Les polynômes

Table des matières

1 L'algèbre des polynômes

1.1 Le groupe des polynômes

Notation. A désigne un anneau quelconque. Par exemple, on peut avoir $A = \mathbb{R}$ ou $A = \mathbb{C}$, mais tout autre anneau est envisageable.

Définition. On note $A[X] \triangleq A^{(\mathbb{N})}$: c'est l'ensemble des suites $(a_k)_{k\in\mathbb{N}}$ d'éléments de A telles que $\{k \in \mathbb{N}/a_k \neq 0\}$ est fini.
Les éléments de $A[X]$ sont appelés des polynômes à coefficients dans A.

Si $P = (a_k) \in A[X]$, on convient de noter $P = \sum_{k\in\mathbb{N}} a_k X^k$, ou encore $P(X) = \sum_{k=0}^{n} a_k X^k$ où n est un entier naturel tel que $a_k = 0$ pour tout $k \geq n$.
Cette notation sera justifiée un peu plus loin.
X s'appelle l'indéterminée.

Exemple. $P(X) = (a_k)_{k\in\mathbb{N}}$ est un polynôme si $a_0 = 0 = a_1$, $a_2 = 1$, $a_3 = -6$, $a_4 = 2$ et, pour tout $k \geq 5$, $a_k = 0$. Dans ce cas, on écrit $P(X) = X^2 - 6X^3 + 2X^4$.

Remarque. Par définition, deux polynômes sont égaux si et seulement si ils ont les mêmes coefficients.

Propriété. $(A[X], +)$ est un sous-groupe commutatif de $A^{\mathbb{N}}$. Son élément neutre est $(0_A)_{n\in\mathbb{N}}$, que l'on appelle le polynôme identiquement nul.

Démonstration.
On sait que $A^{\mathbb{N}} = \mathcal{F}(\mathbb{N}, A)$ est un groupe si l'on convient que $(a_k) + (b_k) = (a_k + b_k)$.
La suite identiquement nulle est un élément de $A[X]$, donc $A[X] \neq \emptyset$.
Soit $(a_k), (b_k) \in A[X]$: $\{k \in \mathbb{N}/a_k - b_k \neq 0\} \subset \{k \in \mathbb{N}/a_k \neq 0\} \cup \{k \in \mathbb{N}/b_k \neq 0\}$,

or $\{k \in \mathbb{N}/a_k \neq 0\}$ et $\{k \in \mathbb{N}/b_k \neq 0\}$ sont finis, donc $\{k \in \mathbb{N}/a_k - b_k \neq 0\}$ est également fini, ce qui prouve que $(a_k) - (b_k) \in A[X]$. □

Remarque. Si $P(X) = \sum_{k\in\mathbb{N}} a_k X^k$ et $Q(X) = \sum_{k\in\mathbb{N}} b_k X^k$, alors $P+Q = \sum_{k\in\mathbb{N}} (a_k+b_k)X^k$.

Définition. Soit $P(X) = (a_k)_{k\in\mathbb{N}} \in A[X] \setminus \{0\}$. Alors $\{k \in \mathbb{N}/a_k \neq 0\}$ est une partie finie et non vide de $\mathbb{N}$, donc elle possède un maximum, que l'on appelle le degré du polynôme P. On le note $\deg(P)$ ou bien $d(P)$.
De plus, on convient que $\deg(0) = -\infty$.

Exemple. $d(5X^3 - X + 2) = 3$.

Définition. Soit $P(X) = \sum_{k\in\mathbb{N}} a_k X^k \in A[X]$ un polynôme de degré $n \in \mathbb{N}$.

- Pour tout $k \in \mathbb{N}$, a_k est le coefficient de P de degré k.
- a_0 est aussi appelé le coefficient constant du polynôme P.
- a_n est appelé le coefficient de plus haut degré de P, ou bien son coefficient dominant.
- On dit que P est unitaire (ou normalisé) si et seulement si $a_n = 1$.
- Le polynôme $a_k X^k$ est appelé un monôme.
- On dit que P est pair si et seulement si pour tout $k \in \mathbb{N}$, $a_{2k+1} = 0$.
  On dit que P est impair si et seulement si pour tout $k \in \mathbb{N}$, $a_{2k} = 0$.

Remarque. Soit $P \in A[X]$ et $n \in \mathbb{N}$. Alors $deg(P) = n$ si et seulement si il existe $a_0, \ldots, a_n \in A$ tels que $P(X) = \sum_{k=0}^{n} a_k X^k$ **avec** $a_n \neq 0$.

Lorsque $P(X) = \sum_{k=0}^{n} a_k X^k$, avec $a_0, \ldots, a_n \in A$, on peut seulement affirmer que $\deg(P) \leq n$.

Notation. Pour tout $n \in \mathbb{N}$, on note $A_n[X] = \{P \in A[X]/\deg(P) \leq n\}$.
Ainsi, $A[X] = \bigcup_{n\in\mathbb{N}} A_n[X]$.

Exemple. $A_0[X]$ est l'ensemble des polynômes constants.
$\mathbb{R}_2[X] = \{aX^2 + bX + c/(a,b,c) \in \mathbb{R}^3\}$.

Définition. (hors programme) Soit $P(X) = (a_k)_{k\in\mathbb{N}} \in A[X] \setminus \{0\}$.
Alors $\{k \in \mathbb{N}/a_k \neq 0\}$ est une partie finie et non vide de $\mathbb{N}$, donc elle possède un minimum, que l'on appelle la valuation du polynôme P.
On le note $\mathrm{val}(P)$ ou bien $v(P)$.
De plus, on convient que $\mathrm{val}(0) = +\infty$.

Propriété. Soit $P, Q \in A[X]$. Alors $\deg(P+Q) \leq \sup(\deg(P), \deg(Q))$.
De plus, lorsque $\deg(P) \neq \deg(Q)$, $\deg(P+Q) = \sup(\deg(P), \deg(Q))$.

Démonstration.
Si $P = 0$ ou $Q = 0$, la propriété est vérifiée.
Supposons maintenant que $P \neq 0$ et $Q \neq 0$. Notons $n = \deg(P)$ et $m = \deg(Q)$. On peut donc écrire $P(X) = \sum_{k=0}^{n} a_k X^k$ et $Q(X) = \sum_{k=0}^{m} b_k X^k$ avec $a_n \neq 0$ et $b_m \neq 0$.
Supposons que $\deg(P) \neq \deg(Q)$: sans perte de généralité, on peut supposer que $m < n$. Alors $P + Q = \sum_{k=0}^{m}(a_k + b_k)X^k + \sum_{k=m+1}^{n} a_k X^k$ et $a_n \neq 0$,
donc $\deg(P + Q) = n = \max(\deg(P), \deg(Q))$.
Si maintenant $n = m$, alors $P + Q = \sum_{k=0}^{n}(a_k + b_k)X^k$ et on peut seulement affirmer que $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$. □

Exemple. Si $P = X^3 - X + 2$ et $Q = -X^3 + X^2$, alors $P + Q = X^2 - X + 2$ et $\deg(P + Q) < \max(\deg(P), \deg(Q))$.

1.2 Produits de polynômes

Exemple. Reprenons $P = X^3 - X + 2$ et $Q = -X^3 + X^2$.
Il est naturel de définir le polynôme PQ par
$PQ = (-X^6 + X^5) + (X^4 - X^3) + (-2X^3 + 2X^2) = -X^6 + X^5 + X^4 - 3X^3 + 2X^2$.
Si l'on cherche à généraliser ce calcul avec $P, Q \in A[X]$, où $P(X) = \sum_{k\in\mathbb{N}} a_k X^k$ et $Q(X) = \sum_{k\in\mathbb{N}} b_k X^k$, on est amené à écrire $PQ = \sum_{k,h\in\mathbb{N}} a_k b_h X^{k+h} = \sum_{n\in\mathbb{N}} \Big(\sum_{\substack{k,h\in\mathbb{N} \\ k+h=n}} a_k b_h \Big) X^n$.

Définition. Soit $P, Q \in A[X]$. Notons $P = (a_k)_{k\in\mathbb{N}}$ et $Q = (b_k)_{k\in\mathbb{N}}$.
Alors $PQ = (c_n)_{n\in\mathbb{N}}$, où pour tout $n \in \mathbb{N}$, $c_n = \sum_{k+h=n} a_k b_h = \sum_{k=0}^{n} a_k b_{n-k}$. Ainsi,

$$\Big(\sum_{n\in\mathbb{N}} a_n X^n\Big) \times \Big(\sum_{n\in\mathbb{N}} b_n X^n\Big) \stackrel{\Delta}{=} \sum_{n\in\mathbb{N}} \Big(\sum_{k=0}^{n} a_k b_{n-k}\Big) X^n.$$

Propriété. Pour tout $P, Q \in A[X]$, PQ est aussi un élément de $A[X]$.
Démonstration.
Soit $P(X) = \sum_{k\in\mathbb{N}} a_k X^k \in A[X]$ et $Q(X) = \sum_{k\in\mathbb{N}} b_k X^k \in A[X]$.
Si $P = 0$ ou $Q = 0$, on vérifie que $PQ = 0$.
Supposons maintenant que $P \neq 0$ et $Q \neq 0$. Notons $n = \deg(P)$ et $m = \deg(Q)$.
Posons $PQ = \sum_{k\in\mathbb{N}} c_k X^k$.

Si $k > n+m$, $c_k = \sum_{\substack{i,j\in\mathbb{N}\\ i+j=k}} a_i b_j = 0$, car $i+j=k \Longrightarrow (i>n)\vee(j>m)$.

Ainsi, $(c_k) \in A^{(\mathbb{N})}$ et PQ est bien un élément de $A[X]$. □

Propriété. $(A[X],+,\times)$ est un anneau et $1_{A[X]} = (\delta_{k,0})_{k\in\mathbb{N}}$ (il s'agit du polynôme dont tous les coefficients sont nuls sauf celui de degré 0, égal à 1_A).

Démonstration.

◇ Posons $\mathbf{1} = (\delta_{k,0})_{k\in\mathbb{N}}$. Soit $P(X) = \sum_{k\in\mathbb{N}} a_k X^k \in A[X]$.

Alors $\mathbf{1}\times P = \sum_{n\in\mathbb{N}}\Big(\sum_{k+h=n} a_k\delta_{h,0}\Big)X^n = \sum_{n\in\mathbb{N}} a_n X^n = P$ et de même, $P\times\mathbf{1} = P$. Ainsi, $\mathbf{1}$ est l'élément neutre pour ce produit.

◇ Soit $P(X) = \sum_{k\in\mathbb{N}} a_k X^k \in A[X]$, $Q(X) = \sum_{k\in\mathbb{N}} b_k X^k \in A[X]$ et $R(X) = \sum_{k\in\mathbb{N}} c_k X^k \in A[X]$.

$$\begin{aligned} P\times(Q+R) &= \sum_{n\in\mathbb{N}}\Big(\sum_{k+h=n} a_k(b_h+c_h)\Big)X^n \\ &= \sum_{n\in\mathbb{N}}\Big(\sum_{k+h=n} (a_k b_h + a_k c_h)\Big)X^n \\ &= \sum_{n\in\mathbb{N}}\Big(\sum_{k+h=n} a_k b_h)\Big)X^n + \sum_{n\in\mathbb{N}}\Big(\sum_{k+h=n} a_k c_h\Big)X^n \\ &= PQ + PR. \end{aligned}$$

De même on montre que $(Q+R)P = QP+RP$, ce qui établit la distributivité de la multiplication par rapport à l'addition.

◇ Posons $PQ = \sum_{k\in\mathbb{N}} d_k X^k$. Ainsi, $(PQ)R = \sum_{n\in\mathbb{N}}\Big(\sum_{k+h=n} d_k c_h\Big)X^n$.

Soit $n\in\mathbb{N}$. $\sum_{k+h=n} d_k c_h = \sum_{k+h=n}\ \sum_{i+j=k} a_i b_j c_h = \sum_{\substack{(k,h,i,j)\in\mathbb{N}^4\\ (k+h=n)\wedge(i+j=k)}} a_i b_j c_h$.

Posons $B = \{(k,h,i,j)\in\mathbb{N}^4/(k+h=n)\wedge(i+j=k)\}$ et $C = \{(i,j,h)\in\mathbb{N}^3/i+j+h=n\}$. L'application $\varphi : \begin{array}{ccc} B & \longrightarrow & C \\ (k,h,i,j) & \longmapsto & (i,j,h) \end{array}$ est une bijection dont la bijection réciproque est $(i,j,h)\longmapsto(n-h,h,i,j)$. Ainsi, $\sum_{k+h=n} d_k c_h = \sum_{\substack{(i,j,h)\in\mathbb{N}^3\\ i+j+h=n}} a_i b_j c_h$, puis $(PQ)R = \sum_{n\in\mathbb{N}}\Big(\sum_{\substack{(i,j,k)\in\mathbb{N}^3\\ i+j+k=n}} a_i b_j c_k\Big)X^n$.

De même, on prouve que $P(QR) = \sum_{n\in\mathbb{N}}\Big(\sum_{\substack{(i,j,k)\in\mathbb{N}^3\\ i+j+k=n}} a_i b_j c_k\Big)X^n$, ce qui prouve l'associativité.

□

Propriété. L'application $i : \begin{array}{ccc} A & \longrightarrow & A[X] \\ a & \longmapsto & (\delta_{0,k}a)_{k\in\mathbb{N}} \end{array}$ est un morphisme injectif d'anneaux. On identifie A avec une partie de $A[X]$ en convenant que, pour tout $a\in A$, $a = i(a)$. Alors $A_0[X] = A$.

C'est en cohérence avec l'écriture $(\delta_{k,0}a)_{k\in\mathbb{N}} = aX^0 + \sum_{k\in\mathbb{N}} 0 \times X^k$.
On dit que $a \in A$ est un polynôme constant de $A[X]$.

Remarque. Avec cette identification, les polynômes de degré nul sont exactement les polynômes constants non nuls, c'est-à-dire les éléments de $A \setminus \{0\}$.

Remarque. Lorsque $b \in A$ et $P \in A[X]$, on dispose donc du produit bP.
Si $P = \sum_{k\in\mathbb{N}} a_k X^k$, on vérifie que $bP = \sum_{k\in\mathbb{N}} ba_k X^k$.

Propriété. $A[X]$ est un anneau intègre si et seulement si A est un anneau intègre.

Démonstration.
$\diamond$ Supposons que $A[X]$ est intègre.
$A[X]$ n'est pas réduit à $\{0\}$, donc A non plus.
$A[X]$ est commutatif donc A est commutatif : en effet, si $b, c \in A$, notons
$B = (b\delta_{k,0})_{k\in\mathbb{N}} \in A[X]$ et $C = (c\delta_{k,0})_{k\in\mathbb{N}} \in A[X]$. On calcule que
$BC = (bc\delta_{k,0})_{k\in\mathbb{N}} \in A[X]$ et $CB = (cb\delta_{k,0})_{k\in\mathbb{N}} \in A[X]$, or $CB = BC$, donc $bc = cb$.
Supposons maintenant que $bc = 0$. Alors $BC = 0$, or $A[X]$ est supposé intègre, donc $B = 0$ ou $C = 0$, d'où l'on déduit que $b = 0$ ou $c = 0$.
On a ainsi prouvé que A est intègre si $A[X]$ est intègre.
$\diamond$ Réciproquement, supposons que A est intègre.
A n'est pas réduit à $\{0\}$, donc $A[X]$ non plus.
A est commutatif donc $A[X]$ est commutatif :
en effet, si $P(X) = \sum_{k\in\mathbb{N}} a_k X^k \in A[X]$ et $Q(X) = \sum_{k\in\mathbb{N}} b_k X^k \in A[X]$, alors
$$PQ = \sum_{n\in\mathbb{N}} \Big(\sum_{\substack{k,h\in\mathbb{N} \\ k+h=n}} a_k b_h \Big) X^n = \sum_{n\in\mathbb{N}} \Big(\sum_{\substack{k,h\in\mathbb{N} \\ k+h=n}} b_h a_k \Big) X^n = QP.$$
Si l'on suppose de plus que $P \neq 0$ et $Q \neq 0$, notons $n = \deg(P)$ et $m = \deg(Q)$.
Posons $PQ = \sum_{k\in\mathbb{N}} c_k X^k$. On a déjà vu, pour montrer que $PQ \in A[X]$, que lorsque $k > n + m$, $c_k = 0$. De plus, pour $k = n + m$, $c_{n+m} = \sum_{\substack{i,j\in\mathbb{N} \\ i+j=n+m}} a_i b_j = a_n b_m$, car lorsque $i + j = n + m$, $a_i b_j \neq 0 \Longrightarrow (i \leq n) \wedge (j \leq m) \Longrightarrow (i = n) \wedge (j = m)$. Mais $a_n \neq 0$, $b_m \neq 0$ et A est intègre, donc $c_{n+m} \neq 0$, ce qui prouve que $PQ \neq 0$, donc que $A[X]$ est intègre. $\square$

Pour toute la suite de ce chapitre, on supposera que A est intègre, de sorte que $A[X]$ est également intègre.

Propriété. Pour tout $P, Q \in A[X]$, $\deg(PQ) = \deg(P) + \deg(Q)$.

Démonstration.
On vient de le démontrer lorsque P et Q sont non nuls.
Lorsque P ou Q est nul, cette relation est vérifiée car $d(0) = -\infty$. $\square$

Définition. Lorsque $P \in A[X] \setminus \{0\}$, on note $\mathrm{dom}(P)$ le coefficient dominant de P. Ce qui précède montre que, pour tout $P, Q \in A[X] \setminus \{0\}$, $\mathrm{dom}(PQ) = \mathrm{dom}(P)\mathrm{dom}(Q)$.

Remarque. Si l'on convient que $\mathrm{dom}(0) = 0$, la formule précédente devient valable pour tout $P, Q \in A[X]$.

Propriété. Les éléments inversibles de $A[X]$ sont exactement les éléments inversibles de A.

Démonstration.
Si a est un élément inversible de A, alors il existe $b \in A$ tel que $ab = ba = 1_A$, donc $i(a)i(b) = i(1_A) = \mathbf{1} = i(b)i(a)$. Ainsi, $i(a) = a$ est inversible dans $A[X]$.
Si maintenant $P \in A[X]$ est inversible dans $A[X]$, il existe $Q \in A[X]$ tel que $PQ = 1_A$. Alors $0 = \deg(1_A) = \deg(PQ) = \deg(P) + \deg(Q)$, or $\deg(P), \deg(Q) \in \mathbb{N} \cup \{-\infty\}$, donc $\deg(P) = 0 = \deg(Q)$. Ainsi, $P, Q \in A \setminus \{0\}$ et $PQ = 1_A$, donc P est un élément inversible de l'anneau A. □

Définition. L'indéterminée X est le polynôme $(\delta_{k,1})_{k\in\mathbb{N}}$.
C'est cohérent avec la notation $P = \sum_{k\in\mathbb{N}} a_k X^k$: lorsque $a_k = 0$ pour tout $k \neq 1$ et $a_1 = 1$, $P = X$.

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

Démonstration.
On procède par récurrence. En effet, si $X^n = (\delta_{k,n})_{k\in\mathbb{N}}$,
alors $X^{n+1} \triangleq X^n \times X = \sum_{k\in\mathbb{N}} \Big(\sum_{i+j=k} \delta_{i,n}\delta_{j,1} \Big) X^k = \sum_{k\in\mathbb{N}} \delta_{k,n+1} X^k$. □

Remarque. Cette propriété justifie la notation $P(X) = \sum_{k\in\mathbb{N}} a_k X^k$
lorsque $P = (a_k)_{k\in\mathbb{N}} \in A^{(\mathbb{N})} = A[X]$,
car pour une famille presque nulle, $(a_k) = \sum_{k\in\mathbb{N}} a_k (\delta_{k,n})_{n\in\mathbb{N}}$.

1.3 Polynômes à plusieurs indéterminées (hors programme)

Définition. A est intègre, donc $A[X]$ est intègre, puis $(A[X])[Y]$ est aussi un anneau intègre. Ce dernier ensemble est l'anneau des polynômes à deux indéterminées à coefficients dans A. On le note plutôt $A[X, Y]$.
Par récurrence, on peut définir $A[X_1, \ldots, X_p]$, l'anneau des polynômes à p indéterminées.

Exemple. Un élément de $\mathbb{R}[X, Y]$ est $(1 + X)Y^2 + (X^2 - 1)Y$.

Plus précisément : Supposons que A est un anneau intègre.

◇ Soit $P \in (A[X])[Y]$: Il existe $n \in \mathbb{N}$ et $P_0, \ldots, P_n \in A[X]$ tels que $P = \sum_{k=0}^{n} P_k(X) Y^k$.

Pour tout $k \in \{0, \ldots, n\}$, il existe $m_k \in \mathbb{N}$ et $a_{0,k}, \ldots, a_{m_k,k} \in A$

tels que $P_k(X) = \sum_{h=0}^{m_k} a_{h,k} X^h$.
Posons $m = \max_{0\leq k\leq n} m_k$ et pour tout $k \in \{0, \dots, n\}$, pour tout $h > m_k$, $a_{h,k} = 0$.
Ainsi, $P = \sum_{k=0}^{n} \Big(\sum_{h=0}^{m} a_{h,k} X^h \Big) Y^k = \sum_{\substack{0\leq h\leq m \\ 0\leq k\leq n}} a_{h,k} X^h Y^k$.

◇ Ceci démontre que l'application $\begin{array}{rccc} \varphi : & A^{(\mathbb{N}^2)} & \longrightarrow & (A[X])[Y] \\ & (a_{h,k})_{(h,k)\in\mathbb{N}^2} & \longmapsto & \sum_{(h,k)\in\mathbb{N}^2} a_{h,k} X^h Y^k \end{array}$ est une application surjective.
De plus, on peut vérifier que φ est un morphisme de groupes additifs.
On vérifie que, pour tout $(a_{h,k})_{(h,k)\in\mathbb{N}^2} \in A^{(\mathbb{N}^2)}$,
$\sum_{\substack{0\leq h\leq m \\ 0\leq k\leq n}} a_{h,k} X^h Y^k = 0 \Longrightarrow [\forall h, k \in \mathbb{N}^2,\ a_{h,k} = 0]$, donc φ est un morphisme injectif.
Ainsi φ est un isomorphisme de groupes.
En posant, pour tout $P, Q \in A^{(\mathbb{N}^2)}$, $P \times Q \triangleq \varphi^{-1}(\varphi(P) \times \varphi(Q))$, on munit $A^{(\mathbb{N}^2)}$ d'une structure d'anneau intègre, isomorphe à $(A[X])[Y]$, dont l'élément neutre multiplicatif est égal à $(\delta_{h,0}\delta_{k,0})_{(h,k)\in\mathbb{N}^2}$.
On note $A^{(\mathbb{N}^2)} \triangleq A[X, Y]$ et on identifie les deux anneaux $A[X, Y]$ et $(A[X])[Y]$.

◇ Pour parachever cette identification, c'est-à-dire pour permettre d'écrire $(a_{h,k})_{(h,k)\in\mathbb{N}^2} = \sum_{(h,k)\in\mathbb{N}^2} a_{h,k} X^h Y^k$, il est naturel de poser, dans le cadre de polynômes aux deux indéterminées X et Y : $\boxed{X = (\delta_{h,1}\delta_{k,0})_{(h,k)\in\mathbb{N}^2} \text{ et } Y = (\delta_{h,0}\delta_{k,1})}$.
On peut vérifier que, pour tout $p, q \in \mathbb{N}^2$, $X^p Y^q = (\delta_{h,p}\delta_{k,q})_{(h,k)\in\mathbb{N}^2}$.
On peut écrire : $\sum_{(h,k)\in\mathbb{N}^2} a_{h,k} X^h Y^k = \sum_{h\in\mathbb{N}} \Big(\sum_{k\in\mathbb{N}} a_{h,k} Y^k \Big) X^h \in (A[Y])[X]$,
en convenant que $A[Y] = \{\sum_{k\in\mathbb{N}} b_k Y^k \ / \ (b_k)_{k\in\mathbb{N}} \in A^{(\mathbb{N})}\}$ (on peut vérifier que c'est un sous-anneau de $A[X, Y]$).
En conclusion, $(A[X])[Y] = A[X, Y] = (A[Y])[X]$.

◇ On peut généraliser à p indéterminées $X_1, \dots, X_p$, où $p \in \mathbb{N}^*$:
$A[X_1, \dots, X_p] \triangleq A^{(\mathbb{N}_p)} = (A[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_p])[X_i]$, quel que soit $i \in \mathbb{N}_p$.

Remarque. Lorsqu'on identifie l'anneau A avec un sous-anneau de $A[X]$, on identifie 1_A avec le polynôme $(\delta_{0,k})_{k\in\mathbb{N}}$ de $A[X]$, égal à $1_{A[X]}$. On s'y perd facilement lorsqu'on identifie ensuite $A[X]$ avec un sous-anneau de $A[X][Y]$. Il est donc préférable de considérer que les éléments de $A[X][Y]$ sont des éléments de $A^{(\mathbb{N}^2)}$.

1.4 Applications polynomiales

Définition. Soit $P = \sum_{k\in\mathbb{N}} a_k X^k \in A[X]$ un polynôme. L'application polynomiale associée à P est l'application $\begin{array}{rccc}\tilde{P}: & A & \longrightarrow & A \\ & x & \longmapsto & \sum_{k\in\mathbb{N}} a_k x^k\,.\end{array}$

Lorsque $A = \mathbb{R}$ ou $A = \mathbb{C}$, on retrouve la notion d'application polynomiale usuelle.

Remarque. Par opposition aux applications polynomiales, les éléments de $A[X]$ sont parfois appelés des polynômes *formels*.

Propriété. L'application $\begin{array}{rccc}\varphi: & A[X] & \longrightarrow & \mathcal{F}(A,A) \\ & P & \longmapsto & \tilde{P}\end{array}$ est un morphisme d'anneaux.

Démonstration.

◇ Pour tout $x \in A$, $\tilde{\mathbf{1}}(x) = \sum_{k\in\mathbb{N}} \delta_{0,k} x^k = x^0 = 1_A$, donc $\tilde{\mathbf{1}}$ est l'application constante égale à 1_A, c'est-à-dire $1_{\mathcal{F}(A,A)}$.

◇ Soit $P(X) = \sum_{k\in\mathbb{N}} a_k X^k \in A[X]$ et $Q(X) = \sum_{k\in\mathbb{N}} b_k X^k \in A[X]$.

Pour tout $x \in A$, $\widetilde{P+Q}(x) = \sum_{k\in\mathbb{N}} (a_k + b_k) x^k = \tilde{P}(x) + \tilde{Q}(x)$.

◇ $\widetilde{PQ}(x) = \sum_{k\in\mathbb{N}} \Big(\sum_{i+j=k} a_i b_j \Big) x^k$, or en calculant dans l'anneau A,

$\tilde{P}(x) \times \tilde{Q}(x) = \Big(\sum_{k\in\mathbb{N}} a_k x^k\Big) \times \Big(\sum_{k\in\mathbb{N}} b_k x^k\Big) = \sum_{k,h\in\mathbb{N}} a_k b_h x^{k+h}$, puis par sommation par paquets, $\tilde{P}(x) \times \tilde{Q}(x) = \sum_{n\in\mathbb{N}} \sum_{\substack{k,h\in\mathbb{N} \\ k+h=n}} a_k b_h x^n$, ce qui montre que $\tilde{P}(x) \times \tilde{Q}(x) = \widetilde{PQ}(x)$. □

Notation. $Im(\varphi)$ est un sous-anneau de $\mathcal{F}(A,A)$, que l'on appelle l'anneau des applications polynomiales de A dans A.

Remarque. $Ker(\varphi) = \{P \in A[X] / \forall x \in A,\ P(x) = 0\}$, donc φ est injective si et seulement si pour tout $P \in A[X]$, $P = 0 \Longleftrightarrow [\forall x \in A,\ P(x) = 0]$.
Dans ce cas, on identifie $Im(\varphi)$ avec $A[X]$.

Théorème. Lorsque A est un corps, φ est injectif si et seulement si A est de cardinal infini.

Démonstration.

Admis pour le moment. C'est démontré un peu plus loin. □

Remarque. En particulier, les polynômes de $\mathbb{C}[X]$ ou de $\mathbb{R}[X]$ peuvent être identifiés à leurs applications polynomiales. Par exemple, le polynôme $X^2 + 1$ de $\mathbb{R}[X]$ est égal à l'application polynomiale $\begin{array}{ccc}\mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2+1\end{array}$.

Remarque. Lorsque A est un corps infini, l'ensemble des applications polynomiales est un sous-anneau intègre de $\mathcal{F}(A,A)$, lequel n'est pas intègre.

Remarque. Ainsi, lorsque $P \in \mathbb{R}[X]$ et $x \in \mathbb{R}$, $\tilde{P}(x)$ s'écrira simplement $P(x)$.
C'est valable dans tout corps infini.

Algorithme d'Hörner : Soit $P = \sum_{k\in\mathbb{N}} a_k X^k \in A[X]$ et $x \in A$. On peut disposer le calcul de $\tilde{P}(x)$ de la manière suivante :

$$\tilde{P}(x) = (\cdots((a_n x + a_{n-1})x + a_{n-2}x) + \cdots + a_1)x + a_0.$$

Cet algorithme permet de calculer $\tilde{P}(x)$ avec n multiplications et n additions.
C'est mieux que l'algorithme naïf consistant à calculer directement $\tilde{P}(x)$ par la formule $\tilde{P}(x) = \sum_{k\in\mathbb{N}} a_k x^k$, même si l'on calcule x^k à partir de x^{k-1} au sein de la boucle.

1.5 Composition de polynômes

Définition. Soit $P = \sum_{k=0}^{n} a_k X^k \in A[X]$ un polynôme de degré $n \in \mathbb{N}$.

Pour tout $Q \in A[X]$, on pose $P \circ Q = \sum_{k=0}^{n} a_k Q^k$.
Lorsque $P = 0$, on convient que $P \circ Q = 0$ pour tout $Q \in A[X]$.

Notation. $P \circ Q$ est aussi noté $P(Q)$.
Lorsque $Q = X$, $P(X) = P \circ X = P$, ce qui explique pourquoi on note indifféremment un polynôme P ou $P(X)$.

Exemple. Si $P = X^3 + 1$ et $Q = X^2 - 1$, alors
$P(Q) = (X^2-1)^3 + 1 = X^6 - 3X^4 + 3X^2$ et $Q(P) = (X^3+1)^2 - 1 = X^6 + 2X^3$.

Exemple. On suppose que la caractéristique de l'anneau A est différente de 2.
Alors, pour tout $P \in A[X]$, P est pair si et seulement si $P(-X) = P(X)$ et P est impair si et seulement si $P(-X) = -P(X)$.
En effet, si l'on pose $P(X) = \sum_{k\in\mathbb{N}} a_k X^k$, on a
$P(X) = P(-X) \iff \sum_{k\in\mathbb{N}} a_k X^k = \sum_{k\in\mathbb{N}} a_k (-1)^k X^k \iff \forall k \in \mathbb{N},\ 2a_{2k+1} = 0$, or $2a_{2k+1} = (2.1_A)a_{2k+1}$ et $2.1_A \neq 0$ par hypothèse,
donc $P(X) = P(-X) \iff \forall k \in \mathbb{N},\ a_{2k+1} = 0 \iff P$ est pair.

Propriété. Pour tout $P, Q, R \in A[X]$,
- $(P+Q) \circ R = P \circ R + Q \circ R$,
- $(PQ) \circ R = (P \circ R) \times (Q \circ R)$,
- $(P \circ Q) \circ R = P \circ (Q \circ R)$.

Démonstration.
Les deux premières propriétés s'obtiennent en passant aux coefficients sur P et Q.
Pour l'associativité, en posant $P = \sum_{k=0}^{n} a_k X^k$, d'après les deux premières propriétés,
$(P \circ Q) \circ R = \Big(\sum_{k=0}^{n} a_k Q^k\Big) \circ R = \sum_{k=0}^{n} a_k (Q \circ R)^k = P \circ (Q \circ R)$. □

Remarque. En général, $P \circ (Q + R) \neq P \circ Q + P \circ R$.

Propriété. Soit $P, Q \in A[X]$. Si $\deg(Q) \geq 1$, alors $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

Exemple. $\deg(P(X+1)) = \deg(P)$.

Propriété. Pour tout $P, Q \in A[X]$, $\widetilde{P \circ Q} = \tilde{P} \circ \tilde{Q}$.

Remarque. C'est cette dernière propriété qui justifie la notation $P \circ Q$.
Démonstration.
Notons $\varphi \ : \ P \longmapsto \tilde{P}$. Soit $P, Q \in A[X]$. Notons $P = \sum_{k=0}^{n} a_k X^k$.
$\widetilde{P \circ Q} = \varphi\Big(\sum_{k=0}^{n} a_k Q^k\Big)$, or φ est un morphisme d'anneaux, donc pour tout $x \in A$,
$\widetilde{P \circ Q}(x) = \Big(\sum_{k=0}^{n} a_k \tilde{Q}^k\Big)(x) = \sum_{k=0}^{n} a_k \tilde{Q}(x)^k = \tilde{P}(\tilde{Q}(x))$. □

1.6 Dérivation formelle

Définition. Soit $P = \sum_{k \in \mathbb{N}} a_k X^k \in A[X]$. La dérivée (formelle) du polynôme (formel) P est $P' \stackrel{\Delta}{=} \sum_{k \in \mathbb{N}^*} k a_k X^{k-1} = \sum_{k \in \mathbb{N}} (k+1) a_{k+1} X^k : P' \in A[X]$.

Remarque. On peut écrire $P' = \sum_{k \in \mathbb{N}} k a_k X^{k-1}$, si l'on convient que $0 X^{-1} = 0$.

Exemple. $(X^2 + 3X + 1)' = 2X + 3$. Pour tout $a \in A$, $a' = 0$.

Définition. Par récurrence, on peut définir la dérivée n-ième d'un polynôme.
Si $P = \sum_{k \in \mathbb{N}} a_k X^k \in A[X]$, on convient que $P^{(0)} = P$ et on vérifie que,
pour tout $n \in \mathbb{N}$, $P^{(n)} = \sum_{k \geq n} \frac{k!}{(k-n)!} a_k X^{k-n} = \sum_{k \in \mathbb{N}} \frac{(k+n)!}{k!} a_{k+n} X^k$.

Propriété. Pour tout $P \in \mathbb{R}[X]$ et $n \in \mathbb{N}$, $\widetilde{P^{(n)}} = \tilde{P}^{(n)}$.

Propriété. Pour tout $P \in A[X]$, $\deg(P') \leq \deg(P) - 1$.

Propriété. Pour tout $P \in A[X] \setminus \{0\}$, $P^{(\deg(P)+1)} = 0$.

Propriété. Soit $P, Q \in A[X]$, $a \in A$ et $n \in \mathbb{N}$.
— $(P+Q)' = P' + Q'$, et plus généralement, $(P+Q)^{(n)} = P^{(n)} + Q^{(n)}$.
— $(aP)' = aP'$, et plus généralement, $(aP)^{(n)} = aP^{(n)}$.
— $(PQ)' = P'Q + PQ'$

Démonstration.
Les deux premières propriétés, qui énoncent la linéarité de la dérivation, sont simples à établir en passant aux coefficients.
Lorsque $Q = X^k$ avec $k \in \mathbb{N}$, en posant $P = \sum_{n\in\mathbb{N}} a_n X^n$ et en convenant que $0.X^{-1} = 0$,
$(PX^k)' = \sum_{n\in\mathbb{N}} a_n (X^{n+k})' = \sum_{n\in\mathbb{N}} (n+k) a_n X^{n+k-1}$ et
$P'X^k + P(X^k)' = \sum_{n\in\mathbb{N}} (n a_n X^{n-1+k} + a_n X^n k X^{k-1})$. Ainsi, $(PX^k)' = P'X^k + P(X^k)'$.
On en déduit la propriété lorsque Q est quelconque par linéarité de la dérivation : en posant $Q = \sum_{k\in\mathbb{N}} b_k X^k$, $(PQ)' = \sum_{k\in\mathbb{N}} b_k (PX^k)' = \sum_{k\in\mathbb{N}} b_k (P'X^k + P(X^k)') = P'Q + PQ'$.
□

Propriété. Pour tout $n \in \mathbb{N}$ et $P_1, \dots, P_n \in A[X]$, $(P_1 \times \cdots \times P_n)' = \sum_{i=1}^{n} P_i' \prod_{j\neq i} P_j$.

Formule de Leibniz : Pour tout $P, Q \in A[X]$, pour tout $n \in \mathbb{N}$,

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

Démonstration.
Adapter la démonstration de la formule de Leibniz pour des fonctions n fois dérivables de I dans $\mathbb{C}$. □

Propriété. Pour tout $P, Q \in A[X]$, $(P \circ Q)' = Q' \times (P' \circ Q)$.

Démonstration.
Posons $P = \sum_{n\in\mathbb{N}} a_n X^n$. Par linéarité de la dérivation,
$(P \circ Q)' = \sum_{k\in\mathbb{N}} a_n (Q^n)' = \sum_{k\geq 1} n a_n Q' Q^{n-1} = Q' \times (P' \circ Q)$. □

Exemple. $[(X-a)^n]' = n(X-a)^{n-1}$.

Pour toute la suite de ce chapitre,
on suppose que A est un corps, que l'on notera plutôt $\mathbb{K}$.

1.7 La structure d'algèbre de $\mathbb{K}[X]$.

On sait que $\mathbb{K}^{\mathbb{N}}$ est un $\mathbb{K}$-espace vectoriel qui contient $\mathbb{K}[X]$.
On a déjà vu que $\mathbb{K}[X]$ est non vide et qu'il est stable pour l'addition.
Soit $\alpha \in \mathbb{K}$ et $P \in \mathbb{K}[X]$. Notons $P = \sum_{k\in\mathbb{N}} a_k X^k = (a_k)_{k\in\mathbb{N}}$.
Alors $\alpha P = (\alpha a_k)_{k\in\mathbb{N}} = \sum_{k\in\mathbb{N}} \alpha a_k X^k \in \mathbb{K}[X]$,
donc $\mathbb{K}[X]$ est un sous-espace vectoriel de $\mathbb{K}^{\mathbb{N}}$.

Remarque. Soit $\alpha \in \mathbb{K}$ et $P = \sum_{k\in\mathbb{N}} a_k X^k \in \mathbb{K}[X]$. On peut considérer α comme un polynôme (constant) de $\mathbb{K}[X]$ et former le produit des deux polynômes α et P. On vérifie que ce produit est égal à $\sum_{k\in\mathbb{N}} \alpha a_k X^k$. Ainsi, $\alpha \times P = \alpha.P$, où le membre de gauche est le produit entre les deux polynômes α et P et où le membre de droite est le produit du scalaire α par le vecteur P.

Propriété. $\mathbb{K}[X]$ est une $\mathbb{K}$-algèbre.

Démonstration.
Soit $\alpha \in \mathbb{K}$ et $P, Q \in \mathbb{K}[X]$. Alors par associativité et commutativité du produit entre polynômes, $\alpha.(P \times Q) = (\alpha.P) \times Q = P \times (\alpha Q)$. □

Propriété. La base canonique de $\mathbb{K}[X]$ est la famille $(X^n)_{n\in\mathbb{N}}$.
Ainsi, pour $P \in \mathbb{K}[X]$, l'écriture $P = \sum_{k\in\mathbb{N}} a_k X^k$ est la décomposition de P dans la base canonique de $\mathbb{K}[X]$.

Démonstration.
$\mathbb{K}[X] = \mathbb{K}^{(\mathbb{N})}$ et pour tout $n \in \mathbb{N}$, $X^n = (\delta_{i,n})_{i\in\mathbb{N}}$. □

Propriété. Soit $n \in \mathbb{N}$. $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$ dont une base est $(1, X, \ldots, X^n)$, encore appelée la base canonique de $\mathbb{K}_n[X]$.
On en déduit que $\dim(\mathbb{K}_n[X]) = n + 1$.

Démonstration.
$\mathbb{K}_n[X] = \mathrm{Vect}((X^k)_{0\leq k\leq n})$. □

Exercice. Soit $(P_n)_{n\in\mathbb{N}}$ une suite de polynômes de $\mathbb{K}[X]$. On suppose que cette suite de polynômes est étagée c'est-à-dire que, $\forall n \in \mathbb{N} \quad \deg(P_n) = n$.
Montrer que pour tout $N \in \mathbb{N}$, $(P_n)_{0\leq n\leq N}$ est une base de $\mathbb{K}_N[X]$.
En déduire que $(P_n)_{n\in\mathbb{N}}$ est une base de $\mathbb{K}[X]$.

Solution :

◇ Soit $N \in \mathbb{N}$. Soit $(\alpha_n)_{0\leq n\leq N}$ une famille de scalaires telle que $\sum_{n=0}^{N} \alpha_n P_n = 0$.

Supposons que cette famille est non nulle. Alors $\{n \in \{0, \ldots, N\} / \alpha_n \neq 0\}$ est un ensemble non vide inclus dans $\mathbb{N}$ et majoré par N, donc il admet un maximum que l'on note p.

Ainsi, $P_p = -\frac{1}{\alpha_p}\sum_{n=0}^{p-1}\alpha_n P_n$. Si $p=0$, alors $P_0=0$, ce qui est faux, donc $p\geq 1$ si bien que $\max_{0\leq n<p} deg(\alpha_n P_n)$ est défini. Alors, $p = deg(P_p) \leq \max_{0\leq n<p} deg(\alpha_n P_n) \leq p-1$. C'est faux, donc la famille $(\alpha_n)_{0\leq n\leq N}$ est nulle. Ainsi la famille $(P_n)_{0\leq n\leq N}$ est une famille libre de $\mathbb{K}_N[X]$ de cardinal $N+1$. Or la famille $(X^n)_{0\leq n\leq N}$ est la base canonique de $\mathbb{K}_N[X]$, donc $\mathbb{K}_N[X]$ est un espace vectoriel de dimension $N+1$. Ainsi $(P_n)_{0\leq n\leq N}$ est une base de $\mathbb{K}_N[X]$.

- Soit $(\alpha_n)_{n\in\mathbb{N}} \in \mathbb{K}^{(\mathbb{N})}$ telle que $\sum_{n\in\mathbb{N}}\alpha_n P_n = 0$. Cette famille de scalaires étant presque nulle, il existe $N\in\mathbb{N}$ tel que pour tout $n>N$, $\alpha_n=0$.

Ainsi $\sum_{n=0}^{N}\alpha_n P_n = 0$, or la famille $(P_n)_{0\leq n\leq N}$ est libre, donc pour tout $n\leq N$, $\alpha_n=0$. Ainsi la famille $(P_n)_{n\in\mathbb{N}}$ est libre.

- *R*emarque. Plus généralement, le même argument permet de démontrer qu'une famille $(x_i)_{i\in I}$ de vecteurs d'un espace vectoriel est libre si et seulement si toute sous-famille finie de $(x_i)_{i\in I}$ est libre.
- Il reste à montrer que $(P_n)_{n\in\mathbb{N}}$ est une famille génératrice de $\mathbb{K}[X]$.

Soit $P\in\mathbb{K}[X]\setminus\{0\}$. Notons N son degré. $P\in\mathbb{K}_N[X]$, donc il existe $(\alpha_n)_{0\leq n\leq N}\in\mathbb{K}^{N+1}$ telle que $P=\sum_{n=0}^{N}\alpha_n P_n$. On complète cette famille finie en la suite $(\alpha_n)_{n\in\mathbb{N}}$ en posant $\alpha_n=0$ pour tout $n>N$. Ainsi $P=\sum_{n\in\mathbb{N}}\alpha_n P_n$. Donc la famille $(P_n)_{n\in\mathbb{N}}$ engendre $\mathbb{K}[X]$.

Exercice. Soit $u\in L(\mathbb{K}[X])$ tel que pour tout $P\in\mathbb{K}[X]$, $\deg(u(P))=\deg(P)$. Montrer que u est un automorphisme sur $\mathbb{K}[X]$.
Solution : Soit $P\in\mathrm{Ker}(u)$: $\deg(P)=\deg(u(P))=-\infty$, donc $P=0$. Ainsi, $\mathrm{Ker}(u)=\{0\}$ et u est injective.
Soit $n\in\mathbb{N}$. Pour tout $P\in\mathbb{K}_n[X]$, $\deg(u(P))=\deg(P)\leq n$, donc $\mathbb{K}_n[X]$ est stable par u et l'endomorphisme u_n induit par u sur $\mathbb{K}_n[X]$ est bien défini. u_n est linéaire injective de $\mathbb{K}_n[X]$ dans $\mathbb{K}_n[X]$ qui est de dimension finie, donc c'est un automorphisme de $\mathbb{K}_n[X]$.
Soit $P\in\mathbb{K}[X]$. Il existe $n\in\mathbb{N}$ tel que $P\in\mathbb{K}_n[X]$, donc il existe $Q\in\mathbb{K}_n[X]$ tel que $u_n(Q)=P$. Alors $u(Q)=P$, ce qui prouve que u est surjective.
Par exemple, $P\longmapsto P+P'+2P''$ est un automorphisme de $\mathbb{R}[X]$.

1.8 Division euclidienne entre polynômes

Théorème. Soit $A,B\in\mathbb{K}[X]$ avec $B\neq 0$. Alors
il existe un unique couple $(Q,R)\in\mathbb{K}[X]^2$ tel que $A=BQ+R$ avec $\deg(R)<\deg(B)$.
On dit que Q est le quotient de la division euclidienne du dividende A par le diviseur B et que R en est le reste.

Exemple. Prenons $\mathbb{K} = \mathbb{R}$, $A = X^4 - X^3$ et $B = X^2 + X - 1$.
On commence par écrire $A = X^2B - 2X^3 + X^2$, or $-2X^3 + X^2 = -2XB + 3X^2 - 2X$, donc $A = (X^2 - 2X)B + 3X^2 - 2X$. Enfin, $3X^2 - 2X = 3B - 5X + 3$,
donc $A = (X^2 - 2X + 3)B - 5X + 3$.
On peut disposer ce calcul comme on le fait pour une division entre entiers.

Démonstration.
$\diamond$ Pour démontrer l'existence, on généralise le procédé détaillé en exemple, dans le cadre d'une récurrence.
Soit $n \in \mathbb{N}$. On note $R(n)$ l'assertion suivante : pour tout $A \in \mathbb{K}[X]$ avec $\deg(A) \leq n$, pour tout $B \in \mathbb{K}[X] \setminus \{0\}$, il existe un couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $A = BQ + R$ avec $\deg(R) < \deg(B)$.
Pour $n = 0$, soit $A \in \mathbb{K}[X]$ avec $\deg(A) \leq 0$ et $B \in \mathbb{K}[X] \setminus \{0\}$.
Si $deg(B) \geq 1$, le couple $(Q, R) = (0, A)$ convient.
Sinon, $deg(B) = 0$, donc $B \in \mathbb{K} \setminus \{0\}$. On peut alors écrire $A = BB^{-1}A + 0$ et $\deg(0) < \deg(B)$.
Pour $n \geq 1$, on suppose $R(n-1)$. Soit $A \in \mathbb{K}[X]$ avec $\deg(A) \leq n$ et $B \in \mathbb{K}[X] \setminus \{0\}$.
Si $\deg(A) < \deg(B)$, il suffit d'écrire $A = 0.B + A$.
Supposons maintenant que $\deg(A) \geq \deg(B)$. Posons $A = a_nX^n + C$
avec $\deg(C) \leq n-1$ et $B = b_pX^p + D$ avec $b_p \neq 0$ et $\deg(D) < p \leq n$.
Alors $A - \left(\frac{a_n}{b_p}X^{n-p}\right)B = a_nX^n + C - a_nX^n - \frac{a_n}{b_p}X^{n-p}D = C - \frac{a_n}{b_p}X^{n-p}D$.
Or $\deg(C - \frac{a_n}{b_p}X^{n-p}D) \leq \max(\deg(C), n-p+\deg(D)) \leq n-1$, donc d'après $R(n-1)$,
il existe $(Q', R) \in \mathbb{K}[X]^2$ tels que $C - \frac{a_n}{b_p}X^{n-p}D = BQ' + R$ et $\deg(R) < \deg(B)$.
Alors $A = \left(\frac{a_n}{b_p}X^{n-p} + Q'\right)B + R$, ce qui prouve $R(n)$.
$\diamond$ Unicité : Supposons qu'il existe $(Q, R), (Q', R') \in \mathbb{K}[X]^2$ tels que
$A = BQ + R = BQ' + R'$ avec $\deg(R) < deg(B)$ et $\deg(R') < deg(B)$.
Alors $B(Q - Q') = R' - R$, donc
$\deg(B) + \deg(Q - Q') = \deg(R - R') \leq \max(\deg(R), \deg(R')) < \deg(B)$.
Ainsi, $\deg(Q - Q') < 0$ donc $Q - Q' = 0$.
On en déduit que $Q = Q'$, puis $R' - R = B(Q - Q') = 0$, donc $R = R'$. □

Définition. Soit $A \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.
On dit que a est une racine du polynôme A si et seulement si $\tilde{A}(a) = 0$.

Propriété. Soit $A \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Le reste de la division euclidienne de A par $X - a$ est égal au polynôme constant $\tilde{A}(a)$.

Démonstration.
Il existe $Q, R \in \mathbb{K}[X]$ tels que $A = (X - a)Q + R$ et $\deg(R) < \deg(X - a) = 1$, donc $R \in \mathbb{K}$. Or $P \longmapsto \tilde{P}$ est un morphisme d'anneaux, donc $\tilde{A} = \widetilde{X - a} \times \tilde{Q} + \tilde{R}$. Ainsi, $\tilde{A}(a) = \widetilde{X - a}(a)\tilde{Q}(a) + \tilde{R}(a) = 0 \times \tilde{Q}(a) + R = R$. □

Corollaire. Soit $A \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.
a est une racine de A si et seulement si A est un multiple de $X - a$, c'est-à-dire si et seulement si il existe $Q \in \mathbb{K}[X]$ tel que $A = (X - a)Q$.

Exercice. Dans $\mathbb{R}[X]$, calculer le reste de la division euclidienne de $A \in \mathbb{R}[X]$ par $(X - a)(X - b)$, où $a, b \in \mathbb{R}$ avec $a \neq b$.

Solution : Il existe $Q, R \in \mathbb{R}[X]$ tels que $A = (X-a)(X-b)Q+R$ et $\deg(R) \leq 1$. Posons $R(X) = \alpha X + \beta$. Alors $A(a) = 0 \times Q(a) + R(a) = \alpha a + \beta$ et de même, $A(b) = \alpha b + \beta$. On en déduit que $\alpha = \dfrac{A(a) - A(b)}{a - b}$ et $\beta = A(a) - \alpha a$.

Propriété. Supposons que $\mathbb{L}$ est un sous-corps de $\mathbb{K}$.
Alors, pour tout $(A, B) \in \mathbb{L}[X] \times (\mathbb{L}[X] \setminus \{0\})$, les quotient et reste de la division euclidienne sont les mêmes que l'on regarde A et B comme des polynômes de $\mathbb{L}[X]$ ou de $\mathbb{K}[X]$.

Démonstration.
Il existe $Q, R \in \mathbb{L}[X]$ et $Q', R' \in \mathbb{K}[X]$ tels que $A = BQ + R = BQ' + R'$,
$\deg(R) < \deg(B)$ et $\deg(R') < \deg(B)$. Or $Q, R, Q', R' \in \mathbb{K}[X]$, donc d'après l'unicité de la division euclidienne, $Q = Q'$ et $R = R$. □

Remarque. Lorsque $A, B \in \mathbb{Z}[X]$, avec $B \neq 0$, les quotient et reste de la division de A par B sont dans $\mathbb{Q}[X]$. De plus, lorsque B est unitaire, en reprenant la démonstration de l'existence de la division euclidienne, on peut montrer que le quotient et le reste sont dans $\mathbb{Z}[X]$.

2 Arithmétique

2.1 Divisibilité

Définition. Soient A un anneau commutatif et $(a, b) \in A^2$.

On dit que a divise b et on note $a|b$ si et seulement si $\exists m \in A \ \ b = ma$.
On dit alors que a est un ***diviseur*** de b et que b est un ***multiple*** de a.

Remarque. Soit A un anneau commutatif.
$0|a \iff a = 0$ et, pour tout $a \in A$, $a|0$.
Selon le sens précédent, tout élément a de A est donc un diviseur de 0, mais, lorsqu'on parlera de "diviseurs de 0" ce sera toujours au sens de la définition donnée dans le chapitre "Groupes et anneaux" page 26.

Exemple. Lorsque $A = \mathbb{Z}$, 3 divise 15.
Lorsque $A = \mathbb{K}[X]$, $X - 1$ divise $(X - 1)(X - 3) = X^2 - 4X + 3$.

Propriété. Soit $P, Q \in \mathbb{K}[X]$ tels que $P \mid Q$ et $Q \neq 0$. Alors $\deg(Q) \geq \deg(P)$.

Propriété. Soit $\mathbb{L}$ un sous-corps d'un corps $\mathbb{K}$. Soit $P, Q \in \mathbb{L}[X]$.
Alors $P \mid Q$ dans $\mathbb{L}[X]$ si et seulement si $P \mid Q$ dans $\mathbb{K}[X]$.

Démonstration.
Si $P \mid Q$ dans $\mathbb{L}[X]$, il existe $H \in \mathbb{L}[X]$ tel que $Q = HP$. Alors $H \in \mathbb{K}[X]$ et $Q = HP$, donc $P \mid Q$ dans $\mathbb{K}[X]$.
Réciproquement, supposons que $P \mid Q$ dans $\mathbb{K}[X]$. Si $P = 0$, alors $P \mid Q$ dans $\mathbb{L}[X]$. On suppose maintenant que $P \neq 0$. Il existe $H \in \mathbb{K}[X]$ tel que $Q = HP$. Ainsi, dans $\mathbb{K}[X]$, les quotient et reste de la division euclidienne de Q par P sont H et 0, or on sait que ce sont les mêmes, que l'on regarde P et Q comme des polynômes de $\mathbb{L}[X]$ ou de $\mathbb{K}[X]$, donc $H \in \mathbb{L}[X]$ et $P \mid Q$ dans $\mathbb{L}[X]$. □

Propriété. Soient A un anneau commutatif et $a, b, c, d \in A$.
- Si $b \mid a$ et $b \mid c$, alors $b \mid (a + c)$.
- Si $b \mid a$ et $d \mid c$, alors $bd \mid ac$.
- si $b \mid a$, pour tout $p \in \mathbb{N}$, $b^p \mid a^p$.

Propriété. Soient A un anneau commutatif et $b, a_1, \ldots, a_p, c_1, \ldots, c_p \in A$.
Si pour tout $i \in \{1, \ldots, p\}$, $b \mid a_i$, alors $b \mid \sum_{i=1}^{p} c_i a_i$.

Propriété. Soient A un anneau commutatif et $(a, b) \in A^2$.

$$a|b \iff bA \subseteq aA.$$

Démonstration.
Supposons que $a|b$. Il existe $m \in A$ tel que $b = ma$. Si $bx \in bA$,
$bx = max = a(mx) \in aA$, donc $bA \subseteq aA$.
Réciproquement, supposons que $bA \subseteq aA$. En particulier, $b \in aA$, donc il existe $m \in A$ tel que $b = ma$. □

Propriété. Soit A un anneau commutatif.
La relation de divisibilité est réflexive et transitive.

Démonstration.
Pour tout $a \in A$, $aA \subset aA$, donc $a|a$ et la relation est réflexive.
Soit $(a, b, c) \in A^3$ tel que $a|b$ et $b|c$. Alors $cA \subset bA \subset aA$, donc $a|c$, ce qui démontre la transitivité. □

Remarque. En général, la relation de divisibilité n'est pas une relation d'ordre. En effet, s'il existe $a \in A$ tel que $a + a \neq 0_A$, alors $a|(-a)$, $(-a)|a$ et $-a \neq a$, donc la relation de divisibilité n'est pas antisymétrique.
Cette remarque justifie l'intérêt de la définition suivante.

Définition. Soient A un anneau commutatif et $(a, b) \in A^2$.
On dit que a et b sont ***associés*** si et seulement si $a|b$ et $b|a$.

Propriété. Soient A un anneau commutatif et $(a, b) \in A^2$.
a et b sont associés si et seulement si $aA = bA$.
On en déduit que la relation "être associé à" est une relation d'équivalence.

Propriété. La relation "être associé à", ci-après notée $\sim$ est compatible avec le produit : Dans un anneau commutatif, si $a \sim b$ et $c \sim d$, alors $ac \sim bd$.

Démonstration.
Par hypothèse, il existe $k, k', h, h' \in A$ tels que $b = ka$, $a = k'b$, $d = hc$, $c = h'd$. Ainsi, $bd = khac$ et $ac = k'h'bd$, donc $ac \sim bd$. □

Hypothèse : Jusqu'à la fin de ce paragraphe, on suppose que A est un anneau intègre.

Notation.
On rappelle que $U(A)$ désigne le groupe des éléments inversibles de l'anneau A.

Propriété. Soit $a, b \in A$.
a et b sont associés si et seulement s'il existe $\lambda \in U(A)$ tel que $a = \lambda b$.

Démonstration.
Supposons que a et b sont associés.
il existe $(m, n) \in A^2$ tel que $a = nb$ et $b = ma$, donc $a = mna$. Si $a = 0$, alors $b = 0$ et on a bien $a = 1_A.b$. Sinon, A étant un anneau intègre, $mn = 1$, donc $n \in U(A)$ et $a = nb$.
Réciproquement, s'il existe $\lambda \in U(A)$ tel que $a = \lambda b$, alors $b = \lambda^{-1}a$, donc $a|b$ et $b|a$. □

Exemple. Dans $\mathbb{Z}$, n et m sont associés si et seulement si $|n| = |m|$.
Dans $\mathbb{K}[X]$, P et Q sont associés si et seulement s'il existe $\lambda \in \mathbb{K}^*$ tel que $Q = \lambda P$.

Propriété. La relation de divisibilité est une relation d'ordre sur $\mathbb{N}$.
La relation de divisibilité est une relation d'ordre sur l'ensemble des polynômes unitaires de $\mathbb{K}[X]$.

Définition. Soit $p \in A$.
p est irréductible dans A si et seulement si $p \notin U(A)$ et si, pour tout $a, b \in A$,
$p = ab \Longrightarrow (a \in U(A)) \vee (b \in U(A))$.
Il est équivalent de dire que p est irréductible dans A si et seulement si p n'est pas inversible et a pour seuls diviseurs les éléments associés à 1 ou à p.

Remarque. Si p est irréductible, il est non nul, car $0 = 0 * 0$ et $0 \notin U(A)$ (A est supposé intègre).

Propriété. Les éléments irréductibles de $\mathbb{Z}$ sont les nombres premiers et leurs opposés.

Démonstration.
On rappelle que $p \in \mathbb{N}$ est un nombre premier si et seulement si $p \geq 2$ et si ses seuls diviseurs dans $\mathbb{N}$ sont 1 et p. □

Exemple. Dans $\mathbb{K}[X]$ (où $\mathbb{K}$ est un corps), un polynôme P est irréductible si et seulement si il est de degré supérieur ou égal à 1 et si, pour tout $A, B \in \mathbb{K}[X]$,
$P = AB \Longrightarrow (\deg(A) = 0) \vee (\deg(B) = 0)$.
Dans $\mathbb{K}[X]$, tout polynôme de degré 1 est irréductible.

Exemple.
- $X^2 + 1$ est irréductible sur $\mathbb{R}[X]$, car sinon, on pourrait écrire $X^2 + 1 = AB$ avec $\deg(A) \geq 1$ et $\deg(B) \geq 1$, donc avec $\deg(A) = \deg(B) = 1$, et $X^2 + 1$ possèderait une racine réelle, ce qui est faux.
- De même, $X^2 - 2$ est irréductible sur $\mathbb{Q}[X]$.

— Plus généralement, si $P \in \mathbb{K}[X]$ avec $\deg(P) = 2$, P est réductible sur $\mathbb{K}[X]$ si et seulement si il possède une racine dans $\mathbb{K}$.
— C'est encore vrai lorsque $\deg(P) = 3$, car l'égalité $P = AB$ avec $\deg(A) \geq 1$ et $\deg(B) \geq 1$ impose que l'un des polynômes A ou B est de degré 1.
— Cependant il existe des polynômes de degré 4 de $\mathbb{K}[X]$, composés sur $\mathbb{K}[X]$, ne possédant aucune racine dans $\mathbb{K}[X]$.
Par exemple, avec $\mathbb{K} = \mathbb{R}$ et $P(X) = (X^2 + 1)(X^2 + 2)$.

Définition. Soit $a, b \in A$. On dit que a et b sont premiers entre eux (ou étrangers) si et seulement si les seuls diviseurs communs de a et b sont les éléments inversibles.

Exemple. Dans $\mathbb{Z}$, deux entiers consécutifs sont toujours premiers entre eux.

Définition. Soit $n \in \mathbb{N}$ avec $n \geq 2$ et $a_1, \ldots, a_n \in A$.
— $a_1, \ldots, a_n$ sont deux à deux premiers entre eux si et seulement si, pour tout $i, j \in \{1, \ldots, n\}$ avec $i \neq j$, a_i et a_j sont premiers entre eux.
— $a_1, \ldots, a_n$ sont globalement premiers entre eux si et seulement si les seuls diviseurs communs de $a_1, \ldots, a_n$ sont les éléments inversibles de A.

Remarque. Lorsque $a_1, \ldots, a_n$ sont deux à deux premiers entre eux, ils sont globalement premiers entre eux, mais la réciproque est fausse.
Par exemple, lorsque $A = \mathbb{Z}$, $6, 10$ et 15 sont globalement premiers entre eux, mais ne sont pas deux à deux premiers entre eux.
De même, lorsque $A = \mathbb{K}[X]$, $X(X-1)$, $X(X+1)$ et $X^2 - 1$ sont globalement premiers entre eux, mais ils ne sont pas deux à deux premiers entre eux (on le démontre facilement en décomposant ces polynômes en produits de polynômes irréductibles, cf le caractère factoriel de $\mathbb{K}[X]$).

Propriété. Soit $p \in A$ un élément irréductible et $a \in A$.
Alors ou bien $p|a$, ou bien p et a sont premiers entre eux.

Démonstration.
Supposons que p ne divise pas a et montrons que a et p sont premiers entre eux.
Soit d un diviseur commun de p et de a. Si $d \sim p$, alors $p \mid a$ ce qui est faux, or d est un diviseur de p qui est irréductible, donc $d \sim 1$. Ainsi, si d est un diviseur commun de p et de a, alors d divise 1. □

2.2 PGCD

Théorème. Si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est un anneau principal.

Démonstration.
$\mathbb{K}[X]$ est un anneau intègre.
Soit I un idéal de $\mathbb{K}[X]$.
• Si $I = \{0\}$, $I = 0\mathbb{K}[X]$. Supposons maintenant que $I \neq \{0\}$.
$\{\deg(P)/P \in I \setminus \{0\}\}$ est une partie non vide de $\mathbb{N}$, donc elle admet un plus petit élément, noté m. Il existe un polynôme P_0 de $I \setminus \{0\}$ de degré m.

• Soit $P \in I$. Effectuons la division euclidienne de P par P_0 : il existe $(Q, R) \in \mathbb{K}[X]^2$ tel que $P = P_0Q + R$ avec $\deg(R) < m$.
$R = P - P_0Q \in I$ car I est un idéal, mais $\deg(R) < m$, donc $R = 0$.
Ainsi $P = P_0Q \in P_0\mathbb{K}[X]$.
On a donc montré que $I \subseteq P_0\mathbb{K}[X]$. Mais réciproquement, $P_0 \in I$ et I est un idéal, donc $P_0\mathbb{K}[X] \subseteq I$. Ainsi $I = P_0\mathbb{K}[X]$. □

Remarque. Soit A un anneau intègre. On dit qu'il est euclidien (hors programme) si et seulement si il existe $v : A \setminus \{0\} \longrightarrow \mathbb{N}$ tel que, pour tout $(a, b) \in A \times (A \setminus \{0\})$, il existe $q, r \in A$ vérifiant $a = bq + r$ et $(r = 0) \vee (v(r) < v(b))$.
En adaptant la démonstration précédente, on peut montrer que si A est euclidien, alors A est principal. On admettra que la réciproque est fausse.

Notation. Jusqu'à la fin de ce chapitre "arithmétique", on fixe un anneau A que l'on suppose principal.
Nous allons développer une arithmétique sur A.
$\mathbb{Z}$ étant un anneau principal, on retrouvera ainsi l'arithmétique de $\mathbb{Z}$.
$\mathbb{K}[X]$ étant un anneau principal, on obtiendra ainsi une arithmétique sur les polynômes, analogue à l'arithmétique sur les entiers relatifs.

Remarque. On peut montrer que $\mathbb{Z}[i] = \{n + mi/(n, m) \in \mathbb{Z}^2\}$ est un anneau principal. C'est l'anneau des entiers de Gauss.

Définition. Soit $(a, b) \in A^2$. $aA + bA$ est un idéal et A est principal, donc il existe $d \in A$ tel que $aA + bA = dA$. On dit que d est un PGCD de a et b.
Dans ce cas, d' est un second PGCD de a et b si et seulement si d et d' sont associés.

Remarque. Lorsqu'on a défini le PGCD de deux entiers relatifs, on a imposé à ce PGCD d'être positif pour en garantir l'unicité. En effet, dans $\mathbb{Z}$, deux éléments sont associés si et seulement si ils sont égaux ou opposés.

Propriété. Soit $(a, b) \in A^2$. Notons d un PGCD de a et b.
Alors d est un diviseur commun de a et b.
De plus, si d' est un autre diviseur commun de a et b, alors d' divise d.
C'est la raison pour laquelle d est appelé le plus grand commun diviseur de a et b, ou, par abréviation, le ***PGCD*** de a et b.

Démonstration.
$a = a.1_A + b.0_A \in aA + bA = dA$, donc a est un multiple de d.
De même, on montre que b est un multiple de d.
Si d' est un diviseur commun de a et de b, $(a, b) \in (d'A)^2$, donc $aA + bA \subset d'A$,
or $d \in aA + bA$, donc $d \in d'A$, ce qui prouve que d' divise d. □

Caractérisation du PGCD par divisibilité :
d est un PGCD de $(a, b) \in A^2$ si et seulement si d est un diviseur commun de a et b et si, pour tout diviseur commun d' de a et b, d' divise d.

Démonstration.
Le sens direct correspond à la propriété précédente.
Réciproquement, supposons que d est un diviseur commun de a et b et que, pour tout diviseur commun d' de a et b, d' divise d.
Il existe $e \in A$ tel que $aA + bA = eA$.
d divise a et b, et e est un PGCD de a et b, donc on a vu que d divise e.
e divise a et b, donc par hypothèse, e divise d. Ainsi, e et d sont associés, donc d est un PGCD de a et b. □

Propriété. a et b sont premiers entre eux si et seulement si 1 est un PGCD de a et b.

Définition. Plus généralement, si $k \in \mathbb{N}^*$ et si $a_1, \dots, a_k \in A$, on dit que d est un PGCD de $a_1, \dots, a_k$ si et seulement si $dA = a_1A + \cdots + a_kA$.
Alors d est un commun diviseur de $a_1, \dots, a_k$ et si d' est un autre commun diviseur de $a_1, \dots, a_k$, alors d' divise d.
Si B est une partie quelconque de A, on dit que d est un PGCD de B si et seulement si $dA = Id(B)$. Alors d est un diviseur commun des éléments de B et si d' est un autre diviseur commun des éléments de B, alors d' divise d.

Propriété. Soit B une partie de A. d est un PGCD de B si et seulement si c'est un diviseur commun des éléments de B et si, pour tout diviseur commun d' des éléments de B, d' divise d.

Démonstration.
Adapter les démonstrations précédentes. □

Propriété. Soit $k \in \mathbb{N}$, $a_1, \dots, a_k \in A$ et $h \in \{1, \dots, k\}$.
Alors, en convenant de noter $a \sim b$ lorsque a et b sont associés,
- Commutativité du PGCD :
  pour tout $\sigma \in \mathcal{S}_k$, $PGCD(a_1, \dots, a_k) \sim PGCD(a_{\sigma(1)}, \dots, a_{\sigma(k)})$.
- Associativité du PGCD :
  $PGCD(a_1, \dots, a_k) \sim PGCD(PGCD(a_1, \dots, a_h), PGCD(a_{h+1}, \dots, a_k))$.
- Distributivité de la multiplication par rapport au PGCD : pour tout $\alpha \in A$,
  $PGCD(\alpha a_1, \dots, \alpha a_k) \sim \alpha PGCD(a_1, \dots, a_k)$.

Démonstration.
◇ La commutativité est claire.
◇ Notons $d = PGCD(a_1, \dots, a_k)$, $d' = PGCD(a_1, \dots, a_h)$
et $d'' = PGCD(a_{h+1}, \dots, a_k)$. Alors
$dA = a_1A + \cdots + a_kA = (a_1A + \cdots + a_hA) + (a_{h+1}A + \cdots + a_kA) = d'A + d''A$,
donc $dA = PGCD(d', d'')A$.
◇ Notons $d = PGCD(a_1, \dots, a_k)$, $d' = PGCD(\alpha a_1, \dots, \alpha a_k)$. Alors

$$\begin{aligned} d'A &= (\alpha a_1)A + \cdots + (\alpha a_k)A \\ &= \{\sum_{i=1}^{k} \alpha a_i b_i \ / \ b_1, \dots, b_k \in A\} \\ &= \alpha(a_1A + \cdots + a_kA) \\ &= \alpha(dA) = (\alpha d)A. \end{aligned}$$

□

Propriété. Lorsque $A = \mathbb{K}[X]$, en imposant au PGCD d'être unitaire ou nul, il est unique et on le note encore $a \wedge b$.

Exemple. $X^2 - 2X + 1 = (X-1)^2$ et $(X-1)(X-2) = X^2 - 3X + 2$, donc $(X^2 - 2X + 1) \wedge (X^2 - 3X + 2) = (X-1) \times [(X-1) \wedge (X-2)]$, or
$(X-1) - (X-2) = 1$, donc $(X-1)\mathbb{K}[X] + (X-2)\mathbb{K}[X] = \mathbb{K}[X]$.
Ainsi, $(X-1) \wedge (X-2) = 1$, puis $(X^2 - 2X + 1) \wedge (X^2 - 3X + 2) = X - 1$.

Remarque. Comme dans le cas des entiers relatifs, en notant $\mathcal{U}$ l'ensemble constitué du polynôme nul et des polynômes unitaires, la relation de divisibilité est une relation d'ordre sur $\mathcal{U}$ et, pour toute partie B de $\mathcal{U}$, le PGCD de B est la borne inférieure de B pour la relation de divisibilité. En particulier, le PGCD de $\emptyset$ est égal à $\max_{|}(\mathcal{U}) = 0$.

2.3 PPCM

Définition. Soit $(a, b) \in A^2$. $aA \cap bA$ est un idéal et A est principal, donc il existe $m \in A$ tel que $aA \cap bA = mA$. On dit que m est un PPCM de a et b.
Dans ce cas, m' est un second PPCM de a et b si et seulement si m et m' sont associés.

Remarque. Comme pour le PGCD, lorsqu'on a défini le PPCM de deux entiers relatifs, on a imposé à ce PPCM d'être positif afin qu'il soit défini de manière unique.

Propriété. Soit $(a, b) \in A^2$. Notons m un PPCM de a et b.
Alors m est un multiple commun de a et b, et si m' est un autre multiple commun de a et b, alors m' est un multiple de m.
C'est la raison pour laquelle m est appelé le plus petit commun multiple de a et b, ou, par abréviation, le ***PPCM*** de a et b.

Démonstration.
$m \in mA = aA \cap bA \subset aA$, donc a divise m.
De même, on montre que b divise m.
Si m' est un multiple commun de a et de b, $m' \in aA \cap bA = mA$, donc m' est un multiple de m. □

Caractérisation du PPCM par divisibilité :
m est un PPCM de $(a, b) \in A^2$ si et seulement si m est un multiple commun de a et b et si, pour tout multiple commun m' de a et b, m' est un multiple de m.

Démonstration.
Le sens direct correspond à la propriété précédente.
Réciproquement, supposons que m est un multiple commun de a et b et que, pour tout multiple commun m' de a et b, m' soit un multiple de m.
Il existe $e \in A$ tel que $aA \cap bA = eA$.
m est un multiple de a et b, et e est un PPCM de a et b, donc on a vu que m est un multiple de e.

e est un multiple de a et b, donc par hypothèse, e est un multiple de m. Ainsi, e et m sont associés, donc m est un PPCM de a et b. □

Définition. Plus généralement, si $k \in \mathbb{N}^*$ et si $a_1, \dots, a_k \in A$, on dit que m est un PPCM de $a_1, \dots, a_k$ si et seulement si $mA = a_1A \cap \dots \cap a_kA$.
Alors m est un commun multiple de $a_1, \dots, a_k$ et si m' est un autre commun multiple de $a_1, \dots, a_k$, alors m' est un multiple de m.
Si B est une partie quelconque de A, on dit que m est un PPCM de B si et seulement si $mA = \bigcap_{b \in B} bA$. Alors m est un multiple commun des éléments de B et si m' est un autre multiple commun des éléments de B, alors m' est un multiple commun de m.

Remarque. Dans ce contexte, on convient que si $B = \emptyset$, $\bigcap_{b \in B} bA = A$, donc 1_A est un PPCM de $\emptyset$.

Propriété. Soit B une partie de A. m est un PPCM de B si et seulement si c'est un multiple commun des éléments de B et si, pour tout multiple commun m' des éléments de B, m' est un multiple de m.

Démonstration.
Adapter les démonstrations précédentes. □

Propriété. Soit $k \in \mathbb{N}$, $a_1, \dots, a_k \in A$ et $h \in \{1, \dots, k\}$.
Alors, en convenant de noter $a \sim b$ lorsque a et b sont associés,
- Commutativité du PPCM :
  pour tout $\sigma \in \mathcal{S}_k$, $PPCM(a_1, \dots, a_k) \sim PPCM(a_{\sigma(1)}, \dots, a_{\sigma(k)})$.
- Associativité du PPCM :
  $PPCM(a_1, \dots, a_k) \sim PPCM(PPCM(a_1, \dots, a_h), PPCM(a_{h+1}, \dots, a_k))$.
- Distributivité de la multiplication par rapport au PPCM :
  pour tout $\alpha \in A$, $PPCM(\alpha a_1, \dots, \alpha a_k) \sim \alpha PPCM(a_1, \dots, a_k)$.

Démonstration.
◇ La commutativité est claire.
◇ Notons $m = PPCM(a_1, \dots, a_k)$, $m' = PPCM(a_1, \dots, a_h)$
et $m'' = PPCM(a_{h+1}, \dots, a_k)$. Alors
$mA = a_1A \cap \dots \cap a_kA = (a_1A \cap \dots \cap a_hA) \cap (a_{h+1}A \cap \dots \cap a_kA) = m'A \cap m''A$,
donc $mA = PPCM(m', m'')A$.
◇ La dernière propriété est évidente lorsque $\alpha = 0$. Supposons maintenant que $\alpha \neq 0$.
Notons $m = PPCM(a_1, \dots, a_k)$, $m' = PPCM(\alpha a_1, \dots, \alpha a_k)$. Alors
$m'A = [(\alpha a_1)A] \cap \dots \cap [(\alpha a_k)A]$.
Soit $x \in m'A$: pour tout $i \in \{1, \dots, k\}$, il existe $b_i \in A$ tel que $x = \alpha a_i b_i$.
Soit $i \in \{2, \dots, k\}$: $\alpha a_1 b_1 = \alpha a_i b_i$ et $\alpha \neq 0$, or A est intègre, donc $a_1 b_1 = a_i b_i$.
Ainsi $a_1 b_1 \in a_1A \cap \dots \cap a_kA$, puis $x = \alpha a_1 b_1 \in \alpha(a_1A \cap \dots \cap a_kA)$, ce qui montre que $m'A \subset \alpha(a_1A \cap \dots \cap a_kA)$.
Réciproquement, si $x \in \alpha(a_1A \cap \dots \cap a_kA)$, il existe $y \in a_1A \cap \dots \cap a_kA$ tel que $x = \alpha y$.
Pour tout $i \in \{1, \dots, k\}$, il existe $b_i \in A$ tel que $y = a_i b_i$, donc $x = \alpha a_i b_i \in \alpha a_i A$. Ainsi $x \in [(\alpha a_1)A] \cap \dots \cap [(\alpha a_k)A] = m'A$.

En conclusion, $m'A = \alpha(a_1A \cap \cdots \cap a_kA) = \alpha(mA) = (\alpha m)A$. □

Propriété. Lorsque $A = \mathbb{K}[X]$, en imposant au PPCM d'être unitaire ou nul, il est unique et on le note encore $a \vee b$.

Remarque. Si l'on note encore $\mathcal{U}$ l'ensemble constitué du polynôme nul et des polynômes unitaires, pour toute partie B de $\mathcal{U}$, le PPCM de B est la borne supérieure de B pour la relation de divisibilité. En particulier, le PPCM de $\emptyset$ est égal à $\min_{|}(\mathcal{U}) = 1$.

2.4 Les théorèmes de l'arithmétique

Théorème de *Bézout*. Soit $(a, b) \in A^2$.
a et b sont premiers entre eux si et seulement si : $\exists (u, v) \in A^2 \ \ ua + vb = 1$.

Démonstration.
a et b sont premiers entre eux si et seulement si $A = aA + bA$, donc si et seulement si $aA + bA$ contient 1. En effet, on a déjà établi qu'un idéal contient 1 si et seulement si il est égal à A. □

Remarque. Dans un anneau intègre quelconque, le sens indirect est toujours vrai mais la réciproque peut être fausse. Ainsi, dans $\mathbb{R}[X, Y]$, X et Y sont premiers entre eux, mais il n'existe aucun $U, V \in \mathbb{R}[X, Y]$ tels que $UX + VY = 1$.

Théorème de Bézout (généralisation). Soit $n \in \mathbb{N}$ avec $n \geq 2$ et $a_1, \ldots, a_n \in A$.
$a_1, \ldots, a_n$ sont globalement premiers entre eux si et seulement si :
$\exists u_1, \ldots, u_n \in A \ , \ \ u_1a_1 + \cdots + u_na_n = 1$.

Propriété. Soit $(a, b) \in A^2$. Notons d un PGCD de a et b. Alors
il existe $(a', b') \in A^2$, avec a' et b' premiers entre eux, tel que $a = a'd$ et $b = b'd$.

Démonstration.
d divise a et b, donc il existe $(a', b') \in A^2$ tel que $a = a'd$ et $b = b'd$.
$d = a \wedge b \sim (a'd) \wedge (b'd) = d(a' \wedge b')$, donc si d est différent de 0, $a' \wedge b' \sim 1$,
et si $d = 0$, alors $aA + bA = \{0\}$, donc $a = b = 0$. Dans ce cas, $a' = b' = 1_A$ conviennent.
□

Théorème de *Gauss*. Soit $(a, b, c) \in A^3$.
Si $a|bc$ avec a et b premiers entre eux, alors $a|c$.

Démonstration.
$PGCD(ac, bc) \sim cPGCD(a, b) \sim c$, or a est un diviseur commun de ac et de bc, donc il divise c. □

Corollaire. Soit $p, a, b \in A$.
Si $p \mid ab$ et si p est irréductible, alors $p \mid a$ ou $p \mid b$.

Démonstration.
p étant irréductible, on sait que $p \mid a$ ou bien $p \wedge a = 1$. □

Remarque. C'est faux lorsque p n'est pas irréductible : dans $\mathbb{Z}$, $6 \mid 2 \times 3$, mais 6 ne divise ni 2, ni 3.

Corollaire. Soit $(a,b,c) \in A^3$, $n \in \mathbb{N}^*$ et $a_1, \dots, a_n \in A$.
On désigne par $a \wedge b$ un PGCD de a et b et par $a \vee b$ un PPCM de a et b.
$\diamond$ Si $a \wedge b = a \wedge c = 1$, alors $a \wedge bc = 1$.
$\diamond$ On en déduit que, si $a \wedge b = 1$, $\forall (k,l) \in (\mathbb{N}^*)^2 \;\; a^k \wedge b^l = 1$.
$\diamond$ Si $a|b$, $c|b$ et $a \wedge c = 1$ alors $ac|b$. Par récurrence, on en déduit que
si pour tout $i \in \{1, \dots, n\}$, $a_i|b$ et si $i \neq j \Longrightarrow a_i \wedge a_j = 1$, alors $a_1 \times \cdots \times a_n \mid b$.
$\diamond$ $ab \sim (a \wedge b)(a \vee b)$. En particulier, $a \wedge b = 1 \Longrightarrow a \vee b \sim ab$.

Démonstration.
$\diamond$ Supposons que $a \wedge b = a \wedge c = 1$. Alors d'après le théorème de Bézout, il existe $u, v, u', v' \in A$ tels que $ua + vb = 1$ et $u'a + v'c = 1$. En formant le produit de ces deux égalités, on obtient $1 = vv'(bc) + a(uu'a + uv'c + vbu')$, donc $a \wedge bc = 1$.
$\diamond$ Supposons que $a|b$, $c|b$ et $a \wedge c = 1$.
$ac \mid bc$ et $ac \mid ab$, donc ac divise $(bc) \wedge (ab) \sim b(c \wedge a) \sim b$.
$\diamond$ Posons $d = a \wedge b$.
On a vu qu'il existe $a', b' \in A$ tels que $a' \wedge b' = 1$, $a = a'd$ et $b = b'd$.
a' et b' divisent $a' \vee b'$, donc d'après la propriété précédente, $a'b' \mid a' \vee b'$, mais $a'b'$ est un multiple commun de a' et b', donc c'est un multiple de $a' \vee b'$. Ainsi $a'b' \sim a' \vee b'$.
Alors, la relation $\sim$ étant compatible avec le produit,
$a \vee b \sim (a'd) \vee (b'd) \sim (a' \vee b')d \sim a'b'd$, puis $ab = d(a'b'd) \sim (a \wedge b)(a \vee b)$. $\square$

Exemple. $X^2 - 2X + 1 = (X-1)^2$ et $(X-1)(X-2) = X^2 - 3X + 2$, donc $(X^2 - 2X + 1) \vee (X^2 - 3X + 2) = (X-1)^2(X-2)$.
En effet, on a déjà vu que $(X^2 - 2X + 1) \wedge (X^2 - 3X + 2) = X - 1$,
donc $[(X^2 - 2X + 1) \vee (X^2 - 3X + 2)](X-1) = (X-1)^3(X-2)$.

ATTENTION : En général, $abc \not\sim (a \wedge b \wedge c)(a \vee b \vee c)$.
Par exemple, dans $\mathbb{Z}$, $6 \wedge 10 \wedge 15 = (6 \wedge 10) \wedge 15 = 1$
et $6 \vee 10 \vee 15 = (6 \vee 10) \vee 15 = 30 \vee 15 = 30$, mais $30 \times 1 \neq 6 \times 10 \times 15$.

2.5 $\mathbb{K}[X]$ est un anneau factoriel

Notation. Dans ce paragraphe, l'anneau A est égal à $\mathbb{Z}$ ou à $\mathbb{K}[X]$ ($\mathbb{K}$ étant un corps quelconque). Ainsi, lorsque $A = \mathbb{Z}$, on va retrouver l'arithmétique connue sur $\mathbb{Z}$ et lorsque $A = \mathbb{K}[X]$, on va développer une arithmétique en tout point analogue.
On note $\mathcal{P}$ l'ensemble suivant : si $A = \mathbb{Z}$, $\mathcal{P}$ est l'ensemble des nombres premiers, et si $A = \mathbb{K}[X]$, $\mathcal{P}$ est l'ensemble des polynômes irréductibles et unitaires.

Théorème. Soit $a \in A$ avec $a \neq 0$. Il existe un unique couple $(u, (\nu_p)_{p \in \mathcal{P}})$, où $u \in U(A)$ et où $(\nu_p)_{p \in \mathcal{P}}$ est une famille presque nulle d'entiers, tel que

$$a = u \prod_{p \in \mathcal{P}} p^{\nu_p}. \tag{1}$$

On dit que (1) est la ***décomposition de a en facteurs irréductibles***.
ν_p s'appelle la valuation p-adique de a.

Démonstration.
On a déjà vu la démonstration de ce théorème lorsque $A = \mathbb{Z}$.
Adaptons cette démonstration au cas où $A = \mathbb{K}[X]$.
◇ L'existence se démontre par récurrence forte : pour tout $n \in \mathbb{N}$, notons $R(n)$ l'assertion suivante : pour tout polynôme N de degré n, il existe une famille presque nulle d'entiers $(\nu_P)_{P\in\mathcal{P}}$ et il existe $u \in \mathbb{K}^*$ tels que $N = u\prod_{P\in\mathcal{P}} P^{\nu_P}$.
Pour $n = 0$, si N est un polynôme de degré nul, $N \in \mathbb{K}^*$, donc il suffit de prendre $(\nu_P)_{P\in\mathcal{P}}$ égale à la famille identiquement nulle.
Pour $n \geq 1$, supposons $R(k)$ pour tout $k \in \{1, \dots, n-1\}$.
Soit N un polynôme de degré égal à n.
Si N est irréductible, l'existence est assurée.
Sinon, il existe $P, Q \in \mathbb{K}[X]$ tels que $\deg(P) \geq 1$, $\deg(Q) \geq 1$ et $PQ = N$. Alors $\deg(P), \deg(Q) \in \{1, \dots, n-1\}$, donc on peut utiliser $R(\deg(P))$ et $R(\deg(Q))$ pour montrer que N se décompose bien en produit de polynômes unitaires irréductibles.
◇ Pour démontrer l'unicité, fixons $N \in \mathbb{K}[X] \setminus \{0\}$ et supposons qu'il existe deux familles presque nulles $(\nu_P)_{P\in\mathcal{P}}$ et $(\eta_P)_{P\in\mathcal{P}}$ ainsi que $u, u' \in \mathbb{K}^*$ tels que
$N = u\prod_{P\in\mathcal{P}} P^{\nu_P} = u'\prod_{P\in\mathcal{P}} P^{\eta_P}$. Alors u est le coefficient dominant de N, ainsi que u', donc $u = u'$ et $\prod_{P\in\mathcal{P}} P^{\nu_P} = \prod_{P\in\mathcal{P}} P^{\eta_P}$.
Supposons qu'il existe $P_0 \in \mathcal{P}$ tel que $\nu_{P_0} \neq \eta_{P_0}$.
Sans perte de généralité, on peut supposer que $\nu_{P_0} < \eta_{P_0}$, donc en posant
$\alpha = \eta_{P_0} - \nu_{P_0} \in \mathbb{N}^*$, on a $\prod_{\substack{P\in\mathcal{P}\\P\neq P_0}} P^{\nu_P} = P_0^{\alpha}\prod_{\substack{P\in\mathcal{P}\\P\neq P_0}} P^{\eta_P}$. Alors $P_0 \mid \prod_{\substack{P\in\mathcal{P}\\P\neq P_0}} P^{\nu_P}$, mais P_0 est premier avec tout $P \in \mathcal{P}$ tel que $P \neq P_0$, donc P_0 est premier avec $\prod_{\substack{P\in\mathcal{P}\\P\neq P_0}} P^{\nu_P}$, puis d'après le théorème de Gauss, $P_0 \mid 1$, ce qui est faux. □

Remarque. (hors programme, purement culturel).
◇ On dit qu'un anneau est factoriel si et seulement si c'est un anneau intègre dans lequel pour tout $a \in A \setminus \{0\}$, il existe $u \in U(A)$, $r \in \mathbb{N}$ et $p_1, \dots, p_r$ irréductibles dans A tels que $a = up_1 \cdots p_r$, cette décomposition étant de plus unique : si $a = vq_1 \cdots q_s$ avec $v \in U(A)$, $s \in \mathbb{N}$ et $q_1, \dots, q_s$ irréductibles dans A, alors $r = s$ et il existe $\sigma \in \mathcal{S}_r$ telle que pour tout $i \in \{1, \dots, r\}$, p_i et $q_{\sigma(i)}$ sont associés.
◇ Ainsi, on vient de montrer que $\mathbb{Z}$ et $\mathbb{K}[X]$ sont des anneaux factoriels.
◇ En fait, on peut montrer que tout anneau principal est factoriel.
◇ Si A est factoriel, alors on peut montrer que $A[X]$ est factoriel.
◇ Ainsi, $\mathbb{R}[X, Y]$ est un anneau factoriel, mais non principal.
◇ En résumé, pour un anneau intègre,
euclidien $\Longrightarrow$ principal $\Longrightarrow$ factoriel, mais les réciproques sont fausses.

Remarque historique. L'anneau $\mathbb{Z}[i] = \{n + mi/(n, m) \in \mathbb{Z}^2\}$ que Gauss étudia au début du $XIX^{\text{ème}}$ est factoriel. En 1843, pour démontrer une conjecture formulée par

Fermat (1601-1665) (pour tout entier $n \geq 3$, pour tout $(x,y,z) \in (\mathbb{Z}^*)^3$, $x^n + y^n \neq z^n$), Kummer considère l'anneau $\mathbb{Z}[e^{\frac{2i\pi}{p}}] = \{\sum_{h=0}^{p-1} a_h e^{\frac{2ih\pi}{p}} / (a_0, \ldots, a_{p-1}) \in \mathbb{Z}^p\}$ que l'on appelle maintenant le $p^{\text{ème}}$ anneau cyclotomique. Kummer suppose, par analogie avec l'anneau de Gauss, que l'anneau cyclotomique est factoriel et parvient à démontrer la conjecture de Fermat ... Mais les anneaux cyclotomiques sont-ils factoriels ? Ce sujet anime alors de nombreux mathématiciens, qui réalisent que malheureusement seuls certains anneaux cyclotomiques sont factoriels. Certains historiens des mathématiques pensent d'ailleurs que Fermat dans sa démonstration "trop longue pour tenir dans cette marge" commet une erreur de ce type.
Mais Kummer ne désarme pas, et il cherche à modifier les anneaux cyclotomiques pour qu'ils deviennent factoriels. Ceci le conduira à la notion de nombre idéal (des nombres formels que l'on rajoute à l'anneau cyclotomique pour qu'il devienne factoriel). En 1845, il parvient ainsi à montrer la conjecture de Fermat pour certains nombres premiers, dont notamment tous les nombres premiers inférieurs à 100.
Devant l'échec relatif de Kummer, Dedekind emprunte une autre voie. Il cherche à reformuler la propriété d'unicité de la décomposition en facteurs premiers sous une forme voisine mais vérifiée par davantage d'anneaux. C'est ce qui l'amène à introduire une nouvelle structure qu'il baptise "idéal" en hommage à Kummer qui l'a largement inspiré.
Cependant, il fallut attendre 1994 pour que la conjecture de Fermat devienne le théorème de Fermat-Wiles.

Propriété. Soit $(a,b) \in (A\backslash\{0\})^2$. Ecrivons les décompositions de a et de b en facteurs irréductibles.

$$a = u \prod_{p \in \mathcal{P}} p^{\nu_p} \text{ et } b = v \prod_{p \in \mathcal{P}} p^{\mu_p}.$$

Alors $a \mid b \iff [\forall p \in \mathcal{P},\ \ \nu_p \leq \mu_p]$. De plus,

$$a \wedge b = \prod_{p \in \mathcal{P}} p^{\min(\nu_p, \mu_p)} \text{ et } a \vee b = \prod_{p \in \mathcal{P}} p^{\max(\nu_p, \mu_p)}.$$

En particulier, a et b sont premiers entre eux si et seulement si aucun élément de $\mathcal{P}$ n'intervient à la fois dans la décomposition en facteurs irréductibles de a et dans celle de b.

Démonstration.
$\diamond$ Si pour tout $p \in \mathcal{P}$, $\nu_p \leq \mu_p$, alors $b = vu^{-1}a \times \prod_{p \in \mathcal{P}} p^{\mu_p - \nu_p}$, donc $a \mid b$.
Réciproquement, supposons que $a \mid b$. Soit $p \in \mathcal{P}$. $p^{\nu_p} \mid a$, donc $p^{\nu_p} \mid b$. Ainsi, d'après le théorème de Gauss, $p^{\nu_p} \mid p^{\mu_p}$. Si $\nu_p > \mu_p$, alors $p \mid p^{\nu_p - \mu_p} \mid 1$, ce qui est faux, donc pour tout $p \in \mathcal{P}$, $\nu_p \leq \mu_p$.
$\diamond$ Notons $d = \prod_{p \in \mathcal{P}} p^{\min(\nu_p, \mu_p)}$: d divise a et b. De plus, soit c un diviseur commun de a

et b. Décomposons c en facteurs irréductibles : $c = w\prod_{p\in\mathcal{P}} p^{\eta_p}$.
$c \mid a$, donc pour tout $p \in \mathcal{P}$, $\eta_p \leq \nu_p$.
$c \mid b$, donc pour tout $p \in \mathcal{P}$, $\eta_p \leq \mu_p$.
Ainsi, pour tout $p \in \mathcal{P}$, $\eta_p \leq \min(\nu_p, \mu_p)$. On en déduit que $c \mid d$. Ainsi, d'après la caractérisation du PGCD par divisibilité, $d = a \wedge b$.
On en déduit la formule pour $a \vee b$, car on a vu que $a \vee b = \dfrac{ab}{a \wedge b}$. □

Exemple. Pour calculer les pgcd et ppcm de 1836 et 234, on peut utiliser leurs décompositions primaires : $1836 = 4 * 459 = 4 * 3 * 153 = 2^2 * 3^2 * 51 = 2^2 * 3^3 * 17$ et $234 = 2 * 117 = 2 * 3 * 39 = 2 * 3^2 * 13$, donc $1836 \wedge 234 = 2 * 3^2 = 18$ et $1836 \vee 234 = 2^2 * 3^3 * 13 * 17 = 23\,868$.

Remarque. Cet algorithme pour le calcul du PGCD de a et b n'est pas efficace, car le calcul de la décomposition de a en facteurs irréductibles est d'une grande complexité algorithmique. L'algorithme d'Euclide présenté ci-dessous est beaucoup plus efficace.

Lemme d'Euclide. Soient $(a, b) \in A^2$ avec $b \neq 0$. Notons q et r les quotient et reste de la division euclidienne de a par b. Alors $a \wedge b = b \wedge r$.

Démonstration.
• $aA + bA = (bq + r)A + bA$.
Soit $c \in (bq + r)A + bA$. Il existe $(x, y) \in A^2$ tel que
$c = (bq + r)x + by = b(qx + y) + rx \in bA + rA$, donc $(bq + r)A + bA \subseteq bA + rA$.
• Réciproquement, soit $c \in bA + rA$. Il existe $(x, y) \in A^2$ tel que
$c = bx + ry = (bq + r)y + b(x - qy) \in (bq + r)A + bA$, donc $bA + rA \subseteq (bq + r)A + bA$.
Ainsi $aA + bA = (bq + r)A + bA = bA + rA$. □

Algorithme d'Euclide. Soit $(a_0, a_1) \in A^2$.
• Pour $i \geq 1$, tant que $a_i \neq 0$, on note a_{i+1} le reste de la division euclidienne de a_{i-1} par a_i.
On définit ainsi une suite finie $(a_i)_{0\leq i\leq N}$ d'éléments de A (lorsque $A = \mathbb{Z}$, cette suite est strictement décroissante pour $i \geq 1$, et lorsque $A = \mathbb{K}[X]$, la suite des degrés des a_i est strictement décroissante pour $i \geq 1$) telle que $a_N = 0$ et, pour tout $i \in \{0, \ldots, N - 1\}$, $a_0 \wedge a_1 = a_i \wedge a_{i+1}$.
En particulier, pour $i = N - 1$, on obtient $a_0 \wedge a_1 = a_{N-1}$.
Cet algorithme, appelé algorithme d'Euclide permet donc de calculer le PGCD de deux éléments de A.
• Supposons maintenant que $a_0 \wedge a_1 = a_{N-1} = 1$. D'après le théorème de Bézout, il existe $(s, t) \in A^2$ tel que $sa_0 + ta_1 = 1$. La suite de l'algorithme d'Euclide permet le calcul d'un tel couple (s, t) :
Notons q_i le quotient de la division euclidienne de a_{i-1} par a_i. Ainsi, $a_{i-1} = q_i a_i + a_{i+1}$, c'est-à-dire $a_{i+1} = a_{i-1} - q_i ai$.
En particulier, avec $i = N - 2$, on obtient $1 = a_{N-3} - q_{N-2}a_{N-2}$.

Supposons que, pour un entier $i \in \{1, \dots, N-3\}$, on dispose d'entiers s_i et t_i tels que $1 = s_i a_i + t_i a_{i+1}$. Alors $1 = s_i a_i + t_i(a_{i-1} - a_i q_i) = (s_i - t_i q_i)a_i + t_i a_{i-1}$, ce qui donne des entiers s_{i-1} et t_{i-1} tels que $1 = s_{i-1}a_{i-1} + t_{i-1}a_i$.
Par récurrence descendante, on peut donc calculer des entier s_0 et t_0
tels que $1 = s_0 a_0 + t_0 a_1$.

Corollaire. Supposons que $\mathbb{L}$ est un sous-corps de $\mathbb{K}$.
Si $(A, B) \in \mathbb{L}[X] \times (\mathbb{L}[X] \setminus \{0\})$, on a vu que les quotient et reste de la division euclidienne sont les mêmes que l'on regarde A et B comme des polynômes de $\mathbb{L}[X]$ ou de $\mathbb{K}[X]$. On en déduit que le PGCD (et donc le PPCM) de A et B est le même, que l'on regarde A et B comme des polynômes de $\mathbb{L}[X]$ ou de $\mathbb{K}[X]$.

Exemple. Dans $\mathbb{R}[X]$ avec $A(X) = X^3 - 2$ et $B(X) = X^2 + 3X + 5$.
$A(X) = (X-3)(X^2+3X+5)+(4X+13)$, puis $X^2+3X+5 = \frac{1}{4}(4X+13)(X-\frac{1}{4})+\frac{93}{16}$,
donc $A \wedge B = 1$. De plus, $\frac{93}{16} = B - \frac{1}{4}(4X+13)(X-\frac{1}{4}) = B - \frac{1}{4}(X-\frac{1}{4})(A-(X-3)B)$,
donc $\frac{93}{16} = -\frac{1}{4}(X-\frac{1}{4})A + B(1+\frac{1}{4}(X-\frac{1}{4})(X-3))$,
puis $-\frac{1}{93}(4X-1)A + B\frac{1}{93}(4X^2-13X+19) = 1$.

Exercice. Soit $a, b, c \in A$ avec a et b non nuls.
Résoudre l'équation de Bézout (B) : $au + bv = c$ en l'inconnue $(u, v) \in A^2$.

Solution : Supposons que (B) possède au moins une solution $(u, v) \in A^2$. Alors $c \in aA + bA = (a \wedge b)A$, donc c est un multiple de $a \wedge b$.
Ainsi, lorsque c n'est pas un multiple de $a \wedge b$, (B) n'admet aucune solution.
Pour la suite, on suppose que $a \wedge b \mid c$. a étant non nul, $a \wedge b \neq 0$, donc, quitte à diviser a, b et c par $a \wedge b$, on peut supposer que a et b sont premiers entre eux.
Alors grâce à l'algorithme d'Euclide, on peut déterminer un couple $(u, v) \in A^2$ tel que $ua + bv = 1$, puis en multipliant par c, on en déduit un couple $(u_0, v_0) \in A^2$ qui est une solution particulière de (B).
Soit $(u, v) \in A^2$ une solution de (B). Alors $(u - u_0)a + (v - v_0)b = 0$, donc $b \mid a(u - u_0)$ puis d'après le théorème de Gauss, $b \mid u - u_0$. Ainsi, il existe $\lambda \in A$ tel que $u = u_0 + \lambda b$. Alors $0 = (u - u_0)a + (v - v_0)b = b(\lambda a + v - v_0)$, or $b \neq 0$ et A est intègre, donc $v = v_0 - \lambda a$. Réciproquement, s'il existe $\lambda \in A$ tel que $(u, v) = (u_0 + \lambda b, v_0 - \lambda a)$, on vérifie que $ua + vb = u_0 a + v_0 b = c$, donc l'ensemble des solutions de l'équation de Bézout est $\{(u_0 + \lambda b, v_0 - \lambda a) \ / \ \lambda \in A\}$.

3 Racines d'un polynôme

3.1 Corps de rupture (hors programme)

Soit $\mathbb{K}$ un corps et P un polynôme irréductible de $\mathbb{K}[X]$ tel que $\deg(P) \geq 2$. Ainsi P ne possède aucune racine dans $\mathbb{K}$.

◇ Posons $\mathbb{L} = \mathbb{K}[X]/P(X)\mathbb{K}[X]$.

Soit $\overline{Q} \in \mathbb{L} \setminus \{0\}$. P étant irréductible et n'étant pas un diviseur de Q, P et Q sont premiers entre eux, donc il existe $U, V \in \mathbb{K}[X]$ tels que $UP + VQ = 1$. Ainsi,
$\overline{V}\ \overline{Q} = \overline{1} = 1$, donc $\overline{Q}$ est inversible dans $\mathbb{L}$.

De plus, $\mathbb{L}$ est non nul et commutatif, donc c'est un corps.

◇ L'application $\begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{L} \\ a & \longmapsto & \overline{a} \end{array}$ est un morphisme de corps, donc il est injectif et il permet d'identifier $\mathbb{K}$ avec une partie de $\mathbb{L}$.

Soit $\lambda \in \mathbb{L}$. Il existe $Q \in \mathbb{K}[X]$ tel que $\lambda = \overline{Q}$.

Par division euclidienne, $Q = PH + R$ avec $\deg(R) < deg(P)$.

Ainsi, $\lambda = \overline{R} = \sum_{k=0}^{n-1} \overline{r_k}\overline{X}^k$, où $n = \deg(P)$.

Alors, en posant $\alpha = \overline{X}$ et en utilisant l'identification précédente entre $\mathbb{K}$ et une partie de $\mathbb{L}$, on obtient que $\mathbb{L} = \{\sum_{k=0}^{n-1} r_k\alpha^k / (r_0, \ldots, r_{n-1}) \in \mathbb{K}^n\}$.

Ainsi, $\mathbb{L}$ est un sur-corps de $\mathbb{K}$. On dit que c'est une extension de $\mathbb{K}$.

◇ Soit $(r_0, \ldots, r_{n-1}) \in \mathbb{K}^n$ tel que $\sum_{k=0}^{n-1} r_k\alpha^k = 0$.

Posons $R(X) = \sum_{k=0}^{n-1} r_k X^k$: $\overline{R} = 0$, donc P divise R : il existe $H \in \mathbb{K}[X]$ tel que $R = PH$. Mais alors $\deg(H) = \deg(R) - \deg(P) < 0$, donc $H = 0$, puis $R = 0$.

On en déduit que $r_0 = \cdots = r_{n-1} = 0$. Ainsi $(1, \alpha, \ldots, \alpha^{n-1})$ est une base de $\mathbb{L}$, en tant que $\mathbb{K}$-espace vectoriel . On en déduit que $\mathbb{L}$ est de dimension finie, avec $\dim_{\mathbb{K}}(\mathbb{L}) = n = \deg(P)$.

◇ $\mathbb{L}$ est une extension du corps $\mathbb{K}$, donc tout polynôme de $\mathbb{K}[X]$ est aussi un polynôme de $\mathbb{L}[X]$. En particulier, $P \in \mathbb{L}[X]$.

Posons $P(X) = \sum_{k=0}^{n} p_k X^k$. Alors $\tilde{P}(\alpha) = \tilde{P}(\overline{X}) = \sum_{k=0}^{n} p_k\overline{X}^k = \sum_{k=0}^{n} \overline{p_k}\overline{X}^k = \overline{P(X)} = 0$.

Ainsi α est une racine dans $\mathbb{L}$ de P. On dit que $\mathbb{L}$ est le corps de rupture du polynôme P, dans lequel P est devenu réductible.

◇ En particulier, avec $\mathbb{K} = \mathbb{R}$ et $P(X) = X^2 + 1$, $\mathbb{R}[X]/(X^2 + 1)\mathbb{R}[X]$ est un corps contenant $\mathbb{R}$ dont une base est $(1, \alpha)$ avec $1 + \alpha^2 = 0$. C'est une nouvelle construction de $\mathbb{C}$.

3.2 Identification entre polynômes formels et applications polynomiales

Notation. On fixe un corps $\mathbb{K}$ quelconque.

Propriété. Soit $P \in \mathbb{K}[X]$ et $a_1, \dots, a_k$ k éléments de $\mathbb{K}$ deux à deux distincts.
Alors $a_1, \dots, a_k$ sont toutes racines de P si et seulement si
P est un multiple de $(X - a_1) \times \cdots \times (X - a_k)$.

Démonstration.
Si P est un multiple de $(X - a_1) \times \cdots \times (X - a_k)$, alors pour tout $i \in \{1, \dots, k\}$, P est un multiple de $X - a_i$, donc a_i est une racine de P. Réciproquement, supposons que $a_1, \dots, a_k$ sont toutes racines de P. Soit $i, j \in \{1, \dots, k\}$ tels que $i \neq j$. $a_i - a_j \neq 0$ et $\mathbb{K}$ est un corps, donc $\dfrac{1}{a_i - a_j}((X - a_j) - (X - a_i)) = 1$, ce qui montre que $X - a_i$ et $X - a_j$ sont premiers entre eux. Or pour tout i, a_i est racine de P, donc $X - a_i \mid P$. Alors, d'après une propriété d'arithmétique, $(X - a_1) \times \cdots \times (X - a_k) \mid P$. □

> **Exercice.** Déterminer tous les polynômes P de $\mathbb{R}[X]$ tels que $(X-1) \mid P$ et tels que les restes de la division euclidienne de P par X, $X - 2$ et $X - 3$ sont égaux entre eux.
>
> **Solution :** Notons (C) la condition de l'énoncé.
> $$\begin{aligned}(C) &\iff P(1) = 0 \text{ et } \exists \lambda \in \mathbb{K},\ X, X-2, \text{et } X-3 \text{ divisent } P - \lambda \\ &\iff (P(1) = 0) \wedge (\exists \lambda \in \mathbb{K},\ X(X-2)(X-3) \mid P - \lambda \\ &\iff \exists T \in \mathbb{K}[X],\ \exists \lambda \in \mathbb{K},\ (P = X(X-2)(X-3)T + \lambda) \wedge (0 = 2T(1) + \lambda) \\ &\iff \exists T \in \mathbb{K}[X],\ P = X(X-2)(X-3)T - 2T(1)\end{aligned}$$

Corollaire. Un polynôme non nul admet au plus $\deg(P)$ racines.

Démonstration.
Soit $P \in \mathbb{K}[X]$ un polynôme non nul admettant k racines deux à deux distinctes, notée $a_1, \dots, a_k$. Alors il existe $Q \in \mathbb{K}[X]$ tel que $P = Q(X) \prod_{i=1}^{k} (X - a_i)$. Or $Q \neq 0$, car $P \neq 0$, donc $\deg(P) \geq \deg\Big(\prod_{i=1}^{k} (X - a_i)\Big) = k$. □

Corollaire. Si $P \in \mathbb{K}[X]$ possède une infinité de racines, alors $P = 0$.

> **Exercice.** Soit $\mathbb{K}$ un corps de caractéristique nulle.
> On convient qu'un polynôme de $\mathbb{K}[X]$ est périodique si et seulement si il existe $c \in \mathbb{K} \setminus \{0\}$ tel que $P(X + c) = P(X)$.
> Déterminer tous les polynômes périodiques de $\mathbb{K}[X]$.
>
> **Solution :** Soit $P \in \mathbb{K}[X]$ un polynôme que l'on suppose périodique : il existe $c \in \mathbb{K} \setminus \{0\}$ tel que $P(X + c) = P(X)$.
> On montre alors par récurrence que, pour tout $n \in \mathbb{N}$, $\tilde{P}(nc) = \tilde{P}(0)$, donc le polynôme $P(X) - \tilde{P}(0)$ admet pour racines les nc où $n \in \mathbb{N}^*$. Or si $nc = mc$

(avec $n, m \in \mathbb{N}$), alors $((n-m).1_{\mathbb{K}})c = 0$, or $c \neq 0$, donc $(n-m).1_{\mathbb{K}} = 0$, mais $\text{car}(\mathbb{K}) = 0$, donc $n = m$. Ainsi, $P(X) - \tilde{P}(0)$ admet une infinité de racines, donc il est nul et $P(X) = \tilde{P}(0)$.
Réciproquement, il est clair que tout polynôme constant est périodique. Ce sont donc les seuls.

Principe de rigidité des polynômes. Soit $n \in \mathbb{N}$ et $P, Q \in \mathbb{K}_n[X]$.
Si $\{x \in \mathbb{K} \ / \ \tilde{P}(x) = \tilde{Q}(x)\}$ contient au moins $n+1$ scalaires, alors $P = Q$.

Théorème. On peut identifier l'ensemble $\mathbb{K}[X]$ des polynômes formels avec l'ensemble $\mathcal{P}_{\mathbb{K}}$ des applications polynomiales de $\mathbb{K}$ dans $\mathbb{K}$ si et seulement si $\mathbb{K}$ est de cardinal infini.

Démonstration.
Rappelons que $\varphi : \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathcal{P}_{\mathbb{K}} \\ P & \longmapsto & \tilde{P} \end{array}$ est un morphisme surjectif d'anneaux. On peut identifier ces deux ensembles, en confondant P et $\tilde{P}$ si et seulement si φ est injectif, donc si et seulement si $\{0\} = Ker(\varphi) = \{P \in \mathbb{K}[X] \ / \ \tilde{P} = 0\}$.
Or si $\mathbb{K}$ est de cardinal fini, alors $P = \prod_{a \in \mathbb{K}} (X - a)$ est un polynôme non nul (car de degré différent de $-\infty$) tel que $\tilde{P} = 0$ (i.e : pour tout $b \in \mathbb{K}$, $\tilde{P}(b) = 0$), donc dans ce cas, φ n'est pas un isomorphisme et l'identification n'est pas possible.
Réciproquement, supposons que $\mathbb{K}$ est de cardinal infini. Soit $P \in Ker(\varphi)$. Alors pour tout $x \in \mathbb{K}$, $\tilde{P}(x) = 0$. Donc P possède une infinité de racines, ce qui impose $P = 0$. Alors φ est un isomorphisme d'anneaux. □

Remarque. Supposons que $\mathbb{K}$ est fini, de cardinal q.
Posons $P = \prod_{a \in \mathbb{K}} (X - a)$ et $Q = X^q - X$.
Pour tout $a \in \mathbb{K} \setminus \{0\}$, l'ordre de a dans le groupe multiplicatif $\mathbb{K} \setminus \{0\}$ divise $|\mathbb{K} \setminus \{0\}| = q - 1$, donc $a^{q-1} = 1$. Ainsi, pour tout $a \in \mathbb{K}$, $a^q = a$.
On en déduit que le polynôme $P - Q$ admet au moins q racines (tous les éléments de $\mathbb{K}$), or $\deg(P - Q) < q$, donc $P = Q$.

Remarque. En pratique, lorsque $\mathbb{K}$ est de cardinal infini, on ne distingue pas P et $\tilde{P}$. Ainsi, pour tout $a \in \mathbb{K}$, on notera $P(a)$ au lieu de $\tilde{P}(a)$.

3.3 Polynôme d'interpolation de Lagrange

Notation. Dans tout ce paragraphe, on fixe un corps quelconque $\mathbb{K}$, $n \in \mathbb{N}$ et une famille $a_0, \ldots, a_n \in \mathbb{K}$ de $n+1$ scalaires deux à deux distincts.
Pour tout $i \in \{0, \ldots, n\}$, posons $L_i = \prod_{\substack{0 \leq j \leq n \\ j \neq i}} \frac{X - a_j}{a_i - a_j}$.

Les L_i sont appelés les polynômes de Lagrange associés à $(a_0, \ldots, a_n)$.

Propriété. Pour tout $i, k \in \{0, \ldots, n\}$, $\widetilde{L_i}(a_k) = \delta_{i,k}$.

Démonstration.
Soit $i, k \in \{0, \dots, n\}$.
Si $k = i$, $\widetilde{L_i}(a_i) = \prod_{\substack{0 \leq j \leq n \\ j \neq i}} \frac{a_i - a_j}{a_i - a_j} = 1$.
Si $k \neq i$, alors $\frac{X - a_k}{a_i - a_k}$ est l'un des facteurs de L_i, donc $\widetilde{L_i}(a_k) = 0$. □

Propriété. Pour tout $P \in \mathbb{K}_n[X]$, $P = \sum_{i=0}^{n} \tilde{P}(a_i) L_i$.

Démonstration.
Posons $Q = \sum_{i=0}^{n} \tilde{P}(a_i) L_i$. D'après la propriété précédente, pour tout $k \in \{0, \dots, n\}$, $\tilde{Q}(a_k) = \sum_{i=0}^{n} \tilde{P}(a_i)\delta_{i,k} = \tilde{P}(a_k)$, or $P, Q \in \mathbb{K}_n[X]$, donc $P = Q$. □

Théorème. Soit $(b_0, b_1, \dots, b_n) \in \mathbb{K}^{n+1}$ une famille quelconque de scalaires.
Il existe un unique polynôme P_0 de degré inférieur ou égal à n tel que, pour tout $i \in \{0, \dots, n\}$, $\widetilde{P_0}(a_i) = b_i$. P_0 est appelé le polynôme d'interpolation de Lagrange (associé aux deux familles $(a_0, a_1, \dots, a_n)$ et $(b_0, b_1, \dots, b_n)$). On dispose de la formule suivante :

$$P_0 = \sum_{i=0}^{n} \left(b_i \prod_{\substack{0 \leq j \leq n \\ j \neq i}} \frac{X - a_j}{a_i - a_j} \right).$$

Enfin, l'ensemble des polynômes P vérifiant, pour tout $i \in \{0, \dots, n\}$, $\tilde{P}(a_i) = b_i$, est égal à $P_0 + (\prod_{i=0}^{n}(X - a_i))\mathbb{K}[X]$.

Remarque. Lorsque $\mathbb{K} = \mathbb{R}$, si f est une application de I dans $\mathbb{R}$, où I est un intervalle contenant $a_0, \dots, a_n$, il existe donc un unique polynôme P_0 de degré inférieur ou égal à n, dont le graphe coupe celui de f en les points d'abscisses $a_0, \dots, a_n$: Le polynôme P_0 interpole la fonction f en ces points. De plus, $P_0 = \sum_{i=0}^{n} f(a_i) L_i$.

Démonstration.
Posons $P_0(X) = \sum_{i=0}^{n} b_i L_i$. Pour tout $k \in \{0, \dots, n\}$, $\tilde{P_0}(a_k) = \sum_{i=0}^{n} b_i \delta_{i,k} = b_k$ et $\deg(P_0) \leq n$, ce qui prouve déjà l'existence.
Soit $P \in \mathbb{K}[X]$,
$(\forall i \in \{0, \dots, n\} \ \tilde{P}(a_i) = b_i) \iff \forall i \in \{0, \dots, n\} \ \widetilde{P - P_0}(a_i) = 0$
$\iff \forall i \in \{0, \dots, n\} \ (X - a_i) | (P - P_0)$.
Or $a_0, \dots, a_n$ sont deux à deux distincts, donc les polynômes $X - a_0, \dots, X - a_n$ sont deux à deux premiers entre eux. Ainsi,

$(\forall i \in \{0,\dots,n\}\ \tilde{P}(a_i) = b_i) \iff \left(\prod_{i=0}^{n}(X-a_i)\right) | (P - P_0)$.
Ceci prouve que l'ensemble des polynômes P vérifiant, pour tout $i \in \{0,\dots,n\}$, $\tilde{P}(a_i) = b_i$, est égal à $P_0 + (\prod_{i=0}^{n}(X-a_i))\mathbb{K}[X]$.

Lorsque $Q \in \mathbb{K}[X] \setminus \{0\}$, $P_0 + Q\prod_{i=0}^{n}(X-a_i)$ est de degré supérieur à $n+1$, donc P_0 est l'unique polynôme de degré inférieur ou égal à n tel que, pour tout $i \in \{0,\dots,n\}$, $\widetilde{P_0}(a_i) = b_i$. □

Propriété. $\mathcal{L} = (L_0,\dots,L_n)$ est une base de $\mathbb{K}_n[X]$, appelée base de Lagrange.
Pour tout $P \in \mathbb{K}_n[X]$, les coordonnées de P dans $\mathcal{L}$ sont les valeurs de P en $a_0,\dots,a_n$.

Propriété. L'application $u : \mathbb{K}[X] \longrightarrow \mathbb{K}^{n+1}$ définie par $u(P) = (\tilde{P}(a_0),\dots,\tilde{P}(a_n))$ est une application linéaire dont le noyau vérifie : $\mathrm{Ker}(u)$ est l'idéal engendré par $\prod_{i=0}^{n}(X-a_i)$.

3.4 Polynôme dérivé

Notation.
Dans ce paragraphe, on suppose que $\mathbb{K}$ est un corps de caractéristique nulle.
En particulier, $\mathbb{K}$ est de cardinal infini, donc on identifiera P et $\tilde{P}$ pour tout $P \in \mathbb{K}[X]$.

Propriété. Pour tout $P \in \mathbb{K}[X]$ tel que $\deg(P) \geq 1$, $\deg(P') = \deg(P) - 1$.
Lorsque $\deg(P) \leq 0$, $\deg(P') = -\infty$.

Démonstration.
On sait déjà que, pour tout $a \in \mathbb{K}$, $a' = 0$, donc, lorsque $\deg(P) \leq 0$, $\deg(P') = -\infty$.
Supposons maintenant que $\deg(P) \geq 1$. Alors, en notant $n = \deg(P)$, P est de la forme $P(X) = a_nX^n + \cdots + a_1X + a_0$ avec $a_n \neq 0$. Alors $P'(X) = na_nX^{n-1} + \cdots + a_1$, or $na_n = (n.1_{\mathbb{K}}) \times a_n \neq 0$, car $n.1_{\mathbb{K}} \neq 0$, $a_n \neq 0$ et $\mathbb{K}$ est intègre.
Ainsi, $\deg(P') = n - 1 = \deg(P) - 1$. □

Corollaire. Soit $P \in \mathbb{K}[X]$.
Alors P est un polynôme constant (i.e : un élément de $\mathbb{K}$) si et seulement si $P' = 0$.

Démonstration.
Si P est constant, alors on sait que $P' = 0$.
Si P n'est pas constant, alors $\deg(P') = \deg(P) - 1 \geq 0$, donc $P' \neq 0$. □

Remarque. Dans $\mathbb{F}_p[X]$, $(X^p)' = 0$.

Corollaire. Pour tout $P \in \mathbb{K}[X]$, si $\deg(P) \geq n$, alors $\deg(P^{(n)}) = \deg(P) - n$
et si $\deg(P) < n$, alors $P^{(n)} = 0$.

Formule de Taylor : Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors
$P = \sum_{n\in\mathbb{N}} \frac{(X-a)^n}{n!.1_\mathbb{K}} P^{(n)}(a)$, i.e $P(X+a) = \sum_{n\in\mathbb{N}} \frac{X^n}{n!.1_\mathbb{K}} P^{(n)}(a)$.

Remarque. $\mathrm{car}(\mathbb{K}) = 0$, donc pour tout $n \in \mathbb{N}$, $n!.1_\mathbb{K} \neq 0$.

Démonstration.
Soit $a \in \mathbb{K}$. Posons $P(X+a) = \sum_{n\in\mathbb{N}} a_n X^n$.
Soit $k \in \mathbb{N}$. Dérivons k fois cette égalité : d'après la formule de dérivation d'une composée de polynômes, $P^{(k)}(X+a) = \sum_{n\geq k} a_n n(n-1)\cdots(n-k+1)X^{n-k}$, donc en substituant X par 0, on obtient : $P^{(k)}(a) = a_k k!$,
ce qui démontre que $P(X+a) = \sum_{n\in\mathbb{N}} \frac{X^n}{n!.1_\mathbb{K}} P^{(n)}(a)$. □

Propriété. Pour tout $P \in \mathbb{K}[X]$, le coefficient de degré n de P est égal à $\frac{P^{(n)}(0)}{n!}$.

Corollaire. Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $k \in \mathbb{N}$. Alors
le reste de la division euclidienne de P par $(X-a)^k$ est égal à $\sum_{h=0}^{k-1} \frac{(X-a)^h}{h!.1_\mathbb{K}} P^{(h)}(a)$.

Démonstration.
$P = \sum_{h=0}^{k-1} \frac{(X-a)^h}{h!.1_\mathbb{K}} P^{(h)}(a) + (X-a)^k \sum_{n\geq k} \frac{(X-a)^{(n-k)}}{n!.1_\mathbb{K}} P^{(n)}(a)$
et $\deg\Big(\sum_{h=0}^{k-1} \frac{(X-a)^h}{h!.1_\mathbb{K}} P^{(h)}(a)\Big) < \deg((X-a)^k)$. □

3.5 Racines multiples

Notation. $\mathbb{K}$ désigne un corps quelconque.

Définition. Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}$.
a est une racine de P de multiplicité m si et seulement si il existe $Q \in \mathbb{K}[X]$ tel que $P(X) = (X-a)^m Q(X)$ avec $\tilde{Q}(a) \neq 0$.

Remarque. Si a est racine de P de multiplicité m, alors $P \neq 0$.

Remarque. a n'est pas racine de P si et seulement si a est racine de P de multiplicité nulle.

Définition. Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}$.
a est racine de P de multiplicité au moins m si et seulement si $(X-a)^m \mid P$.
Ainsi, a est racine de P de multiplicité m si et seulement si elle est racine de P de multiplicité au moins m, mais n'est pas racine de P de multiplicité au moins $m+1$.

Remarque. Lorsque $P \neq 0$, la multiplicité de a en tant que racine de P est l'exposant du polynôme irréductible $X - a$ dans la décomposition primaire de P.

Remarque. a est racine de $P \in \mathbb{K}[X]$ si et seulement si a est racine de P de multiplicité au moins 1.

Remarque. Pour tout $a \in \mathbb{K}$ et $m \in \mathbb{N}$, a est racine de 0 de multiplicité au moins m.

Définition. On dit que $a \in \mathbb{K}$ est une racine simple (resp : double, triple) de $P \in \mathbb{K}[X]$ si et seulement si a est une racine de P de multiplicité 1 (resp : 2, 3).

Définition. Soit $P \in \mathbb{K}[X] \setminus \{0\}$. Posons $\{a_1, \dots, a_k\} = \{x \in \mathbb{K} / \tilde{P}(x) = 0\}$. Pour tout $h \in \mathbb{N}_k$, notons m_h la multiplicité de a_h pour le polynôme P. On dit alors que le nombre de racines de P, **comptées avec multiplicité**, est égal à $\sum_{h=1}^{k} m_h$.
Et k est le nombre de racines de P comptées sans multiplicité.

Propriété. Soit $P \in \mathbb{K}[X]$, $a_1, \dots, a_k \in \mathbb{K}$ et $m_1, \dots, m_k \in \mathbb{N}$.
Pour tout $h \in \{1, \dots, k\}$, a_h est racine de P de multiplicité au moins m_h si et seulement si P est un multiple de $\prod_{h=1}^{k} (X - a_h)^{m_h}$.

Propriété. Soit $P \in \mathbb{K}[X]$ un polynôme non nul. Le nombre de racines de P, comptées avec multiplicité est inférieur ou égal au degré de P.

Hypothèse : Pour la suite de ce paragraphe, on suppose que $\mathbb{K}$ est un corps de caractéristique nulle.

Théorème. Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}$.
a est racine de P de multiplicité au moins m si et seulement si
$\forall i \in \{0, \dots, m-1\}$, $P^{(i)}(a) = 0$.

Démonstration.
$\text{car}(\mathbb{K}) = 0$, donc on peut utiliser la formule de Taylor. On sait alors que le reste de la division euclidienne de P par $(X-a)^m$ est égal à $\sum_{h=0}^{m-1} \frac{(X-a)^h}{h!.1_{\mathbb{K}}} P^{(h)}(a)$.
Dans ces conditions, a est racine de P de multiplicité au moins m si et seulement si $(X-a)^m$ divise P, donc si et seulement si le reste de la division euclidienne de P par $(X-a)^m$ est nul, donc si et seulement si $\sum_{h=0}^{m-1} \frac{(X-a)^h}{h!.1_{\mathbb{K}}} P^{(h)}(a) = 0$. Or, en composant par le polynôme $X + a$ ou $X - a$, cette dernière condition est équivalente à $\sum_{h=0}^{m-1} \frac{X^h}{h!.1_{\mathbb{K}}} P^{(h)}(a) = 0$, donc à la condition $\forall i \in \{0, \dots, m-1\}$, $P^{(i)}(a) = 0$. □

Corollaire. Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}$.
a est racine de P de multiplicité m si et seulement si
$\forall i \in \{0, \dots, m-1\}$, $P^{(i)}(a) = 0$ et $P^{(m)}(a) \neq 0$.

Corollaire. Si $a \in \mathbb{K}$ est racine de $P \in \mathbb{K}[X]$ de multiplicité $m \in \mathbb{N}^*$, alors a est racine de P' de multiplicité $m-1$.

Exemple. Décomposer $A = X^4 - 2X^3 + 2X^2 - 2X + 1$ en produit de polynômes irréductibles dans $\mathbb{R}[X]$.
On remarque que $A(1) = 0$. $A' = 4X^3 - 6X^2 + 4X - 2$ et $A'(1) = 0$. $A'' = 12X^2 - 12X + 4$ et $A''(1) \neq 0$, donc 1 est une racine double de A. Il existe donc B tel que $A = (X-1)^2 B$. B est de degré 2, de coefficient dominant 1 et de coefficient constant 1, donc il existe $a \in \mathbb{R}$ tel que $A = (X^2 - 2X + 1)(X^2 + aX + 1)$. En calculant le coefficient de degré 3, on obtient $-2 = a - 2$, donc $a = 0$ et $A = (X-1)^2(X^2+1)$.

Exercice. Dans $\mathbb{R}[X]$, on pose $P(X) = (X+1)^7 - X^7 - \lambda$, où $\lambda \in \mathbb{R}$.
Déterminer λ pour que P possède au moins une racine multiple réelle.

Solution : Soit $x \in \mathbb{R}$. x est une racine multiple de P si et seulement si

$$\begin{aligned} P(x) = P'(x) = 0 &\iff \begin{cases} (x+1)^7 - x^7 - \lambda = 0 \\ 7(x+1)^6 - 7x^6 = 0 \end{cases} \\ &\iff \begin{cases} (x+1)^6 = x^6 \\ 0 = (x+1)^7 - x^7 - \lambda = (x+1)x^6 - x^7 - \lambda \end{cases} \\ &\iff \begin{cases} x^6 = \lambda \\ (x+1)^6 = x^6 \end{cases} \end{aligned}$$

$x = 0$ n'est pas solution, donc on peut supposer que $x \in \mathbb{R}^*$. Ainsi,
$P(x) = P'(x) = 0 \iff \begin{cases} x^6 = \lambda \\ \left(\dfrac{x+1}{x}\right)^6 = 1 \end{cases}$. Or, dans $\mathbb{R}$,
$\left(\dfrac{x+1}{x}\right)^6 = 1 \iff \dfrac{x+1}{x} = \pm 1 \iff x = -\dfrac{1}{2}$. On en déduit que P possède au moins une racine multiple réelle si et seulement si $\lambda = \dfrac{1}{2^6}$ et que dans ce cas, il y a une unique racine multiple, égale à $-\frac{1}{2}$.

3.6 Polynômes scindés

Notation. $\mathbb{K}$ désigne à nouveau un corps quelconque.

Définition. $P \in \mathbb{K}[X] \setminus \{0\}$ est scindé dans $\mathbb{K}[X]$ si et seulement si il est constant ou bien si c'est un produit de polynômes de degré 1 de $\mathbb{K}[X]$, c'est-à-dire si et seulement si sa décomposition en polynômes irréductibles dans $\mathbb{K}[X]$ ne fait intervenir que des polynômes de degré 1.

Propriété. Soit $P \in \mathbb{K}[X] \setminus \{0\}$. P est scindé dans $\mathbb{K}[X]$ si et seulement si le nombre de racines de P dans $\mathbb{K}$, comptées avec multiplicité, est égal au degré de P.

Démonstration.
Supposons que P est scindé. Alors, il existe $\mu \in \mathbb{K}^*$, $a_1, \dots, a_k \in \mathbb{K}$ et $m_1, \dots, m_k \in \mathbb{N}^*$ tels que $i \neq j \implies a_j \neq a_i$ et $P = \mu \prod_{h=1}^{k} (X - a_h)^{m_h}$. Alors, le nombre de racines de P,

comptées avec multiplicité, est égal à $\sum_{h=1}^{k} m_h = \deg(P)$.
Réciproquement, supposons que le nombre de racines de P dans $\mathbb{K}$, comptées avec multiplicité, est égal au degré de P. Alors d'après une propriété précédente, il existe $Q \in \mathbb{K}[X]$ tel que $P = Q \times \prod_{h=1}^{k}(X - a_h)^{m_h}$, en notant $a_1, \dots, a_k$ les différentes racines de P et $m_1, \dots, m_k$ leurs multiplicités respectives.
Ainsi, $\deg(P) = \deg(Q) + \sum_{h=1}^{k} m_h = \deg(Q) + \deg(P)$, donc $\deg(Q) = 0$ et Q est une constante non nulle. □

Définition. Soit $P \in \mathbb{K}[X] \setminus \{0\}$. On dit que P est simplement scindé dans $\mathbb{K}[X]$ si et seulement si P est scindé dans $\mathbb{K}$ et si toutes ses racines sont simples.

Remarque. On a vu en analyse, grâce au lemme de Rolle, que si P est simplement scindé dans $\mathbb{R}[X]$, avec $\deg(P) \geq 1$, alors P' est aussi simplement scindé..
De plus, on a vu en TD que, si P est scindé dans $\mathbb{R}[X]$, c'est encore le cas pour P'.

Relations de Viète entre coefficients et racines : Soit $P \in \mathbb{K}[X]$ un polynôme **scindé** dans $\mathbb{K}[X]$ de degré n, avec $n \geq 1$. Alors P peut s'écrire sous les deux formes suivantes :
- $P(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$, avec $a_0, \dots, a_n \in \mathbb{K}$ et $a_n \neq 0$;
- $P(X) = a_n(X - \beta_1) \times \cdots \times (X - \beta_n)$, où $\beta_1, \dots, \beta_n$ est la liste des racines de P, comptées avec multiplicité.

Alors, pour tout $p \in \{1, \dots, n\}$,

$$\sigma_p = (-1)^p \frac{a_{n-p}}{a_n}, \text{ où } \sigma_p = \sum_{1 \leq i_1 < \cdots < i_p \leq n} \beta_{i_1} \times \cdots \times \beta_{i_p}.$$

Les σ_p s'appellent les fonctions symétriques élémentaires des racines. En particulier,
- Pour $p = 1$, $\sum_{i=1}^{n} \beta_i = -\frac{a_{n-1}}{a_n}$. Il s'agit de la somme des racines de P, comptées avec multiplicités.
- Pour $p = n$, $\prod_{i=1}^{n} \beta_i = (-1)^n \frac{a_0}{a_n}$. Il s'agit du produit des racines de P, comptées avec multiplicités.

Démonstration.
Il suffit de développer le produit $P(X) = a_n(X - \beta_1) \times \cdots \times (X - \beta_n)$. Pour cela, dans chaque facteur $X - \beta_i$, on choisit le terme X ou bien le terme $-\beta_i$.
On code ces choix par une fonction $f : \{1, \dots, n\} \longrightarrow \{0, 1\}$, en convenant que le terme X est choisi dans le facteur $X - \beta_i$ si et seulement si $f(i) = 1$.

Ainsi, $P(X) = a_n \sum_{f \in \mathcal{F}(\{1,\dots,n\},\{0,1\})} \prod_{i=1}^{n} (X\delta_{f(i),1} - \beta_i \delta_{f(i),0})$.

Formellement, cette formule peut se démontrer par récurrence sur n.
Par sommation par paquets, on partitionne cette somme selon le cardinal de $\{i \in \{1,\dots,n\} \ / \ f(i)=1\}$. Ainsi,

$$\begin{aligned}
P(X) &= a_n \sum_{k=0}^{n} \sum_{\substack{f\in\mathcal{F}(\{1,\dots,n\},\{0,1\}) \\ |\{i\in\{1,\dots,n\} \ / \ f(i)=1\}|=k}} \prod_{i=1}^{n} (X\delta_{f(i),1} - \beta_i \delta_{f(i),0}) \\
&= a_n \sum_{k=0}^{n} \sum_{\substack{f\in\mathcal{F}(\{1,\dots,n\},\{0,1\}) \\ |\{i\in\{1,\dots,n\} \ / \ f(i)=1\}|=k}} X^k \prod_{\substack{1\le i\le n \\ f(i)=0}} (-\beta_i) \\
&= a_n \sum_{k=0}^{n} X^k \sum_{f\in\mathcal{F}_k} \prod_{j\in\varphi^{-1}(f)} (-\beta_j) \\
&= a_n \sum_{k=0}^{n} X^k \sum_{1\le i_1<\dots<i_{n-k}\le n} \prod_{j=1}^{n-k} (-\beta_{i_j}),
\end{aligned}$$

par changement de variable, en utilisant la bijection φ, pour k fixé dans $\{0,\dots,n\}$, de $\mathcal{P}_{n-k} = \{(i_1,\dots,i_{n-k}) \in \{1,\dots,n\}^{n-k} \ / \ 1 \le i_1 < \dots < i_{n-k} \le n\}$
dans $\mathcal{F}_k = \{f \in \mathcal{F}(\{1,\dots,n\},\{0,1\}) \ / \ |\{i \in \{1,\dots,n\} \ / \ f(i)=1\}| = k\}$ définie par $\varphi((i_1,\dots,i_{n-k}))(x) = \begin{cases} 0 \text{ si } \exists j \in \{1,\dots,n-k\}, \ x = i_j \\ 1 \text{ sinon} \end{cases}$. C'est bien une bijection, car on peut montrer que son application réciproque est donnée par : pour tout $f \in \mathcal{F}_k$, $\varphi^{-1}(f)$ est la liste ordonnée des éléments de $f^{-1}(\{0\})$.

On en déduit que $P(X) = a_n \sum_{p=0}^{n} (-1)^p X^{n-p} \sum_{1\le i_1<\dots<i_p\le n} \prod_{j=1}^{p} \beta_{i_j}$,
or $P(X) = a_n X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0$, donc on conclut en égalant les coefficients de ces deux écritures de $P(X)$. □

Remarque. La formule donnant le produit des racines s'obtient immédiatement en calculant $\tilde{P}(0)$: $P(X) = a_n X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0$, donc $\tilde{P}(0) = a_0$, et $P(X) = a_n(X-\beta_1)\times\dots\times(X-\beta_n)$, donc $\tilde{P}(0) = a_n(-\beta_1)\times\dots\times(-\beta_n)$.

Exemple. Dans $\mathbb{C}[X]$, avec $P(X) = X^n - 1 = \prod_{k=0}^{n-1}(X-\omega^k)$, où $\omega = e^{\frac{2i\pi}{n}}$, on retrouve le fait que $\sum_{k=0}^{n-1} \omega^k = 0$.

On obtient de plus que $\prod_{k=0}^{n-1} \omega^k = (-1)^{n+1}$, ce que l'on peut retrouver par le calcul.

Exercice. Soit $P(X) = X^3 + aX^2 + bX + c \in \mathbb{K}[X]$ un polynôme scindé dans $\mathbb{K}[X]$, dont les racines, comptées avec multiplicité sont notées x_1, x_2 et x_3.
Calculer $S_n = x_1^n + x_2^n + x_3^n$ en fonction de a, b, c lorsque $n \in \{0,1,2,3\}$, puis exprimer S_n en fonction de $S_{n-1}, S_{n-2}, S_{n-3}$ lorsque $n \ge 3$.
Calculer S_{-1}.

Solution : ◇ $S_0 = 3$, $S_1 = -a$, $S_2 = (x_1+x_2+x_3)^2 - 2\sigma_2 = a^2 - 2b$.
◇ D'après la formule du multinôme,
$$\begin{aligned}\sigma_1^3 &= S_3 + 3(x_1^2x_2 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_2 + x_3^2x_1) + 6x_1x_2x_3\\ &= S_3 + 3[(x_1+x_2+x_3)(x_1x_2+x_1x_3+x_2x_3) - 3x_1x_2x_3] + 6x_1x_2x_3\\ &= S_3 + 3\sigma_1\sigma_2 - 3\sigma_3,\end{aligned}$$
donc $S_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$, puis $S_3 = -a^3 + 3ab - 3c$.
◇ Soit $n \geq 3$: $\begin{cases} x_1^n = x_1^3x_1^{n-3} &= (-ax_1^2 - bx_1 - c)x_1^{n-3}\\ x_2^n = x_2^3x_2^{n-3} &= (-ax_2^2 - bx_2 - c)x_2^{n-3}\\ x_3^n = x_3^3x_3^{n-3} &= (-ax_3^2 - bx_3 - c)x_3^{n-3}\end{cases}$, donc en sommant ces relations, $S_n = -aS_{n-1} - bS_{n-2} - cS_{n-3}$.
Remarque : on retrouve ainsi S_3.
◇ S_{-1} est défini si et seulement si 0 n'est pas racine de P, donc si et seulement si $c \neq 0$. Dans ce cas, $S_{-1} = \dfrac{1}{x_1} + \dfrac{1}{x_2} + \dfrac{1}{x_3} = \dfrac{\sigma_2}{\sigma_3} = -\dfrac{b}{c}$.

Exercice. Soit $P(X) = X^3 + aX^2 + bX + c \in \mathbb{K}[X]$ un polynôme scindé dans $\mathbb{K}[X]$, dont les racines, comptées avec multiplicité sont notées x_1, x_2 et x_3.
Calculer $S = \dfrac{1}{x_1+1} + \dfrac{1}{x_2+1} + \dfrac{1}{x_3+1}$ en fonction de a, b, c.
Solution : On pourrait réduire au même dénominateur, puis développer, mais c'est un calcul fastidieux. Autre méthode : Posons $Q(X) = P(X-1)$:
les racines de Q sont $y_1 = x_1 + 1$, $y_2 = x_2 + 1$ et $y_3 = x_3 + 1$, or
$$\begin{aligned}Q(X) &= (X-1)^3 + a(X-1)^2 + b(X-1) + c\\ &= X^3 + X^2(-3+a) + X(3-2a+b) - 1 + a - b + c,\end{aligned}$$
donc d'après la fin de l'exercice précédent, S est défini si et seulement si $-1 + a - b + c \neq 0$, et dans ce cas, $S = -\dfrac{3-2a+b}{a-b+c-1}$.

Exercice. On pose $P(X) = X^{11} - X + 1 \in \mathbb{C}[X]$ et on note $(x_i)_{1\leq i\leq 11}$ une liste des racines de P, comptées avec multiplicité. Calculer $S = \displaystyle\sum_{i=1}^{11} \frac{x_i}{x_i+2}$.

Solution : $S = \displaystyle\sum_{i=1}^{11} \frac{x_i+2-2}{x_i+2} = 11 - 2\sum_{i=1}^{11} \frac{1}{y_i}$, où $y_1, \ldots, y_{11}$ sont les racines de $Q(X) = P(X-2) = (X-2)^{11} - (X-2) + 1 = \displaystyle\sum_{i=0}^{11} q_iX^i$.
Ainsi, $S = 11 - 2\dfrac{\sigma_{n-1}}{\sigma_n}$, où σ_j représente la j-ième fonction symétrique élémentaire des racines de Q. On en déduit que $S = 11 + 2\dfrac{q_1}{q_0}$, avec $q_0 = Q(0) = -2^{11} + 3$ et $q_1 = 2^{10}\begin{pmatrix}11\\1\end{pmatrix} - 1 = 11 \times 2^{10} - 1$.
Ainsi, $S = 11 + \dfrac{11\times 2^{11} - 2}{3 - 2^{11}} = \dfrac{31}{3-2^{11}}$.

La suite est hors programme.

Définition. Soit $n \in \mathbb{N}^*$ et $A \in \mathbb{K}[X_1, \dots, X_n]$ un polynôme à n indéterminées.
On dit que A est symétrique si et seulement si, pour tout $\sigma \in \mathcal{S}_n$,

$$A(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = A(X_1, \dots, X_n).$$

Exemples.

— Les polynômes de Newton : $X_1^p + \cdots + X_n^p$, où $n, p \in \mathbb{N}^*$. Ils sont symétriques.

— Les polynômes symétriques élémentaires : pour tout $p \in \{1, \dots, n\}$,
$\Sigma_p(X_1, \dots, X_n) = \sum_{1 \leq i_1 < i_2 < \cdots < i_p \leq n} X_{i_1} \times \cdots \times X_{i_p}$ est bien un polynôme symétrique.
En effet, on peut écrire $\Sigma_p(X_1, \dots, X_n) = \sum_{\substack{A \subset \{1,\dots,n\} \\ |A|=p}} \prod_{a \in A} X_a$.
Soit $\sigma \in \mathcal{S}_n$. Alors $\Sigma_p(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = \sum_{\substack{A \subset \{1,\dots,n\} \\ |A|=p}} \prod_{a \in A} X_{\sigma(a)} = \sum_{\substack{A \subset \{1,\dots,n\} \\ |A|=p}} \prod_{b \in \sigma(A)} X_b$,
car σ est une bijection de A dans $\sigma(A)$.
Notons $P_p = \{A \subset \{1, \dots, n\} \ / \ |A| = p\}$ et $\begin{array}{rccc} \varphi_\sigma : & P_p & \longrightarrow & P_p \\ & A & \longmapsto & \sigma(A) \end{array}$. φ_σ est une bijection dont la bijection réciproque est $\varphi_{\sigma^{-1}}$, donc par changement de variables,
$\Sigma_p(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = \sum_{A \in P_p} \prod_{b \in \varphi_\sigma(A)} X_b = \sum_{B \in P_p} \prod_{b \in B} X_b = \Sigma_p(X_1, \dots, X_n)$.

Propriété. (Admise) Soit $n \in \mathbb{N}^*$. On suppose que $\mathbb{L}$ est un sous-corps de $\mathbb{K}$ et que A est un polynôme symétrique de $\mathbb{L}[X_1, \dots, X_n]$.
Alors il existe $B \in \mathbb{L}[X_1, \dots, X_n]$ tel que $A = B(\Sigma_1, \dots, \Sigma_n)$.

Corollaire. On reprend les notations de la propriété précédente. On suppose de plus que $P \in \mathbb{L}[X]$ est un polynôme scindé dans $\mathbb{K}[X]$, dont les racines dans $\mathbb{K}$, comptées avec multiplicité, sont notées $\beta_1, \dots, \beta_n$. Alors $A(\beta_1, \dots, \beta_n) \in \mathbb{L}$.

Démonstration.
D'après la propriété, $A(\beta_1, \dots, \beta_n) = B(\Sigma_1(\beta_1, \dots, \beta_n), \dots, \Sigma_n(\beta_1, \dots, \beta_n))$, donc d'après les relations de Viète, $A(\beta_1, \dots, \beta_n) = B\Big((-1)^p \frac{a_{n-p}}{a_n}\Big)_{1 \leq p \leq n}$, où a_i désigne le coefficient de P de degré i. Or P et B sont à coefficients dans $\mathbb{L}$, donc $A(\beta_1, \dots, \beta_n) \in \mathbb{L}$. □

Exemple. Avec $\mathbb{L} = \mathbb{Q}$ et $\mathbb{K} = \mathbb{C}$: Soit $P \in \mathbb{Q}[X]$ un polynôme de degré n. Il est scindé sur $\mathbb{C}[X]$ (cf plus loin), donc en notant $\beta_1, \dots, \beta_n$ ses racines complexes, comptées avec multiplicité, pour tout $p \in \mathbb{N}^*$, $\beta_1^p + \cdots + \beta_n^p \in \mathbb{Q}$.

3.7 Polynômes de $\mathbb{R}[X]$ et de $\mathbb{C}[X]$

Définition. Si $P = \sum_{k \in \mathbb{N}} a_k X^k \in \mathbb{C}[X]$, on note $\overline{P} = \sum_{k \in \mathbb{N}} \overline{a_k} X^k$.

Propriété. L'application $\begin{array}{rccc} & \mathbb{C}[X] & \longrightarrow & \mathbb{C}[X] \\ & P & \longmapsto & \overline{P} \end{array}$ est un isomorphisme d'anneaux.

Démonstration.
Notons f cette application.
$f(1) = \overline{1} = 1$.
Soit $P = \sum_{k\in\mathbb{N}} a_k X^k \in \mathbb{C}[X]$ et $Q = \sum_{k\in\mathbb{N}} b_k X^k \in \mathbb{C}[X]$:
$f(P+Q) = \sum_{k\in\mathbb{N}} \overline{a_k + b_k} X^k = f(P) + f(Q)$
et $f(PQ) = \sum_{n\in\mathbb{N}} \overline{\sum_{h+k=n} a_h b_k} X^n = f(P)f(Q)$. □

Remarque. $\overline{X} = X$. Plus généralement, pour tout $P \in \mathbb{R}[X]$, $\overline{P} = P$.

Propriété. Soit $P \in \mathbb{C}[X]$, $\alpha \in \mathbb{C}$ et $m \in \mathbb{N}$. α est racine de P de multiplicité m si et seulement si $\overline{\alpha}$ est racine de $\overline{P}$ de multiplicité m.

Démonstration.
Supposons que α est racine de P de multiplicité m. Alors il existe $Q \in \mathbb{C}[X]$ tel que $P(X) = (X-\alpha)^m Q(X)$ et $Q(\alpha) \neq 0$.
L'application $P \longmapsto \overline{P}$ étant un morphisme d'anneaux,
$\overline{P} = (X-\overline{\alpha})^m \overline{Q}(X)$ et $\overline{Q}(\overline{\alpha}) = \overline{Q(\alpha)} \neq 0$. Ainsi, $\overline{\alpha}$ est racine de $\overline{P}$ de multiplicité m.
Réciproquement, si $\overline{\alpha}$ est racine de $\overline{P}$ de multiplicité m, alors d'après le sens direct, $\alpha = \overline{\overline{\alpha}}$ est racine de $P = \overline{\overline{P}}$ de multiplicité m. □

Corollaire. Si $P \in \mathbb{R}[X]$ et si α est racine de P (resp : racine de multiplicité m), alors $\overline{\alpha}$ est aussi une racine de P (resp : racine de multiplicité m).

Théorème de d'Alembert : Tout polynôme à coefficients complexes de degré supérieur ou égal à 1 possède au moins une racine complexe.

Démonstration.
Admis. □

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

Démonstration.
Pour tout corps $\mathbb{K}$, on sait que les polynômes de degré 1 sont toujours irréductibles.
Soit $P \in \mathbb{C}[X]$ tel que $\deg(P) \neq 1$.
Si $\deg(P) \leq 0$, alors P est nul ou bien est inversible, donc P n'est pas irréductible.
Si $\deg(P) \geq 2$, d'après le théorème de d'Alembert, il possède au moins une racine $\alpha \in \mathbb{C}$. Alors $X - \alpha$ est un diviseur de P qui n'est associé ni à 1, ni à P, donc P n'est pas irréductible. □

Corollaire. Dans $\mathbb{C}[X]$, deux polynômes non nuls sont premiers entre eux si et seulement si ils n'ont aucune racine complexe commune.

Corollaire. Dans $\mathbb{C}[X]$, tout polynôme non nul est scindé.
Dans $\mathbb{C}[X]$, le nombre de racines, comptées avec multiplicité, de tout polynôme non nul est égal à son degré.

Propriété. Soit $P, Q \in \mathbb{C}[X] \setminus \{0\}$. Alors $P \mid Q$ si et seulement si toute racine de P est racine de Q avec une multiplicité pour Q supérieure ou égale à celle pour P.

Exercice. Déterminer les polynômes P de $\mathbb{C}[X]$ tels que $P' \mid P$.

Solution : Supposons que $P' \mid P$.
Si P est constant, $P' = 0$, donc $P' \mid P \iff P = 0$.
Supposons maintenant que $\deg(P) \geq 1$. P est scindé sur $\mathbb{C}[X]$, donc il existe $\mu \in \mathbb{C}^*$, $k \geq 1$, $a_1, \dots, a_k \in \mathbb{C}$, $m_1, \dots, m_k \in \mathbb{N}^*$ tels que $P = \mu \prod_{i=1}^{k} (X - a_i)^{m_i}$.

$P' \mid P$, donc il existe $\mu' \in \mathbb{C}^*$ et $p_1, \dots, p_k \in \mathbb{N}$ tels que $P' = \mu' \prod_{i=1}^{k} (X - a_i)^{p_i}$, avec $p_i \leq m_i$ pour tout $i \in \{1, \dots, k\}$.
Soit $i \in \{1, \dots, k\}$. a_i est racine de P de multiplicité m_i, donc pour tout $h \in \{0, \dots, m_i - 1\}$, $P^{(h)}(a_i) = 0$ et $P^{(m_i)}(a_i) \neq 0$. Ainsi, a_i est racine de P' de multiplicité $m_i - 1$. donc, pour tout $i \in \{1, \dots, k\}$, $p_i = m_i - 1$. On en déduit que $\deg(P') = \sum_{i=1}^{k} p_i = \left(\sum_{i=1}^{k} m_i \right) - k = \deg(P) - k$, donc $k = \deg(P) - \deg(P') = 1$.
P est donc de la forme $P(X) = \mu(X - a_1)^{m_1}$.
La réciproque est claire.

Propriété. Les polynômes irréductibles de $\mathbb{R}[X]$ sont exactement les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatif.

Démonstration.
Soit $P = aX^2 + bX + c \in \mathbb{R}[X]$ tel que $a \neq 0$ et $\Delta = b^2 - 4ac < 0$. Alors les racines complexes de P sont $\dfrac{-b \pm i\sqrt{-\Delta}}{2a} \notin \mathbb{R}$.
Or si P n'est pas irréductible, on peut l'écrire sous la forme $P = AB$ avec $A, B \in \mathbb{R}[X]$, $\deg(A) \geq 1$ et $\deg(B) \geq 1$. Mais $\deg(A) + \deg(B) = \deg(P) = 2$, donc $\deg(A) = 1$. Donc A possède une racine réelle, qui est aussi racine de P, ce qui est faux. Ainsi, P est irréductible.
Réciproquement, supposons que P n'est pas un polynôme de degré 1 ni un polynôme de degré 2 à discriminant strictement négatif.
Si $\deg(P) \leq 0$, alors P est nul ou bien est inversible, donc P n'est pas irréductible.
Si $\deg(P) = 2$, son discriminant est positif, donc il possède une racine $a \in \mathbb{R}$. Il est divisible par $X - a$, donc il n'est pas irréductible.
Supposons maintenant que $\deg(P) \geq 3$. D'après le théorème de d'Alembert, P possède au moins une racine complexe α.
Si $\alpha \in \mathbb{R}$, alors P n'est pas irréductible.
Si $\alpha \notin \mathbb{R}$, alors $\overline{\alpha}$ est également une racine de P et $\alpha \neq \overline{\alpha}$, donc P est un multiple de $(X - \alpha)(X - \overline{\alpha})$ dans $\mathbb{C}[X]$. Or $(X - \alpha)(X - \overline{\alpha}) = X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|^2 \in \mathbb{R}[X]$. On sait alors que $X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|^2$ divise P dans $\mathbb{R}[X]$, donc P n'est pas irréductible dans $\mathbb{R}[X]$. □

Propriété. Soit $P \in \mathbb{R}[X] \setminus \{0\}$. P est scindé dans $\mathbb{R}[X]$ si et seulement si toutes ses racines sont réelles.

Remarque. On peut généraliser cette propriété. En effet, pour tout corps $\mathbb{K}$, en utilisant l'axiome du choix, on peut montrer (hors programme) qu'il existe un surcorps de $\mathbb{K}$, noté $\widehat{\mathbb{K}}$, tel que tout polynôme non nul de $\widehat{\mathbb{K}}[X]$ est scindé dans $\widehat{\mathbb{K}}[X]$ et tel que, pour tout $\alpha \in \widehat{\mathbb{K}}$, il existe $P \in \mathbb{K}[X] \setminus \{0\}$ tel que $\widetilde{P}(\alpha) = 0$.
On dit que $\widehat{\mathbb{K}}$ est la clôture algébrique de $\mathbb{K}$.
Alors si $P \in \mathbb{K}[X] \setminus \{0\}$, P est scindé dans $\mathbb{K}[X]$ si et seulement si toutes ses racines (a priori dans $\widehat{\mathbb{K}}$) sont dans $\mathbb{K}$.

Exercice. Soit $m \in \mathbb{N}$.
Dans $\mathbb{R}[X]$, décomposer $X^{2m} - 1$ en produit de polynômes irréductibles.

Solution : On décompose dans $\mathbb{C}[X]$ puis on regroupe les racines deux à deux conjuguées. Plus précisément,

$$X^{2m} - 1 = \prod_{k=1-m}^{m} (X - e^{\frac{ik\pi}{m}}) = (X-1)(X+1) \prod_{k=1}^{m-1} (X - e^{\frac{ik\pi}{m}})(X - \overline{e^{\frac{ik\pi}{m}}}),$$

$$\text{donc } X^{2m} - 1 = (X-1)(X+1) \prod_{k=1}^{m-1} (X^2 - 2\cos(\frac{k\pi}{m})X + 1).$$

Exercice. Dans $\mathbb{R}[X]$,
décomposer $P = X^4 + \sqrt{2}X^2 + 1$ en produit de polynômes irréductibles.

Solution :
$P = (X^2+1)^2 + (\sqrt{2}-2)X^2 = (X^2 + \sqrt{2-\sqrt{2}}X + 1)(X^2 - \sqrt{2-\sqrt{2}}X + 1)$.
On peut vérifier que ces polynômes de degré 2 sont de discriminants strictement négatifs.

Remarque. Cet exercice s'adapte à tout polynôme à coefficients réels, bicarré, c'est-à-dire de la forme $aX^4 + bX^2 + c$ avec $a \neq 0$, tel que $b^2 - 4ac < 0$.

Exercice. Soit $P \in \mathbb{R}[X]$. Montrer que $P(\mathbb{R}) \subset \mathbb{R}_+$ si et seulement si il existe $A, B \in \mathbb{R}[X]$ tels que $P = A^2 + B^2$.

Solution : Le sens indirect est clair. Réciproquement, supposons que $P(\mathbb{R}) \subset \mathbb{R}_+$.
Si P nul, $A = B = 0$ conviennent.
Supposons maintenant que $P \neq 0$. Notons $a_1, \ldots, a_k$ les racines réelles de P, et notons $m_1, \ldots, m_k$ leurs multiplicités respectives.
Soit $i \in \{1, \ldots, k\}$. Il existe $Q \in \mathbb{R}[X]$ tel que $P = (X - a_i)^{m_i} Q$ avec $Q(a_i) \neq 0$, donc lorsque t est au voisinage de a_i, $P(t) \sim Q(a_i)(t - a_i)^{m_i}$. Ainsi, par hypothèse, $(t - a_i)^{m_i}$ ne change pas de signe au voisinage de a_i, donc m_i est pair.
Notons de plus $z_1, \ldots, z_h$ les racines complexes de P dont la partie imaginaire est strictement positive, et notons $q_1, \ldots, q_h$ leurs multiplicités respectives. On sait alors que les racines de P dont la partie imaginaire est strictement négative sont

les $\overline{z_1}, \dots, \overline{z_h}$ et que leurs multiplicités sont encore $q_1, \dots, q_h$. Ainsi, il existe $a > 0$ tel que $P(X) = a\Big(\prod_{i=1}^{k}(X-a_i)^{m_i}\Big)\Big(\prod_{j=1}^{h}(X-z_j)^{q_j}(X-\overline{z_j})^{q_j}\Big)$.

Posons $Q(X) = \sqrt{a}\Big(\prod_{i=1}^{k}(X-a_i)^{\frac{m_i}{2}}\Big)\Big(\prod_{j=1}^{h}(X-z_j)^{q_j}\Big)$.

Ainsi, pour tout $x \in \mathbb{R}$, $P(x) = Q(x)\overline{Q(x)} = \mathrm{Re}(Q(x))^2 + \mathrm{Im}(Q(x))^2$.
Posons $A(X) = \mathrm{Re}(Q)(X)$ et $B(X) = \mathrm{Im}(Q)(X)$. Alors, d'après l'identification entre polynômes formels de $\mathbb{R}[X]$ et applications polynomiales, on a montré que $P(X) = A^2 + B^2$.

4 Fractions rationnelles

4.1 Le corps des fractions rationnelles

4.1.1 Corps des fractions d'un anneau intègre

En reprenant la construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$, on obtient le théorème suivant :

Théorème. Soit A un anneau intègre. Il existe un corps K, unique à un isomorphisme près, tel que A est un sous-anneau de K, et tel que tout élément de K peut s'écrire sous la forme $\frac{a}{b}$ où $(a,b) \in A^2$ avec $b \neq 0$. a est appelé le numérateur et b le dénominateur de l'écriture $\frac{a}{b}$.
K est appelé le ***corps des fractions*** de A. C'est le plus petit corps contenant A.

Exemple. Le corps des fractions de $\mathbb{Z}$ est $\mathbb{Q}$.

Démonstration.
On adapte la construction de $\mathbb{Q}$:
◇ on définit une relation binaire R sur $A \times (A \setminus \{0\})$ par :

$$\forall (a,b),(c,d) \in A \times (A \setminus \{0\}),\ \ (a,b)R(c,d) \iff ad = bc.$$

On vérifie que R est une relation d'équivalence : pour la transitivité, si $(a,b)R(c,d)R(e,f)$, alors $ad = bc$ et $cf = de$, donc $(ad)f = b(cf) = bde$, donc $d(af - be) = 0$. A est intègre et $d \neq 0$, donc $af = be$ ce qui montre que $(a,b)R(e,f)$.
◇ On pose $K = (A \times (A \setminus \{0\}))/R$.
Pour tout $(a,b) \in A \times (A \setminus \{0\})$, on note $\frac{a}{b} = \overline{(a,b)}$.
Ainsi, pour tout $(a,b),(c,d) \in A \times (A \setminus \{0\})$, $\frac{a}{b} = \frac{c}{d} \iff (a,b)\ R\ (c,d) \iff ad = bc$.
◇ Pour tout $(a,b),(c,d) \in A \times (A \setminus \{0\})$, on pose $\frac{a}{b} \times \frac{c}{d} \triangleq \frac{ac}{bd}$ et $\frac{a}{b} + \frac{c}{d} \triangleq \frac{ad+cb}{bd}$.
Il faut vérifier que ces définitions sont cohérentes :
Supposons que $(a,b)\ R\ (a_1,b_1)$ et $(c,d)\ R\ (c_1,d_1)$, i.e $ab_1 = ba_1$ et $cd_1 = dc_1$. Alors $acb_1d_1 = (ab_1)(cd_1) = (ba_1)(dc_1) = bda_1c_1$, donc $\frac{ac}{bd} = \frac{a_1c_1}{b_1d_1}$ et

$(ad+cb)b_1d_1 = (ab_1)(dd_1)+(cd_1)(bb_1) = ba_1dd_1+dc_1bb_1 = (a_1d_1+c_1b_1)bd$, donc $\dfrac{ad+cb}{bd} = \dfrac{a_1d_1+c_1b_1}{b_1d_1}$.

◇ On vérifie que $(K,+)$ est un groupe abélien :
- L'addition admet pour élément neutre $0_K \overset{\Delta}{=} \dfrac{0_A}{1_A}$.
- $\dfrac{a}{b}+\dfrac{-a}{b} = \dfrac{0}{b} = \dfrac{0}{1} = 0$, donc tout élément de K possède un symétrique.
- $(\dfrac{a_0}{b_0}+\dfrac{a_1}{b_1})+\dfrac{a_2}{b_2} = \dfrac{a_0b_1+b_0a_1}{b_0b_1}+\dfrac{a_2}{b_2} = \dfrac{a_0b_1b_2+b_0a_1b_2+b_0b_1a_2}{b_0b_1b_2}$ et $\dfrac{a_0}{b_0}+(\dfrac{a_1}{b_1}+\dfrac{a_2}{b_2}) = \dfrac{a_0+b_0}{b_0}+\dfrac{a_1b_2+b_1a_2}{b_1b_2} = \dfrac{a_0b_1b_2+b_0a_1b_2+b_0b_1a_2}{b_0b_1b_2}$, d'où l'associativité de l'addition.
- $\dfrac{a}{b}+\dfrac{c}{d} = \dfrac{ad+cb}{bd} = \dfrac{c}{d}+\dfrac{a}{b}$.

◇ On vérifie que $(K,+,\times)$ est un anneau :
- La multiplication admet pour élément neutre $1_K \overset{\Delta}{=} \dfrac{1_A}{1_A}$.
- Elle est clairement associative.
- $\dfrac{a}{b}\times\left(\dfrac{a_1}{b_1}+\dfrac{a_2}{b_2}\right) = \dfrac{a}{b}\times\dfrac{a_1b_2+b_1a_2}{b_1b_2} = \dfrac{aa_1b_2+ab_1a_2}{bb_1b_2}$ et $\dfrac{a}{b}\times\dfrac{a_1}{b_1}+\dfrac{a}{b}\times\dfrac{a_2}{b_2} = \dfrac{aa_1}{bb_1}+\dfrac{aa_2}{bb_2} = \dfrac{aa_1bb_2+bb_1aa_2}{bb_1bb_2}$, donc le produit est distributif par rapport à l'addition.

◇ On vérifie que K est un corps :
- K n'est pas réduit à $\{0_A\}$, car $1_K = \frac{1_A}{1_A} \neq \frac{0_A}{1_A} = 0_K$.
- K est commutatif.
- Soit $f = \dfrac{a}{b} \in K\setminus\{0_K\}$: $\dfrac{a}{b} \neq \dfrac{0_A}{1_A}$, donc $a \neq 0_A$. Ainsi, $(b,a) \in A\times(A\setminus\{0_A\})$ et $\dfrac{b}{a}$ est un élément de K. De plus $\dfrac{a}{b}\times\dfrac{b}{a} = \dfrac{1_A}{1_A} = 1_K$, donc tout élément non nul de K est inversible.

◇ On identifie A avec une partie de K :

Notons $\varphi : \begin{array}{ccc} A & \longrightarrow & K \\ a & \longmapsto & \frac{a}{1_A} \end{array}$. On vérifie que φ est un morphisme injectif d'anneaux, car $\varphi(1_A) = 1_K$, $\varphi(ab) = \varphi(a)\times\varphi(b)$ et $\varphi(a)+\varphi(b) = \dfrac{a}{1_A}+\dfrac{b}{1_A} = \dfrac{a+b}{1_A} = \varphi(a+b)$. On peut donc identifier A avec $\varphi(A)$ qui est un sous-anneau du corps K. Cela revient à confondre a et $\dfrac{a}{1_A}$ pour tout $a \in A$.

◇ Soit $f \in K$. Il existe $(a,b) \in A\times(A\setminus\{0\})$ tel que $f = \frac{a}{b}$.

On peut écrire $f = \dfrac{a}{1_A}\times\left(\dfrac{b}{1_A}\right)^{-1}$, donc grâce à l'identification précédente, $f = a\times b^{-1}$, ce qui montre que $K = \{a\times b^{-1} \ / \ (a,b)\in A\times(A\setminus\{0\})\}$.

◇ Soit maintenant $(K',+',\times')$ un second corps admettant A comme sous-anneau et tel que $K' = \{a\times' b^{-1'} \ / \ (a,b)\in A\times(A\setminus\{0\})\}$.

Alors l'application $\begin{array}{rccc}\Psi : & K & \longrightarrow & K' \\ & a\times b^{-1} & \longmapsto & a\times' b^{-1'}\end{array}$ est un isomorphisme de corps. En effet, si $a\times b^{-1}=c\times d^{-1}$, avec $(a,b),(c,d)\in A\times(A\setminus\{0\})$, alors dans A on a $ad=bc$, donc c'est encore vrai dans K'. Ainsi $a\times' d=b\times' c$ puis $a\times' b^{-1'}=c\times' d^{-1'}$. Ainsi, Ψ est correctement défini.
De même, on peut définir $\begin{array}{ccc}K' & \longrightarrow & K \\ a\times' b^{-1'} & \longmapsto & a\times b^{-1}\end{array}$, qui est clairement l'application réciproque de Ψ : Ψ est donc une bijection.
$\Psi(1_K)=\Psi(1_A\times 1_A^{-1})=1_A\times' 1_A^{-1'}$. Or A est un sous-anneau de K', donc $1_A=1_{K'}$ puis $\Psi(1_K)=1_{K'}$.
$\Psi((a\times b^{-1})\times(c\times d^{-1}))=\Psi((ac)\times(bd)^{-1})=(ac)\times'(bd)^{-1'}$. Or $ac=a\times_A c=a\times' c$, donc $\Psi((a\times b^{-1})\times(c\times d^{-1}))=(a\times' b^{-1'})\times'(c\times' d^{-1'})=\Psi(a\times b^{-1})\times'\Psi(c\times c^{-1})$.

$$\begin{aligned}\Psi((a\times b^{-1})+(c\times d^{-1})) &= \Psi(((ad)\times(db)^{-1})+((cb)\times(db)^{-1})) \\ &= \Psi((ad+cb)\times(db)^{-1}) \\ &= (ad+cb)\times'(db)^{-1'},\end{aligned}$$

donc $\Psi((a\times b^{-1})+(c\times d^{-1}))=(a\times' d+' c\times' b)\times'(d\times' b)^{-1'}$, puis le même calcul mais mené maintenant dans K' donne
$\Psi((a\times b^{-1})+(c\times d^{-1}))=(a\times' b^{-1'})+'(c\times' d^{-1'})=\Psi(a\times b^{-1})+'\Psi(c\times c^{-1})$.
Ceci prouve que Ψ est un isomorphisme de corps et achève la démonstration. □

4.1.2 Forme irréductible

Notation. Pour toute la suite, $\mathbb{K}$ désigne un corps quelconque.

Définition. On note $\mathbb{K}(X)$ le corps des fractions de l'anneau intègre $\mathbb{K}[X]$. Les éléments de $\mathbb{K}(X)$ sont appelés des fractions rationnelles en l'indéterminée X.
$\mathbb{K}(X)$ est une $\mathbb{K}$-algèbre.

Exemple. $\dfrac{X^3-1}{X^2-1}\in\mathbb{Q}(X)$, $\dfrac{2iX+1}{X^3+j}\in\mathbb{C}(X)$.

Remarque. $\mathbb{K}(X)$ est toujours de cardinal infini car il contient la suite des monômes $(X^n)_{n\in\mathbb{N}}$. Ainsi $(\mathbb{Z}/p\mathbb{Z})(X)$ est un exemple de corps de cardinal infini mais de caractéristique non nulle.

Définition. Soit $F\in\mathbb{K}(X)$.
$\dfrac{P}{Q}$ est un représentant irréductible de F si et seulement si $F=\dfrac{P}{Q}$ et si $P\wedge Q=1$.
$\dfrac{P}{Q}$ est un représentant unitaire de F si et seulement si $F=\dfrac{P}{Q}$ et si Q est unitaire.

Propriété. Soit $F\in\mathbb{K}(X)$.
F possède un unique représentant irréductible et unitaire. Si on le note $\dfrac{P}{Q}$, alors
les représentants irréductibles de F sont les $\dfrac{\lambda P}{\lambda Q}$ où $\lambda\in\mathbb{K}^*$,
et les représentants quelconques de F sont les $\dfrac{LP}{LQ}$ où $L\in\mathbb{K}[X]\setminus\{0\}$.

Démonstration.
◇ Il existe $A, B \in \mathbb{K}[X]$ tels que $B \neq 0$ et $F = \dfrac{A}{B}$. Posons $L = A \wedge B$. On sait alors que $A = A'L$ et $B = B'L$ avec $A' \wedge B' = 1$. Alors $B' \neq 0$ et $F = \dfrac{A'}{B'}$. En divisant A' et B' par le coefficient dominant de B', on obtient ainsi un représentant irréductible et unitaire de F, ce qui prouve son existence.
◇ Supposons que F possède deux représentants irréductibles et unitaires :
$F = \dfrac{P}{Q} = \dfrac{A}{B}$, avec Q et B unitaires, $P \wedge Q = A \wedge B = 1$.
Alors $PB = AQ$, donc $B|AQ$, mais $A \wedge B = 1$, donc d'après le théorème de Gauss, $B|Q$. De même, on montre que $Q|B$, donc B et Q sont associés. Or ils sont unitaires, donc ils sont égaux. Ainsi, $(A, B) = (P, Q)$, ce qui prouve l'unicité.
◇ Conformément à l'énoncé, on note maintenant $\dfrac{P}{Q}$ le représentant irréductible unitaire de F.
Supposons que $F = \dfrac{A}{B}$. Alors $AQ = BP$, donc $Q|BP$, or $Q \wedge P = 1$, donc $Q|B$: il existe $L \in \mathbb{K}[X]$ tel que $B = LQ$. Alors $AQ = LQP$, mais $Q \neq 0$, donc $A = LP$.
Si de plus $A \wedge B = 1$, alors on montre également que $B|Q$, donc B et Q sont associés, ce qui impose à L d'être une constante non nulle. □

Exemple. Le représentant irréductible unitaire de $\dfrac{X^3-1}{X^2-1}$ est $\dfrac{X^2+X+1}{X+1}$.

Convention : sauf mention du contraire, dans la suite de ce chapitre, lorsque F est une fraction rationnelle, l'écriture $F = \dfrac{P}{Q}$ sous-entend que $P, Q \in \mathbb{K}[X]$ avec $Q \neq 0$.

4.1.3 Degré

Définition. Soit $F = \dfrac{P}{Q} \in \mathbb{K}(X)$. La quantité $\deg(P) - \deg(Q)$ ne dépend que de F.
Elle est appelée le degré de F. Ainsi, $\deg\Big(\dfrac{P}{Q}\Big) \triangleq \deg(P) - \deg(Q) \in \mathbb{Z} \cup \{-\infty\}$.

Démonstration.
Si $F = 0$, alors $P = 0$ et $\deg(P) - \deg(Q) = -\infty$.
Supposons maintenant que $F \neq 0$. Notons $\dfrac{A}{B}$ son unique représentant unitaire irréductible.
Il existe $L \in \mathbb{K}[X] \setminus \{0\}$ tel que $P = LA$ et $Q = LB$. Ainsi,
$\deg(P) - \deg(Q) = (\deg(L) + \deg(A)) - (\deg(L) + \deg(B)) = \deg(A) - \deg(B)$. □

Remarque. Pour tout $F \in \mathbb{K}(X)$, $F = 0 \iff \deg(F) = -\infty$.
Pour tout $P \in \mathbb{K}[X]$, $\deg\Big(\dfrac{P}{1}\Big) = \deg(P)$, donc l'application $\deg|_{\mathbb{K}(X)}$ est un prolongement de $\deg|_{\mathbb{K}[X]}$.

Exemple. $\deg\Big(\dfrac{X^3+X-3}{2X^2+X+4}\Big) = 1$.

Propriété. Soit $F, G \in \mathbb{K}(X)$.
- $\deg(F+G) \leq \max(\deg(F), \deg(G))$, avec égalité lorsque $\deg(F) \neq \deg(G)$.
- $\deg(FG) = \deg(F) + \deg(G))$.
- $\deg(FG^{-1}) = \deg(F) - \deg(G)$.

Démonstration.
Posons $F = \dfrac{P}{Q}$ et $G = \dfrac{A}{B}$. Alors $F + G = \dfrac{PB + QA}{QB}$,

$$\begin{aligned} \deg(F+G) &= \deg(PB+QA) - \deg(QB) \\ &\leq \max(\deg(PB), \deg(QA)) - \deg(QB) \\ &= \max(\deg(PB) - \deg(QB), \deg(QA) - \deg(QB)) \\ &= \max(\deg(F), \deg(G)). \end{aligned}$$

donc

Supposons de plus que $\deg(F) \neq \deg(G)$. Alors $\deg(PB) \neq \deg(QA)$, donc l'inégalité précédente est maintenant une égalité. □

4.1.4 Racines et pôles

Définition. Soit $F \in \mathbb{K}(X)$ une fraction rationnelle admettant pour représentant **irréductible** $\dfrac{A}{B}$.
- Les racines de F sont, par définition, les racines de A.
  Pour tout $a \in \mathbb{K}$ et $m \in \mathbb{N}$, on dit que a est racine de F de multiplicité m si et seulement si a est racine de A de multiplicité m.
- Les pôles de F sont, par définition, les racines de B.
  Pour tout $a \in \mathbb{K}$ et $m \in \mathbb{N}$, on dit que a est un pôle de F de multiplicité m si et seulement si a est racine de B de multiplicité m.

Exemples.
- Dans $\mathbb{C}(X)$, $F(X) = \dfrac{X^3-1}{X^2-1} = \dfrac{X^2+X+1}{X+1}$, donc F possède exactement 2 racines, j et j^2, qui sont simples, et un unique pôle, égal à -1, également simple.
- Pour tout $a \in \mathbb{K}$, a est racine de la fraction rationnelle nulle, mais cette dernière ne possède aucun pôle, car la forme irréductible unitaire de 0 est $\frac{0}{1}$.
- Pour $n \in \mathbb{N}^*$, dans $\mathbb{C}(X)$, $\dfrac{1}{X^n-1}$ ne possède aucune racine et ses pôles, tous simples, sont les racines n-ièmes de l'unité.

Remarque. $a \in \mathbb{K}$ ne peut pas être à la fois un pôle et une racine de $F \in \mathbb{K}(X)$.

Définition. Si $F = \dfrac{P}{Q} \in \mathbb{C}[X]$, on note $\overline{F} = \dfrac{\overline{P}}{\overline{Q}}$ (on vérifie que la définition de $\overline{F}$ ne dépend que de F et non du représentant (P, Q)).

Propriété. L'application $\begin{array}{ccc} \mathbb{C}(X) & \longrightarrow & \mathbb{C}(X) \\ F & \longmapsto & \overline{F} \end{array}$ est un isomorphisme de corps.

Propriété. Soit $F \in \mathbb{C}(X)$, $\alpha \in \mathbb{C}$ et $m \in \mathbb{N}$. α est racine (resp : pôle) de F de multiplicité m si et seulement si $\overline{\alpha}$ est racine (resp : pôle) de $\overline{F}$ de multiplicité m.

Corollaire. Si $F \in \mathbb{R}(X)$ et si α est racine de F (resp : racine de multiplicité m), alors $\overline{\alpha}$ est aussi une racine de F (resp : racine de multiplicité m).

4.1.5 Fonctions rationnelles

Définition. Soit $F \in \mathbb{K}(X)$ une fraction rationnelle admettant pour représentant **irréductible** $\dfrac{A}{B}$. Notons $\mathcal{P}$ l'ensemble de ses pôles.

La fonction rationnelle associée à F est l'application $\begin{array}{rccc} \tilde{F} : & \mathbb{K} \setminus \mathcal{P} & \longrightarrow & \mathbb{K} \\ & x & \longmapsto & \dfrac{\tilde{A}(x)}{\tilde{B}(x)} \end{array}$.

Exemple. La fonction rationnelle associée à $\dfrac{X^3-1}{X^2-1} \in \mathbb{R}(X)$ est égale à $\begin{array}{rcl} \mathbb{R} \setminus \{-1\} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \dfrac{x^2+x+1}{x+1} \end{array}$.

Remarque. Si $\dfrac{P}{Q}$ est un représentant quelconque de $F \in \mathbb{K}(X)$ et si $x \in \mathbb{K}$ avec $\tilde{Q}(x) \neq 0$, alors $\tilde{F}(x) = \dfrac{\tilde{P}(x)}{\tilde{Q}(x)}$.

Propriété. Si deux fractions rationnelles coïncident pour une infinité de valeurs de $\mathbb{K}$, elles sont égales.

4.1.6 Composition

Définition. Si $P = \sum_{n\in\mathbb{N}} a_n X^n \in \mathbb{K}[X]$ et $F \in \mathbb{K}(X)$,
on note $P \circ F$ ou $P(F)$ la fraction rationnelle $\sum_{n\in\mathbb{N}} a_n F^n$.

Propriété. Pour tout $F \in \mathbb{K}(X)$,
l'application $P \longmapsto P(F)$ est un morphisme d'algèbres de $\mathbb{K}[X]$ dans $\mathbb{K}(X)$.

Démonstration.
Fixons $F \in \mathbb{K}(X)$.
Soit $P, Q \in \mathbb{K}[X]$. Notons $P = \sum_{n\in\mathbb{N}} a_n X^n$ et $Q = \sum_{n\in\mathbb{N}} b_n X^n$. Alors
$(PQ)(F) = \sum_{k\in\mathbb{N}} \Big(\sum_{i+j=k} a_i b_j \Big) F^k$, or en calculant dans le corps $\mathbb{K}(X)$,
$P(F) \times Q(F) = \Big(\sum_{k\in\mathbb{N}} a_k F^k\Big) \times \Big(\sum_{k\in\mathbb{N}} b_k F^k\Big) = \sum_{k,h\in\mathbb{N}} a_k b_h F^{k+h}$, puis par sommation par paquets, $P(F)\times Q(F) = \sum_{n\in\mathbb{N}} \sum_{\substack{k,h\in\mathbb{N} \\ k+h=n}} a_k b_h F^n$, ce qui montre que $P(F)\times Q(F) = (PQ)(F)$.

On vérifie aisément que $P(F)+Q(F)=(P+Q)(F)$, $1(F)=1$ et que $P(\alpha F)=\alpha P(F)$ pour tout $\alpha\in\mathbb{K}$. □

Lemme : Soit $P\in\mathbb{K}[X]$ et $F\in\mathbb{K}(X)$.
Si $P\neq 0$ et si $F\notin\mathbb{K}$, alors $P\circ F\neq 0$.

Démonstration.
Au tableau. □

Définition. Soit $F\in\mathbb{K}(X)$ et $G\in\mathbb{K}(X)\setminus\mathbb{K}$.
Si $F=\dfrac{P}{Q}$, alors on pose $F\circ G=F(G)=\dfrac{P(G)}{Q(G)}$.
On vérifie que cette quantité ne dépend que de F et non de son représentant (P,Q).

Remarque. On utilise le lemme pour garantir que $Q(G)\neq 0$.
Lorsque $G\in\mathbb{K}$, $Q(G)$ peut s'annuler. On a déjà défini $\tilde{F}(G)$ lorsque G n'est pas un pôle de F.

Exemple. Si $G=\dfrac{1+X}{X}$ et $F=\dfrac{X}{1-X}$, alors $G\circ F=\dfrac{1+\dfrac{X}{1-X}}{\dfrac{X}{1-X}}=\dfrac{1}{X}$.

Remarque. La propriété "$\deg(P\circ Q)=\deg(P)\times\deg(Q)$ lorsque $\deg(Q)\geq 1$", valable pour des polynômes, est encore vraie avec des fractions rationnelles (exercice), mais elle ne s'adapte pas du tout au cas où $\deg(Q)\leq -1$. En effet, pour tout $n\geq 2$, en posant $P=X^n+X$ et $G=\dfrac{1}{X}$, $\deg(P)=n$ et $\deg(P(G))=-1$.

Propriété. Pour tout $G\in\mathbb{K}(X)\setminus\mathbb{K}$,
l'application $F\longmapsto F(G)$ est un endomorphisme de l'algèbre $\mathbb{K}(X)$.

Démonstration.
Si $F=\dfrac{A}{B}$ et $H=\dfrac{C}{D}$,
$(F+H)(G)=\Big(\dfrac{AD+BC}{BD}\Big)(G)=\dfrac{A(G)D(G)+B(G)C(G)}{B(G)D(G)}=\Big(\dfrac{A}{B}\Big)(G)+\Big(\dfrac{C}{D}\Big)(G)$,
donc $(F+H)(G)=F(G)+H(G)$.
On vérifie aisément que $(F\times H)(G)=F(G)\times H(G)$, $1(G)=1$ et que
$(\alpha F)(G)=\alpha.F(G)$ pour tout $\alpha\in\mathbb{K}$. □

4.1.7 Dérivation

Définition. Soit $F=\dfrac{P}{Q}\in\mathbb{K}(X)$. On pose $F'\triangleq\dfrac{P'Q-Q'P}{Q^2}\in\mathbb{K}(X)$.
On vérifie que F' ne dépend que de F et non de (P,Q).

Démonstration.
Partons du représentant irréductible unitaire de F, noté $\dfrac{A}{B}$.
Il existe $L\in\mathbb{K}[X]$ tel que $L\neq 0$, $P=AL$ et $Q=BL$.

Alors $\dfrac{P'Q-Q'P}{Q^2}=\dfrac{(A'L+AL')BL-(B'L+BL')AL}{B^2L^2}=\dfrac{A'B-B'A}{B^2}$. □

Définition. Par récurrence, on peut définir la dérivée n-ième formelle d'une fraction rationnelle.

Propriété. Pour tout $F\in\mathbb{R}(X)$ et $n\in\mathbb{N}$, $\widetilde{F^{(n)}}=\tilde{F}^{(n)}$.

Propriété. Pour tout $F\in\mathbb{K}(X)$, $\deg(F')\leq\deg(F)-1$,
avec égalité lorsque $\text{car}(\mathbb{K})=0$ et $\deg(F)\neq 0$.

Démonstration.
Supposons que $\text{car}(\mathbb{K})=0$ et $\deg(F)\notin\{0,-\infty\}$. Notons $F=\dfrac{P}{Q}$ avec $\deg(P)=n$, $\deg(Q)=p$. On a $n\neq p$. On peut supposer que Q est unitaire. On note a_n le coefficient dominant de P. Alors le coefficient de $P'Q-Q'P$ de degré $n+p-1$ vaut $(n-p)a_n$. Il est bien non nul. □

Propriété. Soit $F,G\in\mathbb{K}(X)$, $a\in\mathbb{K}$ et $n\in\mathbb{N}$.
- $(F+G)'=F'+G'$, et plus généralement, $(F+G)^{(n)}=F^{(n)}+G^{(n)}$.
- $(aF)'=aF'$, et plus généralement, $(aF)^{(n)}=aF^{(n)}$.
- $(FG)'=F'G+FG'$.
- Si $G\neq 0$, $\left(\dfrac{F}{G}\right)'=\dfrac{F'G-G'F}{G^2}$.

Démonstration.
Exercice, ainsi que pour les propriétés suivantes. □

Propriété. Pour tout $n\in\mathbb{N}$ et $F_1,\dots,F_n\in\mathbb{K}(X)$, $(F_1\times\cdots\times F_n)'=\displaystyle\sum_{i=1}^{n}F_i'\prod_{j\neq i}F_j$.

Formule de Leibniz : Pour tout $F,G\in\mathbb{K}(X)$, pour tout $n\in\mathbb{N}$,

$$(FG)^{(n)}=\sum_{k=0}^{n}\binom{n}{k}F^{(k)}G^{(n-k)}.$$

Propriété. Pour tout $F,G\in\mathbb{K}(X)$, avec $G\notin\mathbb{K}$, $(F\circ G)'=G'\times(F'\circ G)$.

4.2 Décomposition en éléments simples.

4.2.1 Partie entière

Définition. Un élément simple de $\mathbb{K}(X)$ est une fraction rationnelle de la forme $\dfrac{P}{Q^m}$, où $m\in\mathbb{N}^*$ et $P,Q\in\mathbb{K}[X]$, avec Q irréductible et $\deg(P)<\deg(Q)$.

Nous allons montrer que toute fraction rationnelle s'écrit de manière unique comme la somme d'un polynôme et d'une combinaison linéaire d'éléments simples. Cette écriture s'appelle la décomposition en éléments simples (DES) de la fraction rationnelle.

Propriété de la partie entière :
Soit $F = \dfrac{A}{S} \in \mathbb{K}(X)$. Il existe un unique couple $(E, B) \in \mathbb{K}[X]^2$ tel que

$$F = E + \frac{B}{S} \text{ avec } \deg(B) < \deg(S).$$

De plus, si $\dfrac{A}{S}$ est irréductible alors $\dfrac{B}{S}$ l'est également.
Le polynôme E est appelé la *partie entière* de F. C'est le quotient de la division euclidienne de A par S.
$\dfrac{B}{S}$ (de degré strictement négatif) est appelée la partie fractionnaire de F.
Démonstration.

- *Existence :* La division euclidienne de A par S donne l'existence de $(E, B) \in \mathbb{K}[X]^2$ tel que $A = SE + B$ avec $\deg(B) < \deg(S)$. En divisant dans $\mathbb{K}(X)$ cette égalité par S, on obtient $F = E + \dfrac{B}{S}$. De plus, d'après l'algorithme d'Euclide, si $A \wedge S = 1$, on a $B \wedge S = 1$.
- *Unicité :* Considérons deux couples $(E, B), (D, C) \in \mathbb{K}[X]^2$ tels que l'on ait $F = E + \dfrac{B}{S} = D + \dfrac{C}{S}$ avec $\deg(B) < \deg(S)$ et $\deg(C) < \deg(S)$. On a alors $E - D = \dfrac{C}{S} - \dfrac{B}{S}$ ce qui implique que $\deg(E - D) < 0$, d'où $E - D = 0$, c'est-à-dire $E = D$. Il s'ensuit que $B = C$.

□

Exemple. Dans $\mathbb{R}(X)$, prenons $F(X) = \dfrac{X^3 + X + 1}{X^2 - X + 1}$.
La division euclidienne de $X^3 + X + 1$ par $X^2 - X + 1$ s'écrit
$X^3 + X + 1 = (X^2 - X + 1)(X + 1) + X$, or $X^2 - X + 1$ a pour discriminant $1 - 4 < 0$, donc il est irréductible. Ainsi l'écriture $F(X) = X + 1 + \dfrac{X}{X^2 - X + 1}$ est la DES de F dans $\mathbb{R}(X)$ (mais pas dans $\mathbb{C}(X)$).

4.2.2 Divisions successives

Propriété. Soient $B, S \in \mathbb{K}[X]$ avec $\deg(S) \geq 1$.
Il existe une unique famille $(E, T_1, \ldots, T_m) \in \mathbb{K}[X]^{m+1}$ telle que

$$\frac{B}{S^m} = E + \frac{T_1}{S} + \cdots + \frac{T_m}{S^m} \qquad \text{et} \qquad \forall i \in [\![1; m]\!], \quad \deg(T_i) < \deg(S).$$

De plus, E est la partie entière de B/S^m.
Démonstration.

- *Existence :* pour tout $m \in \mathbb{N}^*$, on pose
  $R(m)$: pour tout $B \in \mathbb{K}[X]$, il existe $E, T_1, \ldots, T_m \in \mathbb{K}[X]$ tels que

$\frac{B}{S^m} = E + \frac{T_1}{S} + \cdots + \frac{T_m}{S^m}$, avec, pour tout $i \in \mathbb{N}_m$, $\deg(T_i) < \deg(S)$.
Initialisation : $R(1)$ est vraie d'après la propriété de la partie entière.
Hérédité : Fixons $m \in \mathbb{N}^*$ tel que $R(m)$ est vraie et démontrons $R(m+1)$.
Soit $B \in \mathbb{K}[X]$. Par division euclidienne, il existe $B', T_{m+1} \in \mathbb{K}[X]$ tels que $B = B'S + T_{m+1}$ et $\deg(T_{m+1}) < \deg(S)$, donc $\frac{B}{S^{m+1}} = \frac{B'}{S^m} + \frac{T_{m+1}}{S^{m+1}}$.
On en déduit $R(m+1)$ en appliquant $R(m)$ à B'.
De plus, on a $\deg\Big(\frac{T_1}{S} + \cdots + \frac{T_m}{S^m}\Big) \leq \max\Big\{\deg\Big(\frac{T_1}{S}\Big), \ldots, \deg\Big(\frac{T_m}{S^m}\Big)\Big\} < 0$, ce qui démontre, d'après la propriété de la partie entière, que E est la partie entière de B/S^m.

— *Unicité :* Considérons deux familles $(E, T_1, \ldots, T_m), (D, U_1, \ldots, U_m) \in \mathbb{K}[X]^{m+1}$ telles que $\frac{B}{S^m} = E + \frac{T_1}{S} + \cdots + \frac{T_m}{S^m} = D + \frac{U_1}{S} + \cdots + \frac{U_m}{S^m}$ avec, pour tout $i \in [\![1; m]\!]$, $\deg(T_i) < \deg(S)$ et $\deg(U_i) < \deg(S)$.
Comme on vient de voir que E et D sont nécessairement la partie entière de $\frac{B}{S^m}$, on a tout de suite $E = D$, ce qui donne $\frac{T_1}{S} + \cdots + \frac{T_m}{S^m} = \frac{U_1}{S} + \cdots + \frac{U_m}{S^m}$: $(*)$.
En multipliant par S^{m-1},
on obtient $(T_1 S^{m-2} + \cdots + T_{m-1}) + \frac{T_m}{S} = (U_1 S^{m-2} + \cdots + U_{m-1}) + \frac{U_m}{S}$.
À nouveau grâce à la propriété sur la partie entière, on en déduit que $T_m = U_m$.
L'égalité $(*)$ devient alors $\frac{T_1}{S} + \cdots + \frac{T_{m-1}}{S^{m-1}} = \frac{U_1}{S} + \cdots + \frac{U_{m-1}}{S^{m-1}}$.
On conclut par récurrence.

□

Exemple. Pour décomposer en éléments simples $F(X) = \frac{X^3 + 2X^2 - 3X + 1}{(X-1)^3}$, on applique la méthode des divisions successives, qui s'inspire de la démonstration précédente :
$X^3 + 2X^2 - 3X + 1 = (X-1)X^2 + 3X^2 - 3X + 1 = (X-1)(X^2 + 3X) + 1$, donc
$F(X) = \frac{1}{(X-1)^3} + \frac{X^2 + 3X}{(X-1)^2}$,
puis $X^2 + 3X = (X-1)X + 4X = (X-1)(X+4) + 4$,
donc $F(X) = \frac{1}{(X-1)^3} + \frac{4}{(X-1)^2} + \frac{X+4}{X-1}$, puis finalement
$F(X) = 1 + \frac{5}{(X-1)} + \frac{4}{(X-1)^2} + \frac{1}{(X-1)^3}$. Il s'agit bien de la DES de F.

4.2.3 Cas général

Lemme de decomposition : Soient $A \in \mathbb{K}[X]$, $n \in \mathbb{N}^*$ et $S_1, \ldots, S_n \in \mathbb{K}[X]$ n polynômes non nuls et deux à deux premiers entre eux.
Il existe $A_1, \ldots, A_n \in \mathbb{K}[X]$ tels que $\frac{A}{S_1 \cdots S_n} = \frac{A_1}{S_1} + \cdots + \frac{A_n}{S_n}$.

Démonstration.
$(S_1 \cdots S_{n-1}) \wedge S_n = 1$ donc, d'après le théorème de Bézout,
il existe $U, V \in \mathbb{K}[X]$ tels que $S_1 \cdots S_{n-1}U + S_nV = 1$.
Ainsi, $\dfrac{A}{S_1 \cdots S_n} = \dfrac{A(S_1 \cdots S_{n-1}U + S_nV)}{S_1 \cdots S_n} = \dfrac{AU}{S_n} + \dfrac{AV}{S_1 \cdots S_{n-1}}$.
On conclut par récurrence sur n. □

Lemme de decomposition avec partie entiere : Soient $A \in \mathbb{K}[X]$, $n \in \mathbb{N}$ et $S_1, \ldots, S_n \in \mathbb{K}[X]$ n polynômes non nuls et deux à deux premiers entre eux.
Il existe une unique famille $(E, B_1, \ldots, B_n) \in K[X]^{n+1}$ telle que

$$\frac{A}{S_1 S_2 \cdots S_n} = E + \frac{B_1}{S_1} + \cdots + \frac{B_n}{S_n} \quad \text{et} \quad \forall i \in [\![1; n]\!], \ \deg(B_i) < \deg(S_i).$$

De plus, E est la partie entière de $\dfrac{A}{S_1 \cdots S_n}$.

Démonstration.
Le cas $n = 1$ n'est rien d'autre que la propriété de la partie entiere.
On suppose donc ici que $n \geq 2$.

— *Existence :* d'après lemme de decomposition, il existe $A_1, \ldots, A_n \in \mathbb{K}[X]$ tels que $\dfrac{A}{S_1 \cdots S_n} = \dfrac{A_1}{S_1} + \cdots + \dfrac{A_n}{S_n}$, puis, d'après la propriété de la partie entiere, il existe $E_1, \ldots, E_n, B_1, \ldots, B_n \in \mathbb{K}[X]$ tels que $\forall i \in [\![1; n]\!], \ \dfrac{A_i}{S_i} = E_i + \dfrac{B_i}{S_i}$ et $\deg(B_i) < \deg(S_i)$. On obtient alors $\dfrac{A}{S_1 \cdots S_n} = E_1 + \dfrac{B_1}{S_1} + \cdots + E_n + \dfrac{B_n}{S_n}$, ce qui donne le résultat attendu en posant $E = E_1 + \cdots E_n$.
De plus, on a $\deg\Big(\dfrac{B_1}{S_1} + \cdots + \dfrac{B_n}{S_n}\Big) \leq \max\Big\{\deg\Big(\dfrac{B_1}{S_1}, \ldots, \dfrac{B_n}{S_n}\Big)\Big\} < 0$, ce qui démontre, d'après la propriété de la partie entiere que E est la partie entière de $\dfrac{A}{S_1 \cdots S_n}$.

— *Unicité :* considérons deux familles $(E, B_1, \ldots, B_n), (D, C_1, \ldots, C_n) \in \mathbb{K}[X]^{n+1}$ telles que $\dfrac{A}{S_1 S_2 \cdots S_n} = E + \dfrac{B_1}{S_1} + \cdots + \dfrac{B_n}{S_n} = D + \dfrac{C_1}{S_1} + \cdots + \dfrac{C_n}{S_n}$ avec, pour tout $i \in [\![1; n]\!]$, $\deg(B_i) < \deg(S_i)$ et $\deg(C_i) < \deg(S_i)$.
Comme on vient de voir que E et D sont nécessairement la partie entière de $\dfrac{A}{S_1 \cdots S_n}$, on a tout de suite $E = D$, ce qui donne

$$\frac{B_1}{S_1} + \cdots + \frac{B_n}{S_n} = \frac{C_1}{S_1} + \cdots + \frac{C_n}{S_n} \quad : \quad (*)$$

Posons $T = S_1 \cdots S_{n-1}$ et réduisons au même dénominateur $\dfrac{B_1}{S_1} + \ldots + \dfrac{B_{n-1}}{S_{n-1}}$ d'une part et $\dfrac{C_1}{S_1} + \ldots + \dfrac{C_{n-1}}{S_{n-1}}$ d'autre part. On obtient ainsi l'existence de $B, C \in$

$\mathbb{K}[X]$ tels que $\dfrac{B}{T}+\dfrac{B_n}{S_n}=\dfrac{C}{T}+\dfrac{C_n}{S_n}$. Cela implique que $S_n(B-C)=T(C_n-B_n)$, donc $S_n \mid T(C_n-B_n)$. Or $T\wedge S_n=1$ donc, d'après le lemme de Gauss, on a $S_n \mid C_n-B_n$.
Par ailleurs, on a $\deg(C_n-B_n)\leq \max\{\deg(B_n);\deg(C_n)\}<\deg(S_n)$.
Ces deux informations ne sont compatibles que si $C_n-B_n=0$, c'est-à-dire $B_n=C_n$. L'égalité $(*)$ devient alors $\dfrac{B_1}{S_1}+\cdots+\dfrac{B_{n-1}}{S_{n-1}}=\dfrac{C_1}{S_1}+\cdots+\dfrac{C_{n-1}}{S_{n-1}}$.
On conclut par récurrence.

□

Théorème de décomposition en éléments simples :
Soit $F\in\mathbb{K}(X)$. On peut toujours écrire F sous la forme $F=\dfrac{A}{S_1^{m_1}S_2^{m_2}\cdots S_n^{m_n}}$,
où $S_1,S_2,\ldots,S_n$ sont des polynômes irréductibles dans $\mathbb{K}[X]$, $m_1,\ldots,m_n\in\mathbb{N}^*$ et $A\in\mathbb{K}[X]$ avec $A\wedge S_i=1$ pour tout $i\in\mathbb{N}_n$. Alors
il existe un unique $E\in\mathbb{K}[X]$ et une unique famille $(T_{i,j})_{\substack{1\leq i\leq n\\ 1\leq j\leq m_i}}$ de polynômes de $\mathbb{K}[X]$ tels que $F=E+\displaystyle\sum_{i=1}^{n}\Big(\sum_{j=1}^{m_i}\frac{T_{i,j}}{{S_i}^j}\Big)$
avec pour tout $i\in[\![1;n]\!]$ et $j\in[\![1;m_i]\!]$, $\deg(T_{i,j})<\deg(S_i)$.
Cette égalité s'appelle la décomposition en éléments simples de F sur $\mathbb{K}$.
Le polynôme E est la *partie entière* de F.
Pour $i\in[\![1;n]\!]$, la somme $\displaystyle\sum_{j=1}^{m_i}\frac{T_{i,j}}{{S_i}^j}$ s'appelle la partie polaire de F relative au polynôme S_i.

Démonstration.
Le lemme précédent garantit l'existence d'une unique famille $(E,B_1,\ldots,B_n)\in\mathbb{K}[X]^{n+1}$ tel que $F=E+\dfrac{B_1}{{S_1}^{m_1}}+\cdots+\dfrac{B_n}{{S_n}^{m_n}}$, avec pour tout $i\in[\![1;n]\!]$, $\deg(B_i)<\deg({S_i}^{m_i})$, où E est la partie entière de F.
Or, pour tout $i\in[\![1;n]\!]$, le lemme des divisions successives garantit l'existence d'une unique famille $(T_{i,1},\ldots,T_{i,m_i})\in\mathbb{K}[X]^{m_i}$ telle que $\dfrac{B_i}{{S_i}^{m_i}}=\dfrac{T_{i,1}}{S_i}+\cdots+\dfrac{T_{i,m_i}}{{S_i}^{m_i}}$, avec pour tout $j\in[\![1;m_i]\!]$, $\deg(T_{i,j})<\deg(S_i)$, où l'absence de partie entière découle du fait que $\deg\Big(\dfrac{B_i}{S_i^{m_i}}\Big)<0$. On en déduit que F s'écrit, de manière unique (y réfléchir), sous la forme $F=E+\displaystyle\sum_{i=1}^{n}\Big(\sum_{j=1}^{m_i}\frac{T_{i,j}}{{S_i}^j}\Big)$, avec pour tout $i\in[\![1;n]\!]$ et $j\in[\![1;m_i]\!]$,
$\deg(T_{i,j})<\deg(S_i)$, où E est la partie entière de F. □

4.2.4 Dérivée logarithmique

Propriété. Soit P un polynôme scindé dans $\mathbb{K}[X]$. Alors, en notant $\alpha_1, \dots, \alpha_n$ les racines de P et $m_1, \dots, m_n$ leurs multiplicités respectives,

$$\frac{P'}{P} = \sum_{i=1}^{n} \frac{m_i}{X - \alpha_i}.$$

Démonstration.
Par hypothèse, il existe $\lambda \in \mathbb{K}^*$ tel que $P = \lambda \prod_{i=1}^{n} (X - \alpha_i)^{m_i}$. Il suffit de dériver. □

Remarque. On retient facilement cette formule, en écrivant, sans aucune rigueur, que $\frac{P'}{P} = (\ln P)'$.

Exemple. La décomposition en éléments simples de $\frac{P'}{P}$, avec $P = X(X-1)^2$ est $\frac{1}{X} + \frac{2}{X-1}$.

4.2.5 Dans $\mathbb{C}(X)$ et $\mathbb{R}(X)$

Propriété.
Les élements simples de $\mathbb{C}(X)$ sont les fractions rationnelles $\frac{a}{(X-b)^m}$, où $a, b \in \mathbb{C}$ et $m \in \mathbb{N}^*$.

Théorème de décomposition en éléments simples dans $\mathbb{C}(X)$:
Soit $F \in \mathbb{C}(X)$. On peut toujours écrire F sous la forme $F = \frac{A}{(X-\alpha_1)^{m_1} \cdots (X-\alpha_n)^{m_n}}$, où $\alpha_1, \dots, \alpha_n$ sont les poles de F, $m_1, \dots, m_n \in \mathbb{N}^*$ sont leurs multiplicités et $A \in \mathbb{K}[X]$. Alors il existe un unique $E \in \mathbb{K}[X]$ et une unique famille $(\lambda_{i,j})_{\substack{1 \le i \le n \\ 1 \le j \le m_i}}$ de complexes tels que $F = E + \sum_{i=1}^{n} \Big(\sum_{j=1}^{m_i} \frac{\lambda_{i,j}}{(X-\alpha_i)^j} \Big)$.
Pour $i \in [\![1; n]\!]$, la somme $\sum_{j=1}^{m_i} \frac{\lambda_{i,j}}{(X-a_i)^j}$ est la partie polaire de F relative au pôle α_i.

Méthode : En pratique, pour décomposer une fraction rationnelle F en éléments simples dans $\mathbb{C}(X)$,

1. on commence par l'écrire sous forme irréductible unitaire, $F = \frac{A}{B}$.
2. En effectuant la division euclidienne de A par B, on écrit $F = E + \frac{C}{B}$, où E est la partie entière de F.
   Lorsque $\deg(F) < 0$, il est évident que $E = 0$, donc on peut supprimer cette étape.

3. On scinde B sous la forme $B = \prod_{i=1}^{n}(X-\alpha_i)^{m_i}$.
4. On écrit la DES de $\dfrac{C}{B}$ à l'aide des coefficients indéterminés $\lambda_{i,j}$.
5. On calcule les $\lambda_{i,j}$
   — par des méthodes astucieuses que l'on va étudier,
   — ou bien en réduisant la DES de F, avec coefficients indéterminés, au même dénominateur, égal à B, puis en identifiant les coefficients du numérateur avec ceux de C. C'est une méthode simple en théorie, mais qui entraîne souvent des calculs fastidieux.
   — On peut éventuellement combiner ces deux techniques en évaluant certains coefficients par des techniques à venir, puis en réduisant au même dénominateur pour calculer les coefficients restants.

Exemple. Avec $F(X) = \dfrac{3X^7+(2-i)X^3-1}{X^2(X-i)(X+j)^3}$,
$F = 3X + a + \dfrac{b}{X} + \dfrac{c}{X^2} + \dfrac{d}{X-i} + \dfrac{e}{X+j} + \dfrac{f}{(X+j)^2} + \dfrac{g}{(X+j)^3}$.

Propriété.
Les élements simples de $\mathbb{R}(X)$ sont les fractions rationnelles $\dfrac{a}{(X-b)^m}$, où $a, b \in \mathbb{R}$ et $m \in \mathbb{N}^*$ et les fractions rationnelles $\dfrac{cX+d}{(X^2+eX+f)^p}$, où $c, d, e, f \in \mathbb{R}$ et $p \in \mathbb{N}^*$, avec $e^2 - 4f < 0$.

Théorème de décomposition en éléments simples dans $\mathbb{R}(X)$:
Soit $F \in \mathbb{R}(X)$. On peut toujours écrire F sous la forme irréductible unitaire suivante :

$$F = \frac{A}{\Big(\prod_{i=1}^{n}(X-a_i)^{m_i}\Big) \times \Big(\prod_{i=1}^{p}(X^2+b_iX+c_i)^{k_i}\Big)},$$

où $a_1, \dots, a_n$ sont les poles réels de F, $m_1, \dots, m_n \in \mathbb{N}^*$ sont leurs multiplicités, où pour tout $i \in \{1, \dots, p\}$, $b_i, c_i \in \mathbb{R}$ avec $b_i^2 - 4c_i < 0$ et où $A \in \mathbb{K}[X]$. Alors il existe un unique $E \in \mathbb{K}[X]$ et trois uniques familles $(\lambda_{i,j})_{\substack{1\le i\le n\\ 1\le j\le m_i}}$, $(f_{i,j})_{\substack{1\le i\le p\\ 1\le j\le k_i}}$ et $(g_{i,j})_{\substack{1\le i\le p\\ 1\le j\le k_i}}$ de réels tels que $F = E + \sum_{i=1}^{n}\Big(\sum_{j=1}^{m_i}\dfrac{\lambda_{i,j}}{(X-a_i)^j}\Big) + \sum_{i=1}^{p}\Big(\sum_{j=1}^{k_i}\dfrac{f_{i,j}X+g_{i,j}}{(X^2+b_iX+c_i)^j}\Big)$.

Méthode : En pratique, pour décomposer une fraction rationnelle F en éléments simples dans $\mathbb{R}(X)$,

1. on commence par l'écrire sous forme irréductible unitaire, $F = \dfrac{A}{B}$.

2. En effectuant la division euclidienne de A par B, on écrit $F = E + \dfrac{C}{B}$, où E est la partie entière de F.
   Lorsque $\deg(F) < 0$, il est évident que $E = 0$, donc on peut supprimer cette étape.
3. On scinde B sous la forme $B = \Big(\prod_{i=1}^{n}(X-a_i)^{m_i}\Big) \times \Big(\prod_{i=1}^{p}(X^2+b_iX+c_i)^{k_i}\Big)$.
4. On écrit la DES de $\dfrac{C}{B}$ à l'aide des coefficients indéterminés $\lambda_{i,j}, f_{i,j}, g_{i,j}$.
5. On calcule les $\lambda_{i,j}, f_{i,j}, g_{i,j}$
   — par des méthodes astucieuses que l'on va étudier,
   — ou bien en réduisant la DES de F, avec coefficients indéterminés, au même dénominateur, égal à B, puis en identifiant les coefficients du numérateur avec ceux de C. C'est une méthode simple en théorie, mais qui entraîne souvent des calculs fastidieux.
   — On peut éventuellement combiner ces deux techniques en évaluant certains coefficients par des techniques à venir, puis en réduisant au même dénominateur pour calculer les coefficients restants.

Exemple. La DES dans $\mathbb{R}(X)$ de $F(X) = \dfrac{X-5}{X^3(X-1)(X^2+1)^2}$ est de la forme $F(X) = \dfrac{a}{X} + \dfrac{b}{X^2} + \dfrac{c}{X^3} + \dfrac{d}{X-1} + \dfrac{eX+f}{X^2+1} + \dfrac{gX+h}{(X^2+1)^2}$.

Remarque. On peut aussi décomposer $F \in \mathbb{R}(X)$ en éléments simples dans $\mathbb{C}(X)$ puis en déduire sa DES dans $\mathbb{R}(X)$. En effet, la DES de F dans $\mathbb{C}(X)$ est de la forme $F = E + \sum_{i=1}^{n}\Big(\sum_{j=1}^{m_i}\dfrac{\lambda_{i,j}}{(X-\alpha_i)^j}\Big) + \sum_{i=1}^{p}\Big(\sum_{j=1}^{k_i}\Big[\dfrac{f_{i,j}}{(X-\beta_i)^j} + \dfrac{g_{i,j}}{(X-\overline{\beta_i})^j}\Big]\Big)$, où $E \in \mathbb{R}[X]$ (car obtenu par division euclidienne de deux polynômes à coefficients réels), $\alpha_1, \dots, \alpha_n$ sont des poles réels de F, $m_1, \dots, m_n \in \mathbb{N}^*$ sont leurs multiplicités, $\beta_1, \dots, \beta_k$ sont les poles complexes de F de partie imaginaire strictement positive, $k_1, \dots, k_p \in \mathbb{N}^*$ sont leurs multiplicités, et où les $\lambda_{i,j}, f_{i,j}, g_{i,j}$ sont des complexes. Mais $F \in \mathbb{R}(X)$, donc $F = \overline{F} = E + \sum_{i=1}^{n}\Big(\sum_{j=1}^{m_i}\dfrac{\overline{\lambda_{i,j}}}{(X-\alpha_i)^j}\Big) + \sum_{i=1}^{p}\Big(\sum_{j=1}^{k_i}\Big[\dfrac{\overline{f_{i,j}}}{(X-\overline{\beta_i})^j} + \dfrac{\overline{g_{i,j}}}{(X-\beta_i)^j}\Big]\Big)$. Alors, d'après l'unicité de la DES de F, on a pour tout i, j, $\lambda_{i,j} = \overline{\lambda_{i,j}}$, $g_{i,j} = \overline{f_{i,j}}$, donc $\lambda_{i,j} \in \mathbb{R}$ et $\dfrac{f_{i,j}}{(X-\beta_i)^j} + \dfrac{g_{i,j}}{(X-\overline{\beta_i})^j} = \dfrac{f_{i,j}(X-\overline{\beta_i})^j + \overline{f_{i,j}}(X-\beta_i)^j}{(X^2 - 2\mathrm{Re}(\beta_j)X + |\beta_j|^2)^j}$.
En particulier, pour $j = 1$, $\dfrac{f_{i,1}}{(X-\beta_i)} + \dfrac{g_{i,1}}{(X-\overline{\beta_i})} = \dfrac{2\mathrm{Re}(f_{i,1})X - 2\mathrm{Re}(f_{i,1}\overline{\beta_i})}{X^2 - 2\mathrm{Re}(\beta_j)X + |\beta_j|^2}$, donc lorsque pour tout $i \in \{1, \dots, p\}$, $k_i = 1$, on en déduit la DES de F dans $\mathbb{R}(X)$. Sinon, le calcul devient fastidieux.

Exercice. Pour $n \in \mathbb{N}^*$, on pose $\begin{array}{rccc} f_n : & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \dfrac{1}{x^2+n^2} \end{array}$. La famille $(f_n)_{n\in\mathbb{N}^*}$ est-elle libre ?

Solution : Soit $(\alpha_n)_{n\in\mathbb{N}^*} \in \mathbb{R}^{(\mathbb{N}^*)}$ telle que $\sum_{n\in\mathbb{N}^*} \alpha_n f_n = 0$.

On dispose ainsi de deux décompositions en éléments simples de la fraction nulle dans $\mathbb{R}(X)$. D'après l'unicité d'une telle décomposition, les α_n sont tous nuls. La famille $(f_n)_{n\in\mathbb{N}^*}$ est donc libre.

4.2.6 Quelques techniques de DES

Remarque. La technique des divisions euclidiennes successives est adaptée à la DES de fractions de la forme $\dfrac{P}{Q^m}$, où Q est irréductible.

Propriété. Soit $F \in \mathbb{K}(X)$ et soit $\alpha \in \mathbb{K}$ un pôle de F de multiplicité $m \in \mathbb{N}^*$. Alors le coefficient λ de l'élément simple $\dfrac{1}{(X-\alpha)^m}$ dans la DES de F vérifie

$$\lambda = \widetilde{[(X-\alpha)^m F]}(\alpha).$$

Démonstration.
En regroupant les autres éléments simples de la DES de F, on peut écrire que $F = \dfrac{\lambda}{(X-\alpha)^m} + G$, où G est une fraction rationnelle pour laquelle α est un pôle de multiplicité inférieure à $m-1$. Ainsi, $\widetilde{[(X-\alpha)^m G]}(\alpha) = 0$, donc $\widetilde{[(X-\alpha)^m F]}(\alpha) = \lambda$. □

Exemple. Calculons la DES dans $\mathbb{R}(X)$ de $F = \dfrac{14}{(X-2)(X+5)}$.
La partie entière est nulle.
Il existe $a, b \in \mathbb{R}$ tels que $F = \dfrac{a}{X-2} + \dfrac{b}{X+5}$.
On a $a = [(X-2)F](2) = \left[\dfrac{14}{X+5}\right](2) = 2$
et $b = [(X+5)F](-5) = \left[\dfrac{14}{X-2}\right](-5) = -2$,
donc $F = \dfrac{2}{X-2} - \dfrac{2}{X+5}$.

Exemple. Calculons la DES dans $\mathbb{R}(X)$ de $F = \dfrac{4X}{(X+1)(X-1)^2}$.
La partie entière est nulle.
Il existe $a, b, c \in \mathbb{R}$ tels que $F = \dfrac{a}{X+1} + \dfrac{b}{X-1} + \dfrac{c}{(X-1)^2}$.
On a $a = [(X+1)F](-1) = \left[\dfrac{4X}{(X-1)^2}\right](-1) = -1$

et $c = [(X-1)^2 F](1) = \left[\frac{4X}{X+1}\right](1) = 2$,
donc $F = -\frac{1}{X+1} + \frac{b}{X-1} + \frac{2}{(X-1)^2}$.
De plus $tF(t) \underset{t\to+\infty}{\longrightarrow} 0 = -1 + b$, donc $F = -\frac{1}{X+1} + \frac{1}{X-1} + \frac{2}{(X-1)^2}$.

Remarque. L'utilisation de $\lim_{t\to+\infty}$ est une astuce à connaître.

Remarque. Lorsque F est paire ou impaire, l'unicité de la DES permet de diviser le nombre de coefficients à peu près par 2.

Exemple. DES de $F(X) = \frac{2X^2+6}{(X^2-1)^2}$ dans $\mathbb{R}(X)$.
La partie entière est nulle.
Il existe $a, b, c, d \in \mathbb{R}$ tels que $F = \frac{a}{X-1} + \frac{b}{(X-1)^2} + \frac{c}{X+1} + \frac{d}{(X+1)^2}$.
F est paire, donc $F(X) = F(-X) = \frac{a}{-X-1} + \frac{b}{(X+1)^2} + \frac{c}{-X+1} + \frac{d}{(X-1)^2}$. Alors, d'après l'unicité de la DES de F, $a = -c$ et $b = d$.
De plus, $d = [(X-1)^2 F](1) = \left[\frac{2X^2+6}{(X+1)^2}\right](1) = 2$,
donc $F = \frac{a}{X-1} + \frac{2}{(X-1)^2} + \frac{c}{X+1} + \frac{2}{(X+1)^2}$.
De plus $F(0) = 6 = -a + 2 + c + 2$, donc $2 = c - a = 2c$.
Ainsi, $F = -\frac{1}{X-1} + \frac{2}{(X-1)^2} + \frac{1}{X+1} + \frac{2}{(X+1)^2}$.

Propriété. Soit $F \in \mathbb{K}(X)$ une fraction rationnelle admettant un pôle simple α.
Si $\dfrac{A}{S}$ est un représentant irréductible de F, alors le coefficient λ de l'élément simple $\dfrac{1}{X-\alpha}$ dans la DES de F vérifie

$$\lambda = \frac{\tilde{A}(\alpha)}{\tilde{S}'(\alpha)}.$$

Démonstration.
On sait déjà que $\lambda = \widetilde{[(X-\alpha)F]}(\alpha)$, donc si l'on pose $S = (X-\alpha)Q$, $\lambda = \dfrac{\tilde{A}(\alpha)}{\tilde{Q}(\alpha)}$, mais $S' = Q + (X-\alpha)Q'$, donc $\tilde{S}'(\alpha) = \tilde{Q}(\alpha)$. □

Généralisation : (hors programme) On suppose que $\mathrm{car}(\mathbb{K}) = 0$.
Soit $F \in \mathbb{K}(X)$ une fraction rationnelle et soit $a \in \mathbb{K}$ l'un de ses pôles, dont la multiplicité est notée m.
Si $\dfrac{A}{S}$ est un représentant irréductible de F, alors le coefficient λ de l'élément simple $\dfrac{1}{(X-\alpha)^m}$ dans la DES de F vérifie $\lambda = \dfrac{m!\tilde{A}(\alpha)}{\widetilde{S^{(m)}}(\alpha)}$.

Démonstration.
On sait déjà que $\lambda = \widetilde{[(X-\alpha)^m F]}(\alpha)$, donc si l'on pose $S = (X-\alpha)^m Q$,
$\lambda = \dfrac{\tilde{A}(\alpha)}{\tilde{Q}(\alpha)}$, mais d'après la formule de Leibniz $S^{(m)} = \displaystyle\sum_{k=0}^{m} \binom{m}{k} Q^{(m-k)}[(X-\alpha)^m]^{(k)}$,
donc $\widetilde{S^{(m)}}(\alpha) = m!\tilde{Q}(\alpha)$. □

Exemple. DES dans $\mathbb{C}(X)$ de $F = \dfrac{1}{X^n - 1}$, où $n \in \mathbb{N}^*$.
La partie entière est nulle.
$X^n - 1 = \displaystyle\prod_{k=0}^{n-1}(X - \omega^k)$, où $\omega = e^{2i\frac{\pi}{n}}$,
donc il existe $(\lambda_k)_{0\leq k\leq n-1} \in \mathbb{C}^n$ tel que $F = \displaystyle\sum_{k=0}^{n-1} \frac{\lambda_k}{X-\omega^k}$.
Pour tout $k \in \{0, \dots, n-1\}$, ω^k est un pôle simple de F,
donc $\lambda_k = \dfrac{1}{(X^n-1)'(\omega^k)} = \dfrac{1}{n\omega^{(n-1)k}} = \dfrac{\omega^k}{n}$, donc $F = \dfrac{1}{n}\displaystyle\sum_{k=0}^{n-1} \frac{\omega^k}{X-\omega^k}$.

4.3 Application au calcul intégral

4.3.1 Primitives d'une fraction rationnelle

Si $F \in \mathbb{R}(X)$, pour calculer $\int F(t)dt$,
la méthode générale consiste à décomposer F en éléments simples dans $\mathbb{R}(X)$.
On est ainsi ramené au problème du calcul des primitives des éléments simples de $\mathbb{R}(X)$, c'est-à-dire des fractions rationnelles de la forme $\dfrac{P(X)}{Q^\alpha(X)}$, où Q est un polynôme irréductible de $\mathbb{R}[X]$ et où P est un polynôme de $\mathbb{R}[X]$ tel que $deg(P) < deg(Q)$.

Premier cas. On suppose que $\deg(Q) = 1$.
$\dfrac{P(X)}{Q^\alpha(X)}$ est de la forme $\dfrac{a}{(X+b)^\alpha}$ que l'on sait intégrer, d'après les formules suivantes :

$$\begin{array}{ll} \text{Pour } \alpha \neq 1 & \displaystyle\int \frac{dt}{(t+b)^\alpha} = \frac{1}{1-\alpha}\frac{1}{(t+b)^{\alpha-1}} + k, \\ \text{et} & \displaystyle\int \frac{dt}{t+b} = \ln|t+b| + k. \end{array}$$

Deuxième cas. On suppose que $\deg(Q) = 2$.
$\dfrac{P(X)}{Q^\alpha(X)}$ est de la forme $\dfrac{aX+b}{(X^2+cx+d)^\alpha}$.
On met $X^2 + cX + d$ sous la forme canonique suivante :

$$X^2 + cX + d = (X + \frac{c}{2})^2 + d - \frac{c^2}{4} = (X-p)^2 + q^2,$$

où $p = -\dfrac{c}{2}$ et $q = \sqrt{d - \dfrac{c^2}{4}}$, lequel est bien défini car $X^2 + cX + d$ est irréductible, donc son discriminant est strictement négatif.
On met ensuite le dénominateur sous la forme

$$aX + b = a(X-p) + pa + b.$$

On est ainsi ramené à intégrer $\dfrac{X-p}{((X-p)^2+q^2)^\alpha}$ et $\dfrac{1}{((X-p)^2+q^2)^\alpha}$.

- Pour la première fraction,

$$\begin{aligned} \int \frac{(t-p)\,dt}{((t-p)^2+q^2)^\alpha} &= \int \frac{1}{2}\frac{d((t-p)^2+q^2))}{dt}((t-p)^2+q^2))^{-\alpha}\,dt \\ &= \begin{cases} \dfrac{1}{2(1-\alpha)}((t-p)^2+q^2)^{1-\alpha} + k, & \text{si } \alpha \neq 1 \\ \dfrac{1}{2}\ln|(t-p)^2+q^2| + k, & \text{si } \alpha = 1 \end{cases}. \end{aligned}$$

- Pour la seconde fraction, en posant $Y = \dfrac{X-p}{q}$, il faut intégrer $F_\alpha(Y) = \dfrac{1}{(Y^2+1)^\alpha}$.

Première méthode. Pour $\alpha \in \{1,2,3\}$.
On pose $t = \tan u$. C'est possible car l'application $u \longmapsto \tan u$ est C^1 et bijective de $]-\frac{\pi}{2}, \frac{\pi}{2}[$ dans $\mathbb{R}$. On obtient

$$\int F_\alpha(t)dt = \int (\cos u)^{2(\alpha-1)} du,$$

et on finit le calcul en linéarisant $(\cos u)^{2(\alpha-1)}$.

Deuxième méthode. Pour $\alpha \geq 4$.
Par intégration par parties,

$$\begin{aligned}\int F_\alpha(t)dt = \int \frac{dt}{(1+t^2)^\alpha} &= \frac{t}{(1+t^2)^\alpha} - \int \frac{t(-\alpha)\times 2t}{(1+t^2)^{\alpha+1}}dt \\ &= \frac{t}{(1+t^2)^\alpha} + 2\alpha \int (F_\alpha(t) - F_{\alpha+1}(t))dt.\end{aligned}$$

On a donc la relation de récurrence suivante :

$$2\alpha \int F_{\alpha+1}(t)dt = \frac{t}{(1+t^2)^\alpha} + (2\alpha-1)\int F_\alpha(t)dt.$$

Exemple. Calcul de $\displaystyle\int \frac{1-t}{(t^2+t+1)^2}dt$.

$$\begin{aligned}\int \frac{1-t}{(t^2+t+1)^2}dt &= \int \frac{-(t+\frac{1}{2})+\frac{3}{2}}{\left((t+\frac{1}{2})^2+\frac{3}{4}\right)^2}dt \\ &= \frac{1}{2(t^2+t+1)} + \frac{3}{2}\int \frac{dt}{\left((t+\frac{1}{2})^2+\frac{3}{4}\right)^2}.\end{aligned}$$

On pose $t + \dfrac{1}{2} = \sqrt{\dfrac{3}{4}}\tan u$, ce qui est possible car $u \longmapsto -\frac{1}{2} + \sqrt{\frac{3}{4}}\tan u$ est C^1 et bijective de $]-\frac{\pi}{2}, \frac{\pi}{2}[$ dans $\mathbb{R}$. On obtient

$$\begin{aligned}\int \frac{dt}{\left((t+\frac{1}{2})^2+\frac{3}{4}\right)^2} &= \int \frac{\frac{\sqrt{3}}{2}\frac{du}{\cos^2 u}}{\frac{9}{16}(\tan^2 u+1)^2} &&= \frac{8}{3\sqrt{3}}\int \cos^2 u\ du \\ &= \frac{8}{3\sqrt{3}}\int \frac{1+\cos(2u)}{2}\ du &&= \frac{8}{3\sqrt{3}}(\frac{u}{2} + \frac{\sin(2u)}{4}) + k.\end{aligned}$$

Or $u = \arctan\Big(\dfrac{2t+1}{\sqrt{3}}\Big)$ et $\sin(2u) = \dfrac{2T}{1+T^2}$ où $T = \tan u = \dfrac{2t+1}{\sqrt{3}}$, donc

$$\begin{aligned}\int \frac{dt}{\left((t+\frac{1}{2})^2+\frac{3}{4}\right)^2} &= \frac{4}{3\sqrt{3}}\left(\arctan\Big(\frac{2t+1}{\sqrt{3}}\Big) + \frac{\frac{2t+1}{\sqrt{3}}}{1+\frac{4t^2+4t+1}{3}}\right) + k \\ &= \frac{4}{3\sqrt{3}}\left(\arctan\Big(\frac{2t+1}{\sqrt{3}}\Big) + \frac{\sqrt{3}(2t+1)}{4(t^2+t+1)}\right) + k,\end{aligned}$$

donc

$$\begin{aligned}\int \frac{1-t}{(t^2+t+1)^2}dt &= \frac{2}{\sqrt{3}}\arctan\Big(\frac{2t+1}{\sqrt{3}}\Big) + \frac{2t+1}{2(t^2+t+1)} + \frac{1}{2(t^2+t+1)} + k\\ &= \frac{2}{\sqrt{3}}\arctan\Big(\frac{2t+1}{\sqrt{3}}\Big) + \frac{t+1}{t^2+t+1} + k.\end{aligned}$$

4.3.2 Fonctions rationnelles de sin et cos : hors programme

On pose $\mathbb{R}(X,Y) = (\mathbb{R}(X))(Y)$ l'ensemble des fractions rationnelles à coefficients réels à deux variables. Par exemple $\dfrac{XY - Y^3 + 2X^2Y}{X^4 + 8XY^3} \in \mathbb{R}(X,Y)$.
Soit $R \in \mathbb{R}(X,Y)$. on veut calculer $\int R(\sin t, \cos t)\ dt$.

Cas particulier. $\int \sin^p t \cos^q t\ dt$, avec p et q pairs. C'est le seul cas où on linéarise.

Exemple. Calcul de $\int \cos^4 t \sin^2 t\ dt$.

$$\begin{aligned}\cos^4 t \sin^2 t &= -\frac{1}{2^6}(e^{4it} + e^{-4it} + 4e^{2it} + 4e^{-2it} + 6)(e^{2it} - 2 + e^{-2it})\\ &= -\frac{1}{2^5}(\cos(6t) + 2\cos(4t) - \cos(2t) - 2),\end{aligned}$$

donc

$$\int \cos^4 t \sin^2 t\ dt = \frac{t}{16} + \frac{\sin(2t)}{64} - \frac{\sin(4t)}{64} - \frac{\sin(6t)}{192} + k.$$

Cas général. On pose $u = \tan\dfrac{t}{2}$. On est ainsi ramené à la recherche des primitives d'une fraction rationnelle. En effet,

$$\cos t = \frac{1-u^2}{1+u^2}, \quad \sin t = \frac{2u}{1+u^2} \quad \text{et } dt = \frac{2du}{1+u^2}.$$

Pour effectuer un tel changement de variable, il faut, pour $m \in \mathbb{Z}$ fixé, se limiter à la recherche des primitives sur l'intervalle $](2m-1)\pi, (2m+1)\pi[$, ou même à des sous-intervalles de cet intervalle s'il n'est pas inclus dans le domaine de définition de $t \longmapsto R(\sin t, \cos t)$.
L'application de changement de variable est $u \longmapsto 2\arctan u + 2m\pi$. Elle est bien C^1 et bijective de $\mathbb{R}$ dans $](2m-1)\pi, (2m+1)\pi[$.
Si le domaine de définition le permet, pour obtenir les primitives sur des intervalles plus larges, il faudra raccorder par continuité.

Exemple. Calcul de $\displaystyle\int \frac{dt}{2+\sin t}$.
Soit $m \in \mathbb{Z}$. On recherche dans un premier temps les primitives sur l'intervalle

$I_m =](2m-1)\pi, (2m+1)\pi[$. Posons $t = 2\arctan u + 2m\pi$. On obtient

$$\int \frac{dt}{2+\sin t} = \int \frac{2du}{(1+u^2)(2+\frac{2u}{1+u^2})} = \int \frac{du}{u^2+u+1}$$
$$= \int \frac{du}{(u+\frac{1}{2})^2+\frac{3}{4}} = \int \frac{\frac{\sqrt{3}}{2}\frac{dx}{\cos^2 x}}{\frac{3}{4}(\cos x)^{-2}},$$

en posant $u + \frac{1}{2} = \sqrt{\frac{3}{4}}\tan x$, ce qui est possible car $x \longmapsto -\frac{1}{2} + \sqrt{\frac{3}{4}}\tan x$ est C^1 et bijective de $]-\frac{\pi}{2}, \frac{\pi}{2}[$ dans $\mathbb{R}$. Ainsi

$$\int \frac{dt}{2+\sin t} = \frac{2}{\sqrt{3}}x + k = \frac{2}{\sqrt{3}}\arctan\left(\frac{2u+1}{\sqrt{3}}\right) + k.$$

Ainsi

$$\int \frac{dt}{2+\sin t} = \frac{2}{\sqrt{3}}\arctan\left(\frac{2\tan(\frac{t}{2})+1}{\sqrt{3}}\right) + k_m, t \in I_m.$$

$f : t \longmapsto \dfrac{1}{2+\sin t}$ étant définie et continue sur $\mathbb{R}$, elle admet une primitive F sur $\mathbb{R}$ telle que $F(0) = \dfrac{2}{\sqrt{3}}\arctan\dfrac{1}{\sqrt{3}} = \dfrac{2}{\sqrt{3}}\dfrac{\pi}{6} = \dfrac{\pi}{3\sqrt{3}}$.
Soit $m \in \mathbb{Z}$. $F|_{I_m}$ est une primitive de $f|_{I_m}$, donc d'après le calcul précédent, il existe $k_m \in \mathbb{R}$ tel que

$$\forall t \in I_m \quad F(t) = \frac{2}{\sqrt{3}}\arctan\left(\frac{2\tan(\frac{t}{2})+1}{\sqrt{3}}\right) + k_m.$$

F étant continue en $(2m-1)\pi$, $F((2m-1)\pi) = \lim\limits_{t \overset{>}{\to} (2m-1)\pi} F(t) = -\dfrac{\pi}{\sqrt{3}} + k_m$ et

$F((2m-1)\pi) = \lim\limits_{t \overset{<}{\to} (2m-1)\pi} F(t) = \dfrac{\pi}{\sqrt{3}} + k_{m-1}$. Donc $k_m = k_{m-1} + \dfrac{2\pi}{\sqrt{3}}$. De plus, comme on a choisi $F(0) = \dfrac{2}{\sqrt{3}}\arctan\dfrac{1}{\sqrt{3}}$, $k_0 = 0$. Ainsi,

$$\forall m \in \mathbb{Z} \quad k_m = \frac{2m\pi}{\sqrt{3}}.$$

$$\text{Ainsi } F(t) = \begin{cases} \dfrac{2}{\sqrt{3}}\arctan\left(\dfrac{2\tan(\frac{t}{2})+1}{\sqrt{3}}\right) + \dfrac{2m\pi}{\sqrt{3}} & \text{si } t \in \mathbb{R} \setminus (\pi + 2\pi\mathbb{Z}) \\ \dfrac{(2m+1)\pi}{\sqrt{3}} & \text{si } t = (2m+1)\pi \end{cases}.$$

et $\displaystyle\int \frac{dt}{2+\sin t} = F(t) + k, \quad t \in \mathbb{R}$.

Les règles de Bioche.
Sous certaines conditions, on peut utiliser un changement de variable souvent plus intéressant que celui du cas général.
Notons $f : t \longmapsto R(\sin t, \cos t)$.

Si $f(-t)d(-t) = f(t)dt$,	on posera $x = \cos t$	(On a $\cos(-t) = \cos t$) ,
Si $f(\pi - t)d(\pi - t) = f(t)dt$,	on posera $x = \sin t$	(On a $\sin(\pi - t) = \sin t$) ,
Si $f(\pi + t)d(\pi + t) = f(t)dt$,	on posera $x = \tan t$	(On a $\tan(\pi + t) = \tan t$).

Si deux des trois relations précédentes sont vérifiées, alors la troisième l'est aussi et dans ce cas, il sera intéressant de poser $x = \sin^2 t$ ou $x = \cos(2t)$ (ces deux fonctions de t vérifiant les trois stabilités simultanément).

Exemple. Calcul de $\displaystyle\int \cos^4 t \sin^3 t \; dt$.

$$\int \cos^4 t \sin^3 t \; dt = \int -\frac{d(\cos t)}{dt} \cos^4 t (1 - \cos^2 t) \; dt = \int (x^2 - 1)x^4 \; dx,$$

en posant $x = \cos t$, ce qui est possible car cos est une application C^1. Ainsi

$$\int \cos^4 t \sin^3 t \; dt = \frac{x^7}{7} - \frac{x^5}{5} + k = \frac{\cos^7 t}{7} - \frac{\cos^5 t}{5} + k, \quad t \in \mathbb{R}.$$

Exemple. Calcul de $\displaystyle\int \frac{dt}{\sin t}$.
Cette primitive est sur le formulaire. Elle est connue et ne doit pas être recalculée en concours. Nous allons le faire à titre d'exemple.
L'application à intégrer est définie et continue sur $\mathbb{R} \setminus \pi\mathbb{Z}$. On recherche donc les primitives sur l'intervalle $I_m =]m\pi, (m+1)\pi[$ où $m \in \mathbb{Z}$ est fixé.

$$\int \frac{dt}{\sin t} = \int -\frac{d(\cos t)}{dt} \frac{dt}{1 - \cos^2 t} = \int \frac{dx}{x^2 - 1},$$

en posant $x = \cos t$, ce qui est possible car cos est une application de classe C^1. Donc

$$\begin{aligned} \int \frac{dt}{\sin t} &= \frac{1}{2} \ln \left| \frac{x-1}{x+1} \right| + k & &= \frac{1}{2} \ln \left| \frac{\cos t - 1}{\cos t + 1} \right| + k \\ &= \frac{1}{2} \ln \left(\frac{\sin^2 (\frac{t}{2})}{\cos^2 (\frac{t}{2})} \right) + k & &= \ln |\tan (\frac{t}{2})| + k. \end{aligned}$$

Bien entendu, connaissant le résultat, il est en fait plus judicieux de poser $x = \tan (\frac{t}{2})$ (cette fonction de t est définie et C^1 sur I_m). On obtient

$$\int \frac{dt}{\sin t} = \int \frac{d\left(\tan (\frac{t}{2})\right)}{dt} \frac{dt}{\frac{1}{2}\left(1 + \tan^2 (\frac{t}{2})\right) \frac{2 \tan \left(\frac{t}{2}\right)}{\left(1 + \tan^2 \left(\frac{t}{2}\right)\right)}}.$$

Donc
$$\int \frac{dt}{\sin t} = \int \frac{dx}{x} = \ln|x| + k = \ln|\tan(\frac{t}{2})| + k.$$
On voit sur cet exemple que les règles de Bioche ne fournissent pas toujours le changement de variable le plus approprié.

Exemple. Calcul de $\displaystyle\int \frac{\cos^3 t}{\sin^5 t}\, dt$.
L'application à intégrer est définie et continue sur $\mathbb{R} \setminus \pi\mathbb{Z}$. On recherche donc les primitives sur l'intervalle $I_m =]m\pi, (m+1)\pi[$ où $m \in \mathbb{Z}$ est fixé.
Par application des règles de Bioche, on pose $x = \sin^2 t$ (l'application de t correspondante est bien de classe C^1). Ainsi

$$\begin{array}{lll}
\displaystyle\int \frac{\cos^3 t}{\sin^5 t}\, dt & = \displaystyle\int \frac{d(\sin^2 t)}{dt}\frac{1}{2\sin t\cos t}\frac{\cos^3 t}{\sin^5 t}\, dt & = \displaystyle\int \frac{d(\sin^2 t)}{dt}\frac{1-\sin^2 t}{2\sin^6 t}\, dt \\
& = \displaystyle\int \frac{1-x}{2x^3}\, dx & = -\frac{1}{4x^2} + \frac{1}{2x} + k \\
& = -\frac{1}{4\sin^4 t} + \frac{1}{2\sin^2 t} + k & = \frac{2\sin^2 t - 1 - \sin^4 t}{4\sin^4 t} + k + \frac{1}{4} \\
& = -\frac{\operatorname{cotan}^4 t}{4} + k'. &
\end{array}$$

4.3.3 Fonctions rationnelles en sh et ch : hors programme

On veut calculer $\int R(\mathrm{sh}t, \mathrm{ch}t)\, dt$ où $R(X,Y) \in \mathbb{R}(X,Y)$.
La méthode consiste à regarder quel procédé serait utilisé
pour le calcul de $\int R(\sin t, \cos t)\, dt$ et à le transposer en trigonométrie hyperbolique.

Ainsi, dans le cas général, on pose $u = \mathrm{th}\left(\frac{t}{2}\right)$.
On dispose des formules suivantes :
$$\mathrm{ch}t = \frac{1+u^2}{1-u^2}, \quad \mathrm{sh}t = \frac{2u}{1-u^2} \quad \text{et } dt = \frac{2du}{1-u^2},$$
ce qui nous ramène à l'intégration d'une fraction rationnelle.
On peut aussi poser $x = e^t$. Ce changement de variable ramène le calcul de $\int S(e^t)\, dt$ où S est une fraction rationnelle quelconque au calcul des primitives d'une fraction rationnelle.

Exemple. Calcul de $\displaystyle\int \frac{dt}{\mathrm{ch}t}$.
Cette primitive fait aussi partie du formulaire. Démontrons la validité de la formule qu'il propose.
L'application des règles de Bioche nous conduit à poser $x = sht$, ce qui est possible car sh est C^1. On obtient
$$\begin{array}{ll}
\displaystyle\int \frac{dt}{\mathrm{ch}t} & = \displaystyle\int \frac{d(\mathrm{sh}t)}{dt}\frac{dt}{1+\mathrm{sh}^2 t} \quad = \displaystyle\int \frac{dx}{1+x^2} \\
& = \arctan(x) + k \qquad = \arctan(\mathrm{sh}t) + k.
\end{array}$$

Cela ne correspond pas exactement au formulaire.
Posons $\theta = \arctan(e^t)$ et $\theta' = \arctan(e^{-t}) = \dfrac{\pi}{2} - \theta$.

$$\begin{array}{lll} \arctan(\mathrm{sh}t) & = \arctan\left(\dfrac{e^t - e^{-t}}{2}\right) & = \arctan\left(\dfrac{\tan\theta - \tan\theta'}{1 + \tan\theta\tan\theta'}\right) \\ & = \arctan(\tan(\theta - \theta')) & = \theta - \theta' - h\pi, \text{ où } h \in \mathbb{Z} \\ & = 2\arctan(e^t) - \dfrac{\pi}{2} - h\pi. & \end{array}$$

Donc on retrouve bien que

$$\int \frac{dt}{\mathrm{ch}t} = 2\arctan(e^t) + k'.$$

En fait, connaissant la formule, il est plus judicieux de poser $x = e^t$.

$$\begin{array}{lll} \displaystyle\int \frac{dt}{cht} & = \displaystyle\int \frac{d(e^t)}{dt}\frac{dt}{e^t\frac{e^t+e^{-t}}{2}} & = \displaystyle\int \frac{2\ dx}{x^2+1} \\ & = 2\arctan(x) + k & = 2\arctan(e^t) + k. \end{array}$$