)| \geqslant \alpha + 1$.

Puisque $\alpha = \inf_{z\in\mathbb{C}} |P(z)|$, on peut trouver une suite de complexes $(u_n)_{n\in\mathbb{N}}$ telle que $\lim_{n\to+\infty} |P(u_n)| = \alpha$. Cette suite est donc, à partir d'un certain rang, dans le disque D, et par suite elle est bornée. On peut donc en extraire une sous-suite $\left(u_{\varphi(n)}\right)_{n\in\mathbb{N}}$ convergeant vers un complexe z_0 (théorème de Bolzano-Weierstrass). Comme

$$P\left(u_{\varphi(n)}\right) = \sum_{k=0}^{p} a_k u_{\varphi(n)}^k,$$

on en déduit $\lim_{n\to+\infty} P\left(u_{\varphi(n)}\right) = P(z_0)$, ce qui donne

$$\alpha = \lim_{n\to+\infty} \left|P\left(u_{\varphi(n)}\right)\right| = |P(z_0)|.$$

Etape 2 - $\alpha = 0$. Montrons par l'absurde que $P(z_0) = 0$ en supposant $\alpha > 0$.

Quitte à considérer le polynôme $\dfrac{P(z_0 + X)}{P(z_0)}$, on peut supposer $\alpha = 1$ et $z_0 = 0$. Le polynôme non constant P s'écrit donc

$$P = 1 - a_q X^q + \sum_{k=q+1}^{p} a_k X^k \quad \text{avec } a_q \neq 0 \text{ et } 1 \leqslant q \leqslant p.$$

Posons $a_q = \rho\, \mathrm{e}^{-i\theta}$ avec $\rho \in \mathbb{R}_+^*$ et $\theta \in \mathbb{R}$. Pour $z = r\, \mathrm{e}^{i\theta/q}$, avec $r > 0$, on a

$$P(z) = 1 - \rho r^q + \sum_{k=q+1}^{p} a_k r^k\, \mathrm{e}^{ik\theta/q}$$

d'où

$$|P(z)| \leqslant |1 - \rho r^q| + \sum_{k=q+1}^{p} |a_k| r^k.$$

Si l'on suppose $r \leqslant \sqrt[q]{1/\rho}$, on a $|1 - \rho r^q| = 1 - \rho r^q$ et donc

$$|P(z)| - 1 \leqslant -\rho r^q + \sum_{k=q+1}^{p} |a_k| r^k$$

soit, sachant $r > 0$,

$$\frac{|P(z)| - 1}{r^q} \leqslant -\rho + \sum_{k=q+1}^{p} |a_k| r^{k-q} \xrightarrow[r\to 0]{} -\rho < 0.$$

Ainsi, le majorant $-\rho r^q + \sum_{k=q+1}^{p} |a_k| r^k$ de $|P(z)| - 1$ est strictement négatif au voisinage de 0. Par conséquent, il existe $z \in \mathbb{C}$ tel que $|P(z)| < 1 = \alpha$, ce qui est contradictoire.