# Polynômes

## Table des matières



# 1 Arithmétique des polynômes

## 1.1 Relation de divisibilité

**Définition 1.1**

Soit $A, B \in \mathbb{K}[X]$. On dit que $A$ divise $B$ lorsqu'il existe $P \in \mathbb{K}[X]$ tel que $B = PA$.

**Remarques**

- Si $A, B \in \mathbb{K}[X]$ et $B \neq 0$, alors $B$ divise $A$ si et seulement si le reste de la division euclidienne de $A$ par $B$ est nul.
- Si $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$, $X - \alpha$ divise $P$ si et seulement si $\alpha$ est une racine de $P$.

**Proposition 1.2**

La relation de divisibilité
- est réflexive : $\forall A \in \mathbb{K}[X], \quad A|A$.
- est transitive : $\forall A, B, C \in \mathbb{K}[X], \quad [A|B \quad \text{et} \quad B|C] \Longrightarrow A|C$.
- n'est pas antisymétrique. Cependant

$$\forall A, B \in \mathbb{K}[X], \quad [A|B \quad \text{et} \quad B|A] \quad \Longleftrightarrow \quad [\exists \lambda \in \mathbb{K}^*, \quad A = \lambda B]\,.$$

Si tel est le cas, on dit que $A$ et $B$ sont *associés*.

**Remarque**

- En particulier, si $A, B \in \mathbb{K}[X]$ sont unitaires ou nuls et si $A|B$ et $B|A$, alors $A = B$.

**Proposition 1.3**

Soit $A, B, C \in \mathbb{K}[X]$ et $P, Q \in \mathbb{K}[X]$, alors

$$[A|B \quad \text{et} \quad A|C] \quad \Longrightarrow \quad A|\,(PB + QC)\,.$$

**Proposition 1.4**

Soit $A, B \in \mathbb{K}[X]$.
- Si $B \neq 0$, alors
$$A|B \quad \Longrightarrow \quad \deg A \leqslant \deg B.$$
- Si $A|B$ et $\deg A = \deg B$, alors $A$ et $B$ sont associés.

## 1.2 Plus grand commun diviseur

**Définition 1.5**

Soit $A, B \in \mathbb{K}[X]$. Il existe un unique polynôme unitaire ou nul $P$ tel que

— $P|A$ et $P|B$.

— $\forall Q \in \mathbb{K}[X], \quad [Q|A \text{ et } Q|B] \Longrightarrow Q|P$.

On l'appelle pgcd (plus grand commun diviseur) de $A$ et de $B$ et on le note $\operatorname{pgcd}(A, B)$, $(A, B)$ ou $A \wedge B$.

**Remarque**

⇨ Soit $A, B \in \mathbb{K}[X]$. Si l'un des deux polynômes est non nul, le pgcd de $A$ et $B$ est le polynôme unitaire de plus grand degré qui divise $A$ et $B$.

**Proposition 1.6**

$$\begin{aligned} \forall A \in \mathbb{K}[X], \quad & A \wedge 0 = A_u \\ \forall A \in \mathbb{K}[X], \quad & A \wedge 1 = 1 \\ \forall A, B \in \mathbb{K}[X], \quad & A \wedge B = 0 \Longleftrightarrow [A = 0 \quad \text{et} \quad B = 0] \end{aligned}$$

**Proposition 1.7**

$$\begin{aligned} \forall A, B \in \mathbb{K}[X], \quad & A \wedge B = B \wedge A \\ \forall A, B \in \mathbb{K}[X], \quad \forall \lambda, \mu \in \mathbb{K}^*, \quad & A \wedge B = (\lambda A) \wedge (\mu B) = A_u \wedge B_u \\ \forall A, B, P \in \mathbb{K}[X], \quad & (PA) \wedge (PB) = P_u (A \wedge B) \end{aligned}$$

**Définition 1.8**

Soit $A_1, \ldots, A_n \in \mathbb{K}[X]$. Il existe un unique polynôme unitaire ou nul $P$ tel que

— $\forall i \in [\![1, n]\!], \quad P|A_i$.

— $\forall Q \in \mathbb{K}[X], \quad [\forall i \in [\![1, n]\!], \quad Q|A_i] \Longrightarrow Q|P$.

On l'appelle pgcd (plus grand commun diviseur) de la famille $(A_1, \ldots, A_n)$ et on le note $\operatorname{pgcd}(A_1, \ldots, A_n)$, ou $A_1 \wedge \cdots \wedge A_n$.

**Remarque**

⇨ Le pgcd d'une famille $(A_1, \ldots, A_n)$ de polynômes ne dépend pas de l'ordre de ces derniers.

**Proposition 1.9**

Soit $A_1, \ldots, A_n \in \mathbb{K}[X]$ et $p \in [\![1, n-1]\!]$. Alors

$$A_1 \wedge \cdots \wedge A_n = (A_1 \wedge \cdots \wedge A_p) \wedge (A_{p+1} \wedge \cdots \wedge A_n).$$

## 1.3 Algorithme d'Euclide

**Proposition 1.10**

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

$$A \wedge B = A \wedge (B + PA) = (A + PB) \wedge B.$$

En particulier, si $B \neq 0$ et $R$ est le reste de la division euclidienne de $A$ par $B$, on a

$$A \wedge B = B \wedge R.$$

**Exercice 1**

⇨ Calculer $A \wedge B$ où $A := X^4 - X^3 + X^2 + X - 2$ et $B := X^3 + X^2 - X - 1$.

## 1.4 Relation de Bézout

**Proposition 1.11**

Si $A, B \in \mathbb{K}[X]$, alors il existe $U, V \in \mathbb{K}[X]$ tels que

$$UA + VB = A \wedge B.$$

**Remarques**

- ⇨ Les polynômes $U$ et $V$ sont appelés polynômes de Bézout.
- ⇨ Le couple $(U, V)$ n'est pas unique. En effet, si $(U_0, V_0) \in \mathbb{K}[X]^2$ est un couple de polynômes de Bézout, alors pour tout $P \in \mathbb{K}[X]$, $(U_0 + PB, V_0 - PA)$ en est un autre.

**Exercice 2**

- ⇨ Calcul d'un couple de polynômes de Bézout pour $A = (X-1)^2$ et $B = (X+2)^2$.

**Définition 1.12**

Soit $A, B \in \mathbb{K}[X]$. On dit que $A$ et $B$ sont premiers entre eux lorsque $A \wedge B = 1$.

**Remarques**

- ⇨ Si $\alpha, \beta \in \mathbb{K}$ sont distincts, alors $(X - \alpha) \wedge (X - \beta) = 1$.
- ⇨ Deux polynômes premiers entre eux n'admettent aucune racine commune. Cependant, la réciproque est fausse. En effet, si $\mathbb{K} = \mathbb{R}$, $P := X^2 + 1$ n'admet aucune racine réelle, donc aucune racine commune avec lui-même. Pourtant $P \wedge P = P \neq 1$.

**Exercice 3**

- ⇨ Montrer que si $A$ et $B$ sont premiers entre eux, il en est de même pour $A - B$ et $A + B$.

**Proposition 1.13**

Soit $A, B \in \mathbb{K}[X]$. Alors $A$ et $B$ sont premiers entre eux si et seulement si il existe $U, V \in \mathbb{K}[X]$ tels que

$$UA + VB = 1.$$

**Proposition 1.14**

- Soit $A, B, C \in \mathbb{K}[X]$ tels que $A \wedge B = 1$ et $A \wedge C = 1$. Alors $A \wedge (BC) = 1$.
- Plus généralement, si $A \in \mathbb{K}[X]$ est premier avec chaque élément d'une famille de polynômes $B_1, \dots, B_n \in \mathbb{K}[X]$, alors $A$ est premier avec leur produit.
- Soit $A, B \in \mathbb{K}[X]$ deux polynômes premiers entre eux et $m, n \in \mathbb{N}$. Alors $A^m \wedge B^n = 1$.

**Définition 1.15**

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

- On dit que $A_1, \dots, A_n$ sont deux à deux premiers entre eux lorsque

$$\forall i, j \in [\![1, n]\!], \quad i \neq j \Longrightarrow A_i \wedge A_j = 1.$$

- On dit que $A_1, \dots, A_n$ sont premiers entre eux dans leur ensemble lorsque

$$A_1 \wedge \cdots \wedge A_n = 1.$$

**Remarque**

- ⇨ Si les polynômes $A_1, \dots, A_n$ sont deux à deux premiers entre eux, alors ils sont premiers entre eux dans leur ensemble. Cependant, la réciproque est fausse. Par exemple, les polynômes $A_1 = (X-2)(X-3)$, $A_2 = (X-1)(X-3)$ et $A_3 = (X-1)(X-2)$ sont premiers entre eux dans leur ensemble mais ne sont pas deux à deux premiers entre eux.

**Proposition 1.16**

Soit $A_1, \dots, A_n \in \mathbb{K}[X]$. Alors $A_1, \dots, A_n$ sont premiers entre eux dans leur ensemble si et seulement si il existe $U_1, \dots, U_n \in \mathbb{K}[X]$ tels que

$$U_1 A_1 + \cdots + U_n A_n = 1.$$

## 1.5 Lemme de Gauss

**Proposition 1.17: Lemme de Gauss**

Soit $A, B, C \in \mathbb{K}[X]$. Alors
$$[A|BC \quad \text{et} \quad A \wedge B = 1] \quad \Longrightarrow \quad A|C.$$

**Remarque**

⇨ Si $A, B \in \mathbb{K}[X]$ sont premiers entre eux et le couple $(U_0, V_0) \in \mathbb{K}[X]^2$ est tel que $U_0A + V_0B = 1$, l'ensemble des couples de polynômes de Bézout pour $A$ et $B$ est
$$\{(U_0 + PB, V_0 - PA) \mid P \in \mathbb{K}[X]\}$$

**Proposition 1.18**

- Soit $A, B, C \in \mathbb{K}[X]$. On suppose que $A|C$, $B|C$ et $A \wedge B = 1$. Alors $AB|C$.
- Plus généralement si $A \in \mathbb{K}[X]$ est divisé par chaque élément d'une famille $B_1, \dots, B_n \in \mathbb{K}[X]$ de polynômes deux à deux premiers entre eux, alors il est divisé par leur produit.

## 1.6 Plus petit commun multiple

**Définition 1.19**

Soit $A, B \in \mathbb{K}[X]$. Il existe un unique polynôme unitaire ou nul $P$ tel que
- $A|P \quad \text{et} \quad B|P$.
- $\forall Q \in \mathbb{K}[X], \quad [A|Q \quad \text{et} \quad B|Q] \Longrightarrow P|Q$.

On l'appelle ppcm (plus petit commun multiple) de $A$ et de $B$ et on le note $\operatorname{ppcm}(A, B)$, ou $A \vee B$.

**Proposition 1.20**

$$\begin{aligned}
\forall A \in \mathbb{K}[X], &\qquad A \vee 0 = 0\\
\forall A \in \mathbb{K}[X], &\qquad A \vee 1 = A_u\\
\forall A, B \in \mathbb{K}[X], &\qquad A \vee B = 0 \Longleftrightarrow [A = 0 \quad \text{ou} \quad B = 0]
\end{aligned}$$

**Proposition 1.21**

$$\begin{aligned}
\forall A, B \in \mathbb{K}[X], &\qquad A \vee B = B \vee A\\
\forall A, B \in \mathbb{K}[X], \quad \forall \lambda, \mu \in \mathbb{K}^*, &\qquad A \vee B = (\lambda A) \vee (\mu B) = A_u \vee B_u\\
\forall A, B, P \in \mathbb{K}[X], &\qquad (PA) \vee (PB) = P_u\,(A \vee B)
\end{aligned}$$

**Proposition 1.22**

Soit $A, B \in \mathbb{K}[X]$.
- Si $A \wedge B = 1$, alors
$$A \vee B = (AB)_u\,.$$
- De manière générale
$$(A \wedge B)\,(A \vee B) = (AB)_u\,.$$

## 1.7 Polynôme irréductible

**Définition 1.23**

On dit qu'un polynôme $P \in \mathbb{K}[X]$ de degré supérieur ou égal à 1 est irréductible lorsque ses seuls diviseurs sont les polynômes associés à 1 ou à $P$.

**Remarques**

⇨ Un polynôme $P$ de degré supérieur ou égal à 1 est irréductible si et seulement si ses diviseurs sont de degré 0 ou de même degré que $P$.

- ⇨ Si $\alpha \in \mathbb{K}$, $P \coloneqq X - \alpha$ est irréductible. Plus généralement, les polynômes de degré 1 sont irréductibles.
- ⇨ Les polynômes de degré supérieur ou égal à 2 admettant une racine ne sont pas irréductibles.
- ⇨ Réciproquement, un polynôme $P \in \mathbb{K}[X]$ de degré 2 ou 3 n'admettant aucune racine dans $\mathbb{K}$ est irréductible. En particulier, les polynômes de $\mathbb{R}[X]$ de degré 2 dont le discriminant est strictement négatif sont irréductibles. Cependant, il existe des polynômes $P \in \mathbb{K}[X]$ n'admettant aucune racine dans $\mathbb{K}$ et qui ne sont pas irréductibles. Par exemple le polynôme $P = (X^2+1)^2$ n'admet aucune racine dans $\mathbb{R}$ sans être irréductible.

**Proposition 1.24**

Soit $P$ un polynôme irréductible et $A \in \mathbb{K}[X]$. Alors $P|A$ ou $P \wedge A = 1$.

**Proposition 1.25**

Soit $P \in \mathbb{K}[X]$ un polynôme irréductible.

— Si $A, B \in \mathbb{K}[X]$

$$P|AB \iff [P|A \quad \text{ou} \quad P|B] \,.$$

— Plus généralement, $P$ divise un produit si et seulement si il divise un de ses facteurs.

**Proposition 1.26**

Tout polynôme non constant admet un diviseur irréductible.

**Remarque**

- ⇨ En particulier, un polynôme est associé à 1 si et seulement si il n'admet aucun diviseur irréductible.

**Définition 1.27**

Lorsque $A \in \mathbb{K}[X] \setminus \{0\}$ et $P$ est un polynôme unitaire irréductible, on appelle *valuation de $P$ dans $A$* et on note $\mathrm{Val}_P(A)$ le plus grand $\alpha \in \mathbb{N}$ tel que $P^\alpha | A$.

**Remarques**

- ⇨ Soit $P$ et $Q$ sont deux polynômes unitaires irréductibles. Alors

$$\mathrm{Val}_P(Q) = \begin{cases} 1 & \text{si } P = Q, \\ 0 & \text{sinon.} \end{cases}$$

- ⇨ Si $A \in \mathbb{K}[X] \setminus \{0\}$, il n'existe qu'un nombre fini de polynômes unitaires irréductibles $P$ tels que $\mathrm{Val}_P(A) > 0$.

**Proposition 1.28**

Soit $A, B \in \mathbb{K}[X] \setminus \{0\}$ et $P$ un polynôme unitaire irréductible. Alors

$$\mathrm{Val}_P\,(AB) = \mathrm{Val}_P(A) + \mathrm{Val}_P(B).$$

**Remarque**

- ⇨ Plus généralement, si $P$ est un polynôme unitaire irréductible, $A_1, \ldots, A_r \in \mathbb{K}[X] \setminus \{0\}$ et $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$, alors

$$\mathrm{Val}_P\left(\prod_{k=1}^{r} A_k^{\alpha_k}\right) = \sum_{k=1}^{r} \alpha_k \mathrm{Val}_P\,(A_k)\,.$$

**Théorème 1.29: Factorisation irréductible**

Soit $A \in \mathbb{K}[X] \setminus \{0\}$. Alors, il existe $\lambda \in \mathbb{K}^*$, $P_1, \ldots, P_r$ des polynômes unitaires irréductibles deux à deux distincts et $\alpha_1, \ldots, \alpha_r \in \mathbb{N}^*$ tels que

$$A = \lambda \prod_{k=1}^{r} P_k^{\alpha_k}.$$

De plus, à permutation près des $P_k$, cette décomposition est unique.

**Remarque**

⇨ Soit $A \in \mathbb{K}[X] \setminus \{0\}$. On note $\lambda \in \mathbb{K}^*$ le coefficient dominant de $A$. Alors la factorisation irréductible de $A$ s'écrit

$$A = \lambda \prod_{P \in \mathcal{I}} P^{\mathrm{Val}_P(A)},$$

où $\mathcal{I}$ désigne l'ensemble des polynômes unitaires irréductibles de $\mathbb{K}[X]$. Ce produit ne contient qu'un nombre fini de termes différents de 1.

**Proposition 1.30**

Soit $A, B \in \mathbb{K}[X] \setminus \{0\}$. Alors

— $A|B$ si et seulement si

$$\forall P \in \mathcal{I}, \quad \mathrm{Val}_P(A) \leqslant \mathrm{Val}_P(B).$$

— $A$ et $B$ sont associés si et seulement si

$$\forall P \in \mathcal{I}, \quad \mathrm{Val}_P(A) = \mathrm{Val}_P(B).$$

**Proposition 1.31**

Soit $A, B \in \mathbb{K}[X] \setminus \{0\}$. Alors le pgcd et le ppcm de $A$ et $B$ sont donnés par les relations

$$\begin{aligned} \forall P \in \mathcal{I}, \quad \mathrm{Val}_P(A \wedge B) &= \min\left(\mathrm{Val}_P(A), \mathrm{Val}_P(B)\right), \\ \mathrm{Val}_P(A \vee B) &= \max\left(\mathrm{Val}_P(A), \mathrm{Val}_P(B)\right). \end{aligned}$$

## 1.8 Changement de corps

**Définition 1.32**

Soit $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{C}[X]$. On définit le polynôme $\overline{P} \in \mathbb{C}[X]$ par

$$\overline{P} := \overline{a_0} + \overline{a_1} X + \cdots + \overline{a_n} X^n.$$

**Remarque**

⇨ Si $P \in \mathbb{C}[X]$ et $z \in \mathbb{C}$, alors

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

**Proposition 1.33**

Soit $P, Q \in \mathbb{C}[X]$.

— Si $\lambda, \mu \in \mathbb{C}$, alors

$$\begin{aligned} \overline{\lambda P + \mu Q} &= \overline{\lambda}\,\overline{P} + \overline{\mu}\,\overline{Q} \\ \overline{PQ} &= \overline{P}\,\overline{Q} \end{aligned}$$

— $\deg \overline{P} = \deg P$.

**Proposition 1.34**

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

$$\overline{\overline{P}} = P \qquad \text{et} \qquad \left[P \in \mathbb{R}[X] \quad \Longleftrightarrow \quad \overline{P} = P\right].$$

Si $\mathbb{L}$ est un corps, $\mathbb{K}$ est un sous-corps de $\mathbb{L}$ et $P \in \mathbb{K}[X]$, certaines notions que nous avons définies peuvent différer selon qu'on considère $P$ comme un élément de $\mathbb{K}[X]$ ou comme un élément de $\mathbb{L}[X]$. Par exemple, si $P := X^2+1 \in \mathbb{R}[X]$, alors $P$ est irréductible dans $\mathbb{R}[X]$ car c'est un polynôme de degré 2 qui n'admet pas de racine dans $\mathbb{R}$. Cependant, il n'est pas irréductible dans $\mathbb{C}[X]$ car $P = (X - \mathrm{i})(X + \mathrm{i})$. Nous allons voir cependant que les notions de division euclidienne, de divisibilité, de pgcd et de ppcm ne dépendent pas du corps.

**Proposition 1.35**

Soit $\mathbb{L}$ un corps, $\mathbb{K}$ un sous-corps de $\mathbb{L}$ et $A, B \in \mathbb{K}[X]$ tels que $B \neq 0$. Alors, le quotient et le reste de la division euclidienne de $A$ par $B$ dans $\mathbb{L}[X]$ sont les mêmes que dans $\mathbb{K}[X]$.

**Proposition 1.36**

Soit $\mathbb{L}$ un corps, $\mathbb{K}$ un sous-corps de $\mathbb{L}$ et $A, B \in \mathbb{K}[X]$. Alors
- — $A$ divise $B$ dans $\mathbb{L}[X]$ si et seulement si $A$ divise $B$ dans $\mathbb{K}[X]$.
- — Le pgcd et le ppcm de $A$ et $B$ dans $\mathbb{L}[X]$ sont les mêmes que ceux dans $\mathbb{K}[X]$.

# 2 Racines d'un polynôme

## 2.1 Racine

**Proposition 2.1**

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Alors $\alpha$ est une racine de $P$ si et seulement si $X - \alpha$ divise $P$.

**Remarque**

⇨ Si $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$ et $x = p/q$ est une racine rationnelle de $P$ mise sous forme irréductible, alors $q | a_n$ et $p | a_0$. Cette relation nous permet de trouver les racines rationnelles de $P$. Par exemple, si $P = 2X^3 + 5X^2 + X - 3$ et $p/q$ est une racine rationnelle de $P$ mise sous forme irréductible, alors $q|2$ et $p|3$ donc $p \in \{-3, -1, 1, 3\}$ et $q \in \{1, 2\}$. Réciproquement, on constate que seul $-3/2$ est une racine de $P$. On peut donc factoriser $P$ par $2X + 3$. On obtient $P = (2X+3)\left(X^2 + X - 1\right)$, ce qui permet d'obtenir toutes les racines de $P$.

**Définition 2.2**

Soit $P \in \mathbb{K}[X]$ un polynôme non nul et $\alpha \in \mathbb{K}$. On appelle *multiplicité* de $\alpha$ dans $P$ le plus grand entier $\omega \in \mathbb{N}$ tel que $(X - \alpha)^\omega | P$.

**Remarques**

⇨ La multiplicité de $\alpha$ dans $P$ sera parfois notée $\omega(\alpha, P)$.

⇨ L'entier $\omega \in \mathbb{N}$ est la multiplicité de $\alpha$ dans $P$ si et seulement si il existe $Q \in \mathbb{K}[X]$ tel que

$$P = (X - \alpha)^\omega Q \qquad \text{et} \qquad Q(\alpha) \neq 0.$$

⇨ L'élément $\alpha$ est une racine de $P$ si et seulement si $\omega(\alpha, P) \geqslant 1$. Si $\alpha$ est une racine de $P$, on dit que c'est une *racine simple* lorsque $\omega(\alpha, P) = 1$ et que c'est une *racine double* lorsque $\omega(\alpha, P) = 2$.

⇨ L'élément $\alpha$ n'est pas une racine de $P$ si et seulement si $\omega(\alpha, P) = 0$. On se permet donc parfois de dire que $\alpha$ est racine de $P$ de multiplicité nulle pour signifier que $\alpha$ n'est pas racine de $P$.

⇨ La multiplicité de $\alpha$ dans $P$ n'est rien d'autre que la valuation de $X - \alpha$ dans $P$.

**Proposition 2.3**

Soit $\mathbb{K}$ un corps de caractéristique nulle, $P \in \mathbb{K}[X]$ un polynôme non nul et $\alpha \in \mathbb{K}$. Si $\alpha$ est de multiplicité $\omega \geqslant 1$ dans $P$, alors $\alpha$ est de multiplicité $\omega - 1$ dans $P'$.

**Proposition 2.4**

Soit $\mathbb{K}$ un corps de caractéristique nulle, $P \in \mathbb{K}[X]$ un polynôme non nul, $\alpha \in \mathbb{K}$ et $\omega \in \mathbb{N}$. Alors les deux assertions suivantes sont équivalentes.
- — $\alpha$ est de multiplicité $\omega$ dans $P$.
- — $P(\alpha) = 0, P'(\alpha) = 0, \ldots, P^{(\omega-1)}(\alpha) = 0$ et $P^{(\omega)}(\alpha) \neq 0$.

**Exercice 4**

⇨ Calculer la multiplicité de 1 dans $P \coloneqq X^4 - 2X^3 + 2X^2 - 2X + 1$.

**Proposition 2.5**

Soit $P \in \mathbb{C}[X]$ un polynôme non nul et $\alpha \in \mathbb{C}$. Alors la multiplicité de $\bar{\alpha}$ dans $\bar{P}$ est égale à celle de $\alpha$ dans $P$.

**Remarque**

⇨ En particulier, si $\alpha \in \mathbb{C}$ est une racine de $P \in \mathbb{R}[X]$, alors $\overline{\alpha}$ est une racine de $P$ et sa multiplicité dans $P$ est la même que celle de $\alpha$ dans $P$.

**Proposition 2.6**

Soit $P \in \mathbb{K}[X]$ un polynôme non nul de degré $n \in \mathbb{N}$. On suppose que $P$ admet (au moins) $r$ racines $\alpha_1, \dots, \alpha_r \in \mathbb{K}$ deux à deux distinctes ayant des multiplicités respectives (au moins) égales à $\omega_1, \dots, \omega_r \in \mathbb{N}$. Alors, il existe $Q \in \mathbb{K}[X]$ tel que

$$P = (X - \alpha_1)^{\omega_1} \cdots (X - \alpha_r)^{\omega_r} Q.$$

En particulier $\omega_1 + \cdots + \omega_r \leqslant n$.

**Proposition 2.7**

Tout polynôme de degré $n \in \mathbb{N}$ admet au plus $n$ racines comptées avec leurs multiplicités.

**Remarque**

⇨ Un polynôme de degré inférieur ou égal à $n \in \mathbb{N}$ admettant au moins $n+1$ racines comptées avec leurs multiplicités est donc nul.

**Définition 2.8**

Soit $P \in \mathbb{K}[X]$ un polynôme non nul de degré $n \in \mathbb{N}$.

— On dit que $P$ est *scindé* lorsqu'il admet exactement $n$ racines comptées avec leurs multiplicités, c'est-à-dire lorsqu'il existe $\lambda \in \mathbb{K}^*$, $\alpha_1, \dots, \alpha_r \in \mathbb{K}$ et $\omega_1, \dots, \omega_r \in \mathbb{N}^*$ tels que

$$P = \lambda \prod_{k=1}^{r} (X - \alpha_k)^{\omega_k}.$$

— On dit que $P$ est *scindé simple* lorsqu'il admet exactement $n$ racines simples, c'est-à-dire lorsqu'il existe $\lambda \in \mathbb{K}^*$ et $\alpha_1, \dots, \alpha_n \in \mathbb{K}$ deux à deux distincts tels que

$$P = \lambda \prod_{k=1}^{n} (X - \alpha_k).$$

**Remarques**

⇨ Un polynôme non nul $P \in \mathbb{K}[X]$ de degré $n$ est scindé si et seulement si il existe $\lambda \in \mathbb{K}^*$ et $\alpha_1, \dots, \alpha_n \in \mathbb{K}$ tels que

$$P = \lambda \prod_{k=1}^{n} (X - \alpha_k).$$

De plus, $P$ est scindé simple si et seulement si les $\alpha_k$ sont deux à deux distincts.

⇨ La notion de polynôme scindé dépend du corps considéré. Par exemple, le polynôme $P := X^2 + 1$ est scindé (simple) sur $\mathbb{C}$ car $P = (X - \mathrm{i})(X + \mathrm{i})$. Cependant, il n'est pas scindé sur $\mathbb{R}$, car il n'admet aucune racine réelle.

**Proposition 2.9**

Soit $P \in \mathbb{K}[X]$ un polynôme non nul de degré $n \in \mathbb{N}$.

— On suppose que $P$ admet (au moins) $r$ racines $\alpha_1, \dots, \alpha_r \in \mathbb{K}$ deux à deux distinctes de multiplicités (au moins) $\omega_1, \dots, \omega_r \in \mathbb{N}$ telles que $\omega_1 + \cdots + \omega_r = n$. Alors $P$ est scindé et en notant $\lambda \in \mathbb{K}^*$ le coefficient dominant de $P$, on a

$$P = \lambda \prod_{k=1}^{r} (X - \alpha_k)^{\omega_k}.$$

En particulier $\alpha_1, \dots, \alpha_r$ sont les seules racines de $P$ et leurs multiplicités dans $P$ sont $\omega_1, \dots, \omega_r$.

— On suppose que $P$ admet (au moins) $n$ racines $\alpha_1, \dots, \alpha_n \in \mathbb{K}$ deux à deux distinctes. Alors $P$ est scindé simple et en notant $\lambda \in \mathbb{K}^*$ le coefficient dominant de $P$, on a

$$P = \lambda \prod_{k=1}^{n} (X - \alpha_k).$$

En particulier $\alpha_1, \dots, \alpha_n$ sont les seules racines de $P$ et elles sont simples.

**Exercice 5**

⇨ Soit $n \in \mathbb{N}^*$. Factoriser $X^n - 1$ sur $\mathbb{C}[X]$.

## 2.2 Théorème fondamental de l'algèbre

**Théorème 2.10: Théorème de d'Alembert-Gauss**

Tout polynôme de $\mathbb{C}[X]$ de degré supérieur ou égal à 1 admet au moins une racine dans $\mathbb{C}$.

**Exercice 6**

⇨ Soit $P \in \mathbb{C}[X]$ est de degré supérieur ou égal à 1. Montrer que l'application $\tilde{P}$ de $\mathbb{C}$ dans $\mathbb{C}$ qui à $z$ associe $P(z)$ est surjective.

**Proposition 2.11**

Les polynômes unitaires irréductibles de $\mathbb{C}[X]$ sont les $X - \alpha$ avec $\alpha \in \mathbb{C}$.

**Remarques**

⇨ Soit $P$ et $Q$ deux polynômes non nuls de $\mathbb{C}[X]$. Alors $P$ divise $Q$ si et seulement si toute racine de $P$ est racine de $Q$ et sa multiplicité dans $P$ est inférieure ou égale à sa multiplicité dans $Q$.

⇨ Dans $\mathbb{C}[X]$, deux polynômes non nuls sont premiers entre eux si et seulement si ils n'admettent aucune racine commune. Deux polynômes de $\mathbb{R}[X]$ sont premiers entre eux si et seulement si ils n'admettent aucune racine commune dans $\mathbb{C}$.

⇨ Un polynôme non nul $P \in \mathbb{C}[X]$ est scindé simple si et seulement si $P$ et $P'$ sont premiers entre eux.

**Proposition 2.12: Factorisation irréductible dans $\mathbb{C}[X]$**

Soit $P \in \mathbb{C}[X]$ un polynôme non nul. Alors, il existe $\alpha_1, \ldots, \alpha_r \in \mathbb{C}$ deux à deux distincts, $\omega_1, \ldots, \omega_r \in \mathbb{N}^*$ et $\lambda \in \mathbb{C}^*$ tels que

$$P = \lambda \prod_{k=1}^{r} (X - \alpha_k)^{\omega_k}.$$

De plus, à permutation près de $(\alpha_k, \omega_k)$, cette décomposition est unique.

**Remarques**

⇨ Les polynômes non nuls de $\mathbb{C}[X]$ sont donc scindés.

⇨ En pratique, cette décomposition est équivalente à la recherche du coefficient dominant de $P$, de ses racines et de leurs multiplicités. Deux polynômes non nuls de $\mathbb{C}[X]$ sont donc égaux si et seulement si ils ont le même coefficient dominant et les mêmes racines avec les mêmes multiplicités.

**Exercices 7**

⇨ Montrer que $X^2 + 1$ divise $X^n + X$ si et seulement si $n \equiv 3$ $[4]$.

⇨ Soit $n, m \in \mathbb{N}^*$. Montrer que $(X^n - 1) \wedge (X^m - 1) = X^{n \wedge m} - 1$.

**Proposition 2.13**

Les polynômes unitaires irréductibles de $\mathbb{R}[X]$ sont les
- $X - \alpha$ avec $\alpha \in \mathbb{R}$.
- $X^2 + bX + c$ avec $\Delta = b^2 - 4c < 0$.

**Proposition 2.14: Factorisation irréductible dans $\mathbb{R}[X]$**

Soit $P \in \mathbb{R}[X]$ un polynôme non nul. Alors, il existe $\alpha_1, \ldots, \alpha_r \in \mathbb{R}$ deux à deux distincts, $\omega_1, \ldots, \omega_r \in \mathbb{N}^*$, $(b_1, c_1), \ldots, (b_s, c_s) \in \mathbb{R}^2$ deux à deux distincts tels que $\Delta_l = b_l^2 - 4c_l < 0$ pour tout $l \in [\![1, s]\!]$, $\omega'_1, \ldots, \omega'_s \in \mathbb{N}^*$ et $\lambda \in \mathbb{R}^*$ tels que

$$P = \lambda \prod_{k=1}^{r} (X - \alpha_k)^{\omega_k} \prod_{l=1}^{s} \left(X^2 + b_l X + c_l\right)^{\omega'_l}.$$

De plus, à permutation près des $(\alpha_k, \omega_k)$ et des $(b_l, c_l, \omega'_l)$, cette décomposition est unique.

**Remarque**

⇨ En pratique, si on a effectué la décomposition de $P \in \mathbb{R}[X]$ en produit de polynômes unitaires irréductibles dans $\mathbb{C}[X]$, il suffit de regrouper les racines conjuguées et de développer ces produits pour obtenir la décomposition dans $\mathbb{R}[X]$. En effet, si $\alpha \in \mathbb{C}$

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

Cependant, il est parfois possible d'aboutir plus rapidement à la décomposition dans $\mathbb{R}[X]$ en utilisant les identités algébriques.

**Exercices 8**

⇨ Factoriser $X^6 - 1$ et $X^4 + 1$ sur $\mathbb{R}[X]$.

⇨ Soit $n \in \mathbb{N}^*$. Factoriser $X^n - 1$ sur $\mathbb{R}[X]$.

## 2.3 Fonctions symétriques élémentaires

Soit $P \coloneqq X^3 + aX^2 + bX + c \in \mathbb{K}[X]$ un polynôme unitaire scindé de degré 3 et $\alpha, \beta, \gamma \in \mathbb{K}$ ses racines comptées avec leurs multiplicités. Alors

$$\begin{aligned} P &= X^3 + aX^2 + bX + c \\ &= (X - \alpha)(X - \beta)(X - \gamma) \\ &= X^3 - (\alpha + \beta + \gamma) X^2 + (\alpha\beta + \alpha\gamma + \beta\gamma) X - \alpha\beta\gamma \\ &= X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3. \end{aligned}$$

où $\sigma_1 \coloneqq \alpha + \beta + \gamma$, $\sigma_2 \coloneqq \alpha\beta + \alpha\gamma + \beta\gamma$ et $\sigma_3 \coloneqq \alpha\beta\gamma$. Par unicité des coefficients de $P$, on a $\sigma_1 = -a$, $\sigma_2 = b$ et $\sigma_3 = -c$. Remarquons que $\sigma_1, \sigma_2$ et $\sigma_3$ sont des expressions symétriques en $\alpha, \beta, \gamma$, c'est-à-dire qu'elles sont invariantes par permutation de ces 3 variables. On peut montrer que toute expression polynomiale symétrique en $\alpha, \beta, \gamma$ peut s'exprimer comme un polynôme en ces 3 quantités. Par exemple $\Sigma \coloneqq \alpha^2 + \beta^2 + \gamma^2$ est symétrique en $\alpha, \beta, \gamma$ et on remarque que

$$\begin{aligned} \sigma_1^2 &= (\alpha + \beta + \gamma)^2 \\ &= \alpha^2 + \beta^2 + \gamma^2 + 2(\alpha\beta + \alpha\gamma + \beta\gamma) \\ &= \Sigma + 2\sigma_2 \end{aligned}$$

donc $\Sigma = \sigma_1^2 - 2\sigma_2$. Ainsi, toute expression symétrique en les racines de $P$ s'exprime en fonction des coefficients de $P$. Dans notre cas, on trouve $\Sigma = a^2 - 2b$.

**Définition 2.15**

Soit $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$. On définit les *polynômes symétriques élémentaires* en les $\alpha_1, \ldots, \alpha_n$ par

$$\begin{aligned} \sigma_1 &\coloneqq \alpha_1 + \cdots + \alpha_n \\ \sigma_2 &\coloneqq \sum_{i_1 < i_2} \alpha_{i_1}\alpha_{i_2} \\ &\vdots \\ \sigma_n &\coloneqq \alpha_1 \cdots \alpha_n. \end{aligned}$$

Plus précisément, pour tout $k \in [\![1, n]\!]$

$$\sigma_k \coloneqq \sum_{i_1 < \cdots < i_k} \alpha_{i_1} \cdots \alpha_{i_k}.$$

**Remarque**

⇨ On peut montrer que tout polynôme symétrique en les $\alpha_1, \ldots, \alpha_n$ s'écrit comme un polynôme en les $\sigma_1, \ldots, \sigma_n$. Cette propriété justifie leur appellation de polynômes symétriques *élémentaires*.

**Proposition 2.16: Relations coefficients-racines, formules de Viète**

Soit $P \in \mathbb{K}[X]$ un polynôme scindé de degré $n$. Alors il existe $a_0, \ldots, a_n \in \mathbb{K}$ et $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ tels que

$$\begin{aligned} P &= a_0 + a_1 X + \cdots + a_n X^n \\ &= a_n \prod_{k=1}^{n} (X - \alpha_k). \end{aligned}$$

Alors

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

**Exercices 9**

⇨ Soit $z_1, z_2, z_3 \in \mathbb{C}$ les racines de $P \coloneqq 2X^3 + 3X^2 + X + 1$. Calculer

$$a \coloneqq \sum_{k=1}^{3} z_k^2, \qquad b \coloneqq \sum_{k=1}^{3} z_k^3, \qquad c \coloneqq \sum_{k=1}^{3} \frac{1}{z_k}.$$

⇨ Montrer que si $n \geqslant 2$, la somme des racines $n$-ièmes de l'unité est nulle et le produit des racines $n$-ièmes de l'unité est égal à $(-1)^{n-1}$.