Polynômes

Jeremy Daniel

> Les géomètres se sont beaucoup occupés de la résolution générale des équations algébriques, et plusieurs d'entre eux ont cherché à en prouver l'impossibilité ; mais si je ne me trompe pas, on n'y a pas réussi jusqu'à présent. J'ose donc espérer que les géomètres recevront avec bienveillance ce mémoire qui a pour but de remplir cette lacune dans la théorie des équations algébriques.
>
> Niels Henrik Abel [1]

On désigne par $\mathbb{K}$ un corps quelconque.

1 Présentation de $\mathbb{K}[X]$

1.1 L'anneau $\mathbb{K}[X]$

Définition 1.1 (Suites à support fini)
Une suite $(u_n) \in \mathbb{K}^{\mathbb{N}}$ est à support fini s'il existe $N \in \mathbb{N}$ tel que $\forall n \geq N, u_n = 0$.

Notation 1.2
On note $\mathbb{K}^{(\mathbb{N})}$ l'ensemble des suites à support fini.

Définition 1.3 (Opérations sur $\mathbb{K}^{(\mathbb{N})}$)
Soient $(u_n)_{n\in\mathbb{N}}, (v_n)_{n\in\mathbb{N}} \in \mathbb{K}^{(\mathbb{N})}$. Soit $\lambda \in \mathbb{K}$. On définit

- $(u_n)_{n\in\mathbb{N}} + (v_n)_{n\in\mathbb{N}} = (u_n + v_n)_{n\in\mathbb{N}} \in \mathbb{K}^{(\mathbb{N})}$;
- $\lambda(u_n)_{n\in\mathbb{N}} = (\lambda u_n)_{n\in\mathbb{N}}$;

1. Phrase introductive du *Mémoire sur les équations algébriques, où l'on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré.*

- $(u_i)_{i\in\mathbb{N}} \times (v_j)_{j\in\mathbb{N}} = (w_k)_{k\in\mathbb{N}}$, où pour tout $k \in \mathbb{N}$:

$$w_k = \sum_{i+j=k} u_i v_j.$$

Remarque 1.4
La somme et la multiplication externe par un élément de $\mathbb{K}$ sont déjà définies sur $\mathbb{K}^{\mathbb{N}}$. En revanche, le produit *de convolution* n'est pas la restriction du produit usuel défini sur $\mathbb{K}^{\mathbb{N}}$.

Définition 1.5 (Indéterminée X)
On note $X \in \mathbb{K}^{(\mathbb{N})}$ la suite $(\delta_{n,1})_{n\in\mathbb{N}}$.

Lemme 1.6 (Calcul de X^k)
Pour tout $k \in \mathbb{N}$, on définit X^k comme le k-ème itéré de X pour la loi $\times$. Alors,

$$\forall k \in \mathbb{N}, X^k = (\delta_{k,n})_{n\in\mathbb{N}}.$$

Remarque 1.7
Si $P = (p_k)_{k\in\mathbb{N}} \in \mathbb{K}^{(\mathbb{N})}$, on a donc $P = \sum_{k\in\mathbb{N}} p_k X^k$, la somme étant en réalité finie puisque p_k est nul à partir d'un certain rang. On utilise systématiquement ce mode de représentation des éléments de $\mathbb{K}^{(\mathbb{N})}$.

Définition 1.8 (Ensemble des polynômes $\mathbb{K}[X]$)
On note $\mathbb{K}[X]$, ce qui a été dénoté jusque là par $\mathbb{K}^{(\mathbb{N})}$. Les éléments de $\mathbb{K}[X]$ sont les polynômes à coefficients dans $\mathbb{K}$.

Remarque 1.9
On pourra parfois utiliser une autre lettre T, U, Y, Z... au lieu de X. On évitera cependant l'emploi d'une lettre minuscule.

Remarque 1.10
Soient $P = \sum_k p_k X^k$ et $Q = \sum_k q_k X^k$. Soit $\lambda \in \mathbb{K}$.
Les opérations dans $\mathbb{K}[X]$ sont données par :

- $\lambda P = \sum_k \lambda p_k X^k$;
- $P + Q = \sum_k (p_k + q_k) X^k$;
- $PQ = \sum_k \big(\sum_{i+j=k} p_i q_j \big) X^k$.

Théorème 1.11 ($\mathbb{K}[X]$ est un anneau commutatif)
Muni des lois $+$ et $\times$, $\mathbb{K}[X]$ est un anneau commutatif.

Définition 1.12 (Degré)
Soit $P = \sum p_k X^k \in \mathbb{K}[X]$. On définit le degré de P par

$$\deg P = \begin{cases} -\infty & \text{si } P = 0 \\ \max\{k \in \mathbb{N} \mid p_k \neq 0\} & \text{sinon.} \end{cases}$$

Remarque 1.13
Si d est le degré de $P \neq 0$, on peut donc écrire $P = \sum_{k=0}^{d} p_k X^k$. On prendra garde au fait que réciproquement une écriture $P = \sum_{k=0}^{d} p_k X^k$ implique seulement que $\deg P \leq d$ (le coefficient p_d pouvant être nul).

Notation 1.14 ($\mathbb{K}_n[X]$)
Pour tout $n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré $\leq n$.

Définition 1.15 (Coefficient dominant, coefficient constant)
Soit $P = \sum_{k=0}^{d} p_k X^k$ un polynôme non nul de degré d.
On appelle p_d le coefficient dominant de P, p_0 le coefficient constant de P.

Définition 1.16 (Polynôme unitaire, polynôme constant)
Un polynôme P est unitaire s'il est non nul et si son coefficient dominant est égal à 1.
Un polynôme est constant s'il est nul ou de degré 0.

Remarque 1.17
On identifie les polynômes constants aux éléments de $\mathbb{K}$.

Proposition 1.18 (Degré de la somme, du produit)
Soient $P, Q \in \mathbb{K}[X]$.
- $\deg(P + Q) \leq \max(\deg P, \deg Q)$, *avec égalité si* $\deg P \neq \deg Q$.
- $\deg(PQ) = \deg P + \deg Q$.

Corollaire 1.19 (Intégrité de $\mathbb{K}[X]$)
L'anneau $\mathbb{K}[X]$ est intègre.

Corollaire 1.20 (Inversibles de $\mathbb{K}[X]$)
Les inversibles de $\mathbb{K}[X]$ sont les polynômes constants non nuls.

Définition 1.21 (Polynômes associés)
Deux polynômes P et Q sont associés s'ils sont tous les deux nuls, ou s'il existe $\lambda \in \mathbb{K}$ tels

que $P = \lambda Q$.

Remarque 1.22
On définit ainsi une relation d'équivalence sur $\mathbb{K}[X]$. Un ensemble de représentants des classes est formé par le polynôme nul et l'ensemble des polynômes unitaires.

1.2 Composition et évaluation

Définition 1.23 (Polynôme composé)
Soient P et Q deux polynômes. On note $P = \sum_k p_k X^k$. On définit le polynôme composé $P \circ Q$ – noté parfois $P(Q)$ – par $P \circ Q = \sum_k p_k Q^k$.

Attention !
Comme pour les fonctions, $P \circ Q \neq Q \circ P$ en général.

Remarque 1.24
En particulier, en prenant $Q = X$, on a $P \circ X = P$. On notera indifféremment P ou $P(X)$ par la suite.

Proposition 1.25 (Degré du polynôme composé)
Soient $P, Q \in \mathbb{K}[X]$, avec Q non nul. On a :

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

Définition 1.26 (Évaluation)
Soit $P = \sum_k p_k X^k$ et $a \in \mathbb{K}$. L'évaluation de P en a – notée $P(a)$ – est $P(a) = \sum_k p_k a^k$.

Définition 1.27 (Polynômes et applications polynomiales)
Soit $P \in \mathbb{K}[X]$. On note $\widetilde{P} \in \mathbb{K}^{\mathbb{K}}$ la fonction définie par $\widetilde{P}(a) = P(a)$, pour tout $a \in \mathbb{K}$.
On définit ainsi une application $\Phi : \mathbb{K}[X] \to \mathbb{K}^{\mathbb{K}}$, par $\Phi(P) = \widetilde{P}$.

Remarque 1.28
L'application Φ est compatible avec la somme, le produit, la multiplication externe par un élément de $\mathbb{K}$ et avec la composition.

1.3 Dérivation

Définition 1.29 (Polynôme dérivé)
Soit $P = \sum_{k=0}^{d} p_k X^k$. Son polynôme dérivé, noté P' est

$$P' = \sum_{k=1}^{d} k p_k X^{k-1} = \sum_{k=0}^{d-1} (k+1) p_{k+1} X^k.$$

On définit récursivement $P^{(k)}$ par $P^{(0)} = P$ et $P^{(k)} = \left(P^{(k-1)}\right)'$, pour $k \geq 1$.

Remarque 1.30
Pour $\mathbb{K} = \mathbb{R}$, cette définition est compatible avec la notion classique de dérivée des applications polynomiales.

Proposition 1.31 (Degré du polynôme dérivé)
Si $\mathrm{car}(\mathbb{K}) = 0$ *et si* P *n'est pas constant,* $\deg P' = \deg P - 1$.

Proposition 1.32 (Formules sur la dérivation)
Soient $P, Q \in \mathbb{K}[X]$*, soient* $\lambda, \mu \in \mathbb{K}$*, soit* $n \in \mathbb{N}$*.*
- $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$;
- $(PQ)' = P'Q + PQ'$;
- *Formule de Leibniz :* $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$;
- $(P \circ Q)' = Q' \times P' \circ Q$.

Théorème 1.33 (Formule de Taylor formelle)
On suppose $\mathrm{car}(\mathbb{K}) = 0$*. Soit* $P \in \mathbb{K}[X]$ *de degré* d*, soit* $a \in \mathbb{K}$*.*

$$P = \sum_{k=0}^{d} \frac{P^{(k)}(a)}{k!} (X-a)^k.$$

Remarque 1.34
Ainsi, un polynôme P est entièrement déterminé par la suite des valeurs $P^{(k)}(a)$, où $k \in \mathbb{N}$.

2 Arithmétique de $\mathbb{K}[X]$

2.1 Division euclidienne

Définition 2.1 (Relation de divisibilité)
Soient $A, B \in \mathbb{K}[X]$. On dit que B divise A – ou que B est un diviseur de A ou que A est un multiple de B – s'il existe $Q \in \mathbb{K}[X]$ tel que $A = B \times Q$.

Proposition 2.2
Soient $A, B \in \mathbb{K}[X]$ tels que A divise B et B divise A. Alors, A et B sont associés.

Remarque 2.3
La relation de divisibilité est ainsi une relation d'ordre (non totale) sur l'ensemble des classes d'équivalence pour la relation *être associé*.

Théorème 2.4 (Division euclidienne dans $\mathbb{K}[X]$)
Soient $A, B \in \mathbb{K}[X]$, avec $B \neq 0$.
Il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que : $A = BQ + R$ et $\deg R < \deg B$.

Définition 2.5 (Quotient et reste)
Dans le théorème précédent, Q est le quotient dans la division euclidienne de A par B, R est le reste.

Remarque 2.6
B divise A ssi le reste dans la division euclidienne de A par B est nul.

Définition 2.7 (Idéal dans un anneau commutatif)
Soit A un anneau commutatif. Un idéal I de A est une partie I de A telle que
- I est un sous-groupe de $(A, +)$;
- $\forall a \in A, x \in I, xa \in I$.

Exercice 2.8
Montrer que si un idéal I contient un élément inversible de A, alors $I = A$.
En déduire quels sont les idéaux d'un corps $\mathbb{K}$.

Définition 2.9 (Idéal principal, anneau principal)
Un idéal I d'un anneau commutatif A est principal s'il est de la forme $xA = \{xa, a \in A\}$, pour un élément $x \in A$.
Un anneau est principal s'il est commutatif, intègre et si tous ses idéaux sont principaux.

Exemples 2.10
- Les idéaux de $\mathbb{Z}$ étant en particulier des sous-groupes de $\mathbb{Z}$, ils sont de la forme $n\mathbb{Z}$, pour un $n \in \mathbb{Z}$. Donc, $\mathbb{Z}$ est un anneau principal.
- L'anneau $\mathbb{Z}[X]$ (sous-anneau de $\mathbb{Q}[X]$ des polynômes à coefficients entiers) n'est pas principal : l'idéal $I = \big\{2k + XP, (k, P) \in \mathbb{Z} \times \mathbb{Z}[X]\big\}$ n'est pas principal.

Corollaire 2.11 ($\mathbb{K}[X]$ est un anneau principal)
$\mathbb{K}[X]$ est un anneau principal : les idéaux de $\mathbb{K}[X]$ sont de la forme $A\mathbb{K}[X]$, où $A \in \mathbb{K}[X]$.

Remarque 2.12
Si A et B sont deux générateurs du même idéal, alors ils sont associés. En général, on choisira le générateur unitaire (pour un idéal non nul) si on a besoin d'en fixer un.

Remarque 2.13
Cet énoncé explique en grande partie pourquoi l'arithmétique de $\mathbb{K}[X]$ est très proche de celle de $\mathbb{Z}$.

2.2 PGCD, PPCM

Définition 2.14 (PGCD de deux polynômes)
Soient $A, B \in \mathbb{K}[X]$. On appelle PGCD de A et B tout générateur de l'idéal

$$A\mathbb{K}[X] + B\mathbb{K}[X] = \left\{AP + BQ, (P, Q) \in \mathbb{K}[X]^2\right\}.$$

Notation 2.15
Les PGCD de A et B sont donc associés. L'unique unitaire (si $(A, B) \neq (0, 0)$) est noté $A \wedge B$. Si $(A, B) = (0, 0)$, on définit $0 \wedge 0 = 0$.

Remarque 2.16
On a donc $(A \wedge B)\mathbb{K}[X] = A\mathbb{K}[X] + B\mathbb{K}[X]$. Conséquences :
- $A \wedge B$ est un diviseur commun de A et B.
- Il existe un couple $(U, V) \in \mathbb{K}[X]^2$ tel que $AU + BV = A \wedge B$. On parle de relation de Bézout.
- Les diviseurs communs à A et B sont exactement les diviseurs communs de $A \wedge B$.
- $A \wedge B$ est l'unique polynôme unitaire de degré maximal divisant A et B.

Remarque 2.17
D'un point de vue algorithmique, le calcul de $A \wedge B$ ou d'une relation de Bézout entre A et B se fait comme pour les entiers, respectivement par l'algorithme d'Euclide et l'algorithme d'Euclide étendu.

Exercice 2.18
Déterminer un PGCD et une relation de Bézout pour

$$A = X^3 + 3X^2 + 2X \text{ et } B = X^2 + 5X + 6.$$

Proposition 2.19 ($A \wedge B$ ne dépend pas du corps)
Soient $\mathbb{L}$ un corps, tel que $\mathbb{K}$ est un sous-corps de $\mathbb{L}$. Soient $A, B \in \mathbb{K}[X]$. En considérant A et B dans $\mathbb{L}[X]$, on calcule $(A \wedge B)$ dans $\mathbb{L}[X]$. Alors, $A \wedge B \in \mathbb{K}[X]$.

Remarque 2.20
Le cas le plus important en pratique est celui où $\mathbb{K} = \mathbb{R}$ et $\mathbb{L} = \mathbb{C}$. Le PGCD unitaire de deux polynômes à coefficients réels, calculé dans $\mathbb{C}[X]$, est en fait à coefficients réels.

DÉFINITION 2.21 (PPCM de deux polynômes)
Soient $A, B \in \mathbb{K}[X]$. On appelle PPCM de A et B tout générateur de l'idéal

$$A\mathbb{K}[X] \cap B\mathbb{K}[X].$$

NOTATION 2.22
Deux PPCM de A et B sont associés. On note $A \vee B$ l'unique PPCM unitaire – si A et B sont non nuls. Si A ou B est nul, $A \vee B = 0$.

REMARQUE 2.23
On a donc $(A \vee B)\mathbb{K}[X] = A\mathbb{K}[X] \cap B\mathbb{K}[X]$. Conséquences :
- $A \vee B$ est un multiple commun de A et B.
- Les multiples communs de A et B sont exactement les multiples de $A \vee B$.
- $A \vee B$ est l'unique polynôme unitaire de degré minimal multiple de A et B.

DÉFINITION 2.24 (PGCD et PPCM d'un nombre fini de polynômes)
Soient $A_1, \ldots, A_n \in \mathbb{K}[X]$. On appelle
- PGCD de $A_1, \ldots, A_n$ tout générateur de l'idéal $A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X]$.
- PPCM de $A_1, \ldots, A_n$ tout générateur de l'idéal $A_1\mathbb{K}[X] \cap \cdots \cap A_n\mathbb{K}[X]$.

NOTATION 2.25
Si $(A_1, \ldots, A_n) \neq (0, \ldots, 0)$, on note $A_1 \wedge \cdots \wedge A_n$ l'unique PGCD unitaire de $A_1, \ldots, A_n$ (0 si tous les A_i sont nuls). Si aucun des A_i n'est nul, on note $A_1 \vee \cdots \vee A_n$ l'unique PPCM unitaire de $A_1, \ldots, A_n$ (0 si l'un des A_i est nul).

REMARQUE 2.26
Ainsi,
- Les diviseurs communs de $A_1, \ldots, A_n$ sont les diviseurs de $A_1 \wedge \cdots \wedge A_n$.
- Les multiples communs de $A_1, \ldots, A_n$ sont les multiples de $A_1 \vee \cdots \vee A_n$.
- Il existe $(U_1, \ldots, U_n) \in \mathbb{K}[X]$ tels que $A_1U_1 + \cdots + A_nU_n = A_1 \wedge \cdots \wedge A_n$.
- $\wedge$ et $\vee$ sont associatives et commutatives.

2.3 Polynômes irréductibles et polynômes premiers entre eux

DÉFINITION 2.27 (Polynômes premiers entre eux)
Soient $A, B \in \mathbb{K}[X]$. Ils sont premiers entre eux si $A \wedge B = 1$.

THÉORÈME 2.28 (Identité de Bézout)
Deux polynômes $A, B \in \mathbb{K}[X]$ sont premiers entre eux ssi $\exists (U, V) \in \mathbb{K}[X]^2 : AU + BV = 1$.

PROPOSITION 2.29
Soient $A, B \in \mathbb{K}[X]$ non tous les deux nuls. Alors, $\dfrac{A}{A \wedge B}$ et $\dfrac{B}{A \wedge B}$ sont premiers entre eux.

Proposition 2.30 (Polynôme premier avec un produit)
Soient $A, B_1, \ldots, B_n \in \mathbb{K}[X]$.
Alors, A est premier avec $B_1 \ldots B_n$ ssi A est premier avec chaque B_i.

Proposition 2.31 (Produit de premiers entre eux)
Soient $A, B, C \in \mathbb{K}[X]$.
Si A et B divisent C et que A et B sont premiers entre eux, alors AB divise C.

Proposition 2.32 (Lemme de Gauss)
Soient $A, B, C \in \mathbb{K}[X]$.
On suppose que $A \mid BC$ et que A est premier avec B, alors A divise C.

Définition 2.33 (Premiers entre eux dans leur ensemble)
Des polynômes $P_1, \ldots, P_n \in \mathbb{K}[X]$ sont premiers entre eux dans leur ensemble si

$$P_1 \wedge \cdots \wedge P_n = 1.$$

Remarque 2.34
Comme pour les entiers, on notera la distinction entre *premiers entre eux dans leur ensemble* et *deux à deux premiers entre eux.* Considérer par exemple $P_1 = X(X-1)$, $P_2 = X(X-2)$ et $P_3 = (X-1)(X-2)$ dans $\mathbb{R}[X]$.

Définition 2.35 (Polynôme irréductible)
Un polynôme $A \in \mathbb{K}[X]$ est irréductible s'il n'est pas constant et si

$$\forall (B, C) \in \mathbb{K}[X]^2, (A = BC) \implies (\deg B = 0 \text{ ou } \deg C = 0).$$

Remarque 2.36
Si deux polynômes sont associés, l'un est irréductible ssi l'autre l'est.

Proposition 2.37 ($X - \alpha$ est irréductible)
Pour tout $\alpha \in \mathbb{K}$, $X - \alpha$ est irréductible dans $\mathbb{K}[X]$.

Proposition 2.38
Soient $A, B \in \mathbb{K}[X]$. Si A est irréductible et ne divise pas B, alors A est premier avec B.

Corollaire 2.39 (Lemme d'Euclide)
Soient $A, B, C \in \mathbb{K}[X]$ tels que A est irréductible et A divise BC.
Alors A divise B ou A divise C.

Théorème 2.40 (Factorisation en produit d'irréductibles)
Soit $P \in \mathbb{K}[X] - \{0\}$. Il existe $\lambda \in \mathbb{K}^*$, un nombre fini de polynômes irréductibles unitaires

deux à deux distincts $P_1, \ldots, P_k$, des entiers $n_1, \ldots, n_k \geq 1$ tels que

$$P = \lambda \prod_{i=1}^{k} P_i^{n_i}.$$

Cette écriture est unique, à permutation près des facteurs.

Remarque 2.41
Les polynômes constants non nuls sont obtenus en considérant le produit vide ($k = 0$).

Proposition 2.42 (Divisibilité avec la factorisation)
Soient $P = \lambda \prod_{i=1}^{k} P_i^{n_i}$ et $Q = \mu \prod_{i=1}^{k} P_i^{m_i}$ deux polynômes écrits en produit d'irréductibles – on convient que n_i ou m_i peut être nul. Alors,

$$P \text{ divise } Q \iff \forall i \in [\![1, k]\!], n_i \leq m_i.$$

Corollaire 2.43 (PGCD et PPCM)
Avec les notations précédentes, $P \wedge Q = \prod_{i=1}^{k} P_i^{\min(n_i, m_i)}$ et $P \vee Q = \prod_{i=1}^{k} P_i^{\max(n_i, m_i)}$.

Corollaire 2.44 (PGCD $\times$ PPCM)
Si $P, Q \in \mathbb{K}[X]$, $(P \wedge Q)(P \vee Q) = PQ$.

3 Racines d'un polynôme

3.1 Généralités

Définition 3.1 (Racine d'un polynôme)
Soient $P \in \mathbb{K}[X], \alpha \in \mathbb{K}$. On dit que α est racine – ou zéro – de P si $P(\alpha) = 0$.

Proposition 3.2 (Factorisation par $X - \alpha$)
Soient $P \in \mathbb{K}[X], \alpha \in \mathbb{K}$. Alors, α est racine de P ssi $X - \alpha$ divise P.

Proposition 3.3 (Factorisations successives)
Soit $P \in \mathbb{K}[X]$, soient $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ deux à deux distincts. On suppose que pour tout $i \in [\![1, n]\!]$, α_i est racine de P. Alors, $\prod_{i=1}^{n}(X - \alpha_i)$ divise P.

Corollaire 3.4 (Borne sur le nombre de racines)
Un polynôme $P \in \mathbb{K}[X]$ de degré d a au plus d racines distinctes.

Remarque 3.5
En particulier, si un polynôme a une infinité de racines, alors il est nul.

Corollaire 3.6 (Morphisme d'évaluation)
L'application $\Phi : \mathbb{K}[X] \to \mathbb{K}^{\mathbb{K}}, P \mapsto \widetilde{P}$ *est injective ssi* $\mathbb{K}$ *est infini.*

Définition 3.7 (Multiplicité d'une racine)
Soit $P \in \mathbb{K}[X] - \{0\}$, soit $\alpha \in \mathbb{K}$. La multiplicité – ou ordre de multiplicité – de α dans P est le plus grand entier k tel que $(X-\alpha)^k$ divise P.

Remarque 3.8
Ainsi, α est racine de P ssi la multiplicité de α dans P est au moins 1.
Si, la multiplicité est au moins 2, on parle de racine multiple.

Proposition 3.9
Avec les notations précédentes, α *est racine de* P *de multiplicité* p *ssi*

$$\exists Q \in \mathbb{K}[X] : A = Q \times (X-\alpha)^p \text{ et } Q(\alpha) \neq 0.$$

Proposition 3.10 (Factorisations successives, avec multiplicité)
Soient $P \in \mathbb{K}[X]$, $\alpha_1, \ldots, \alpha_r \in \mathbb{K}$, *deux à deux distincts de multiplité* $n_1, \ldots, n_r$ *dans* P.
Alors, $\displaystyle\prod_{i=1}^{r}(X-\alpha_i)^{n_i}$ *divise* P.

Définition 3.11 (Polynôme scindé, scindé à racines simples)
Un polynôme $P \in \mathbb{K}[X]$ non nul est scindé s'il s'écrit $P = \lambda \displaystyle\prod_{i=1}^{r}(X-\alpha_i)^{n_i}$, où les α_i sont deux à deux distincts et $n_i \geq 1$.
Si de plus, pour tout i, $n_i = 1$, on dit qu'il est scindé à racines simples.

Remarque 3.12
Un polynôme est scindé à racines simples s'il a autant de racines que son degré. Il est scindé si la somme des multiplicité de ses racines est égale à son degré ; on dit encore que son degré est égal à son nombre de racines, *en comptant les multiplicités.*

3.2 Multiplicité et dérivées successives

On suppose car $\mathbb{K} = 0$.

Proposition 3.13
Soit $P \in \mathbb{K}[X] - \{0\}$, *soit* $\alpha \in \mathbb{K}$.
Alors, α *est racine de* P *d'ordre au moins* k *ssi* $P(\alpha) = P'(\alpha) = \cdots = P^{(k-1)}(\alpha) = 0$.

Corollaire 3.14 (Caractérisation de la multiplicité par les dérivées successives)
Avec les mêmes notations, α est racine de P d'ordre exactement k ssi

$$P(\alpha) = P'(\alpha) = \cdots = P^{(k-1)}(\alpha) = 0 \text{ et } P^{(k)}(\alpha) \neq 0.$$

Exercice 3.15
Soit $P \in \mathbb{R}[X]$.
- Montrer que si P est scindé à racines simples, alors P' aussi.
- Montrer que si P est scindé, alors P' aussi.

3.3 Relations coefficients-racines

Définition 3.16 (Expressions symétriques élémentaires)
Soient $x_1, \ldots, x_n \in \mathbb{K}$. On note, pour tout $k \in [\![1, n]\!]$:

$$\sigma_k = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \ldots x_{i_k}.$$

On appelle σ_k la k-ème expression symétrique élémentaire en $x_1, \ldots, x_n$.

Remarque 3.17
En particulier, σ_1 est la somme et σ_n le produit de $x_1, \ldots, x_n$.

Théorème 3.18 (Formules de Viète)
Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ un polynôme scindé de degré n.
On note $x_1, \ldots, x_n$ les racines de P, éventuellement répétées selon leur multiplicité. Alors,

$$\forall k \in [\![1, n]\!], \sigma_k = (-1)^k \frac{a_{n-k}}{a_n},$$

où σ_k est la k-ème expression symétrique élémentaire en les racines $x_1, \ldots, x_n$.

Remarque 3.19
Si $P = aX^2 + bX + c$ a pour racines x_1 et x_2, on retrouve les formules

$$x_1 + x_2 = -\frac{b}{a} \text{ et } x_1 x_2 = \frac{c}{a}.$$

3.4 Interpolation de Lagrange

Lemme 3.20 (Polynômes de Lagrange)
Soient $x_1, \ldots, x_n$ deux à deux distincts dans $\mathbb{K}$. Pour tout $i \in [\![1, n]\!]$, il existe un unique polynôme $L_i \in \mathbb{K}_{n-1}[X]$ tel que $\forall j \in [\![1, n]\!], L_i(x_j) = \delta_{i,j}$.

Théorème 3.21 (Interpolation de Lagrange)
Soient $x_1, \dots, x_n$ deux à deux distincts dans $\mathbb{K}$. Soient $y_1, \dots, y_n \in \mathbb{K}$. Il existe un unique polynôme $L \in \mathbb{K}_{n-1}[X]$ tel que $\forall i \in [\![1, n]\!], L(x_i) = y_i$.

Remarque 3.22
Soit $f : \mathbb{R} \to \mathbb{R}$, soient n réels distincts $x_1, \dots, x_n$. Il existe donc un unique $L \in \mathbb{R}_{n-1}[X]$ tel que $L(x_i) = f(x_i)$, pour tout $i \in [\![1, n]\!]$.
Ce polynôme est le polynôme d'interpolation de f en les points x_i.

3.5 Factorisation dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$

Proposition 3.23 (Corps algébriquement clos)
Les assertions suivantes sont équivalentes :
1. *Tout polynôme $P \in \mathbb{K}[X]$ non constant a une racine dans $\mathbb{K}$.*
2. *Tout polynôme $P \in \mathbb{K}[X]$ non nul est scindé.*
3. *Les irréductibles de $\mathbb{K}[X]$ sont les associés des polynômes $X - \alpha$, où $\alpha \in \mathbb{K}$.*

Définition 3.24 (Corps algébriquement clos)
Si $\mathbb{K}$ vérifie l'une des assertions précédentes, on dit que $\mathbb{K}$ est algébriquement clos.

Remarques 3.25
- $\mathbb{R}$ n'est pas algébriquement clos : le polynôme $X^2 + 1$ n'a pas de racines dans $\mathbb{R}$.
- Un corps fini n'est pas algébriquement clos. Notons en effet $\alpha_1, \dots, \alpha_q$ les éléments d'un corps fini $\mathbb{K}$. Alors $P = \displaystyle\prod_{i=1}^{q}(X - \alpha_i) + 1$ n'a pas de racines dans $\mathbb{K}$, puisque $P(x) = 1$, pour tout $x \in \mathbb{K}$.

Théorème 3.26 (d'Alembert-Gauss)
$\mathbb{C}$ est algébriquement clos.

Corollaire 3.27 (Factorisation en irréductibles dans $\mathbb{C}[X]$)
Soit $P \in \mathbb{C}[X]$, non nul.
Il existe $\alpha_1, \dots, \alpha_r \in \mathbb{C}$ deux à deux distincts, $n_1, \dots, n_r \geq 1$ et $\lambda \in \mathbb{C}^*$ tels que

$$P = \lambda \prod_{i=1}^{r}(X - \alpha_i)^{n_i}.$$

Cette décomposition est unique à l'ordre près des facteurs.

Proposition 3.28 (Polynômes irréductibles de $\mathbb{R}[X]$)
Les polynômes irréductibles de $\mathbb{R}[X]$ sont les associés des polynômes :
- *$X - \alpha$, où $\alpha \in \mathbb{R}$;*

– $X^2 + aX + b$, *où* $a, b \in \mathbb{R}$ *sont tels que* $a^2 - 4b < 0$.

COROLLAIRE 3.29 (Factorisation en irréductibles dans $\mathbb{R}[X]$)
Soit $P \in \mathbb{R}[X] - \{0\}$.
Il existe $\alpha_1, \ldots, \alpha_r \in \mathbb{R}$ *deux à deux distincts,* $n_1, \ldots, n_r \geq 1$, $(\beta_1, \gamma_1), \ldots, (\beta_s, \gamma_s) \in \mathbb{R}^2$, *deux à deux distincts tels que* $\beta_j^2 - 4\gamma_j < 0$, $m_1, \ldots, m_s \geq 1$ *et* $\lambda \in \mathbb{R}^*$ *tels que :*

$$P = \lambda \prod_{i=1}^{r} (X - \alpha_i)^{n_i} \prod_{j=1}^{s} (X^2 + \beta_j X + \gamma_j)^{m_j}$$

La décomposition est unique à l'ordre près des facteurs dans chaque produit.