Polynômes et fractions rationnelles

Cornou Jean-Louis

27 février 2023

On poursuit l'illustration des notions d'anneaux et de corps avec les polynômes et les fractions rationnelles. Dans tout ce qui suit, $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$ (typiquement $\mathbb{R}$ ou $\mathbb{C}$). On pourra généraliser tout ce chapitre, hormis les techniques de dérivation, à un corps quelconque. Les applications de ce champ sont innombrables dans tous les champs des mathématiques. Par exemple, la construction des polynômes repose sur les notions de corps. En retour, ce sont les propriétés des polynômes qui sont centrales dans la compréhension des corps finis.

1 Anneau des polynômes à une indéterminée.

Les polynômes sont introduits dans le secondaire via les fonctions polynomiales. Ces deux notions sont en réalité distinctes et la notion de polynôme est plus abstraite, intrinsèquement liée à la suite de ses coefficients. Prenons le cas du corps $\mathbb{K}$ à deux éléments $\{0,1\}$. Sur ce corps, le polynôme $X^2 - X$ est un polynôme non nul de degré 2. Pourtant, $0^2 = 0$ et $1^2 = 1$, donc sa fonction polynomiale est nulle. Rappelons que $\mathbb{K}^{\mathbb{N}}$ désigne l'ensemble des applications de $\mathbb{N}$ dans $\mathbb{K}$, i.e des suites à valeurs dans $\mathbb{K}$.

1.1 Opérations dans $\mathbb{K}[X]$.

Définition 1 *L'ensemble $\mathbb{K}^{\mathbb{N}}$ est muni des opérations suivantes :*

— *Une multiplication externe $\mathbb{K} \times \mathbb{K}^{\mathbb{N}} \to \mathbb{K}^{\mathbb{N}}, (\lambda, u) \mapsto (\lambda u)$ avec*

$$\forall n \in \mathbb{N}, (\lambda u)_n = \lambda u_n$$

— *Une addition interne $\mathbb{K}^{\mathbb{N}} \times \mathbb{K}^{\mathbb{N}}, (u, v) \mapsto (u + v)$ avec*

$$\forall n \in \mathbb{N}, (u + v)_n = u_n + v_n$$

Propriété 1 *L'ensemble $(\mathbb{K}^{\mathbb{N}}, +)$ est un groupe commutatif.*

Démonstration. — L'addition telle que définie plus haut est bien une loi de composition interne.

— Associativité : soit $(u, v, w) \in (\mathbb{K}^{\mathbb{N}})^3$ et $n \in \mathbb{N}$. Comme l'addition est associative dans $\mathbb{K}$,

$$((u + v) + w)_n = (u + v)_n + w_n = (u_n + v_n) + w_n = u_n + (v_n + w_n) = u_n + (v + w)_n = (u + (v + w))_n$$

Comme cela est vrai pour tout entier n, on a l'égalité des suites $(u + v) + w = u + (v + w)$.

— Neutre : On pose 0 la suite nulle. Soit $u \in \mathbb{K}^{\mathbb{N}}$. Alors

$$\forall n \in \mathbb{N}, 0 + u_n = u_n + 0 = u_n$$

— Symétrique : Soit $u \in \mathbb{K}^{\mathbb{N}}$. On pose $v = -u$. Alors

$$\forall n \in \mathbb{N}, v_n + u_n = u_n + v_n = 0$$

☞ **Remarque**
La multiplication externe fournit une structure d'espace vectoriel comme dans le cas des matrices. More on that later. D'autre part, il existe une multiplication interne « naïve » sur $\mathbb{K}^{\mathbb{N}}$, mais nous allons en définir une autre plus adaptée au cadre des polynômes.

Définition 2 *Soit $(u,v)\in(\mathbb{K}^{\mathbb{N}})^2$. On définit la suite $w:\mathbb{N}\to\mathbb{K}, n\mapsto\sum_{k=0}^{n}u_kv_{n-k}$. Elle est appelée produit de Cauchy de u et v, notée uv.*

Propriété 2 *La structure $(\mathrm{K}^{\mathbb{N}},+,\times)$ est un anneau commutatif.*

Démonstration. — On a déjà prouvé que $(\mathrm{K}^{\mathbb{N}},+)$ est un groupe commutatif.

— Associativité du produit de Cauchy : Soit $(u,v,w)\in(\mathbb{K}^{\mathbb{N}})^3$ et $n\in\mathbb{N}$. L'associativité et la distributivité du produit dans $\mathbb{K}$ permet d'écrire :

$$((uv)w)_n=\sum_{k=0}^{n}(uv)_kwn-k=\sum_{k=0}^{n}\sum_{l=0}^{k}u_lv_{k-l}w_{n-k}=\sum_{0\leq l\leq k\leq n}u_lv_{k-l}w_{n-k}$$

On a affaire à une somme triangulaire que l'on inverse comme suit :

$$((uv)w)_n=\sum_{l=0}^{n}\sum_{k=l}^{n}u_lv_{k-l}w_{n-k}=\sum_{l=0}^{n}u_l\sum_{k=l}^{n}v_{k-l}w_{n-k}$$

On effectue le changement d'indice $m=k-l$ dans cette dernière somme. On a alors

$$((uv)w)_n=\sum_{l=0}^{n}u_l\sum_{m=0}^{n-l}v_mw_{n-l-m}=\sum_{l=0}^{n}u_l(vw)_{n-l}=(u(vw))_n$$

— Commutativité : Soit $(u,v)\in(\mathbb{K}^{\mathbb{N}})^2$ et $n\in\mathbb{N}$. Le changement d'indice $l=n-k$ dans le produit de Cauchy, la commutativité de l'addition et du produit dans $\mathbb{K}$ entraînent

$$(uv)_n=\sum_{k=0}^{n}u_kv_{n-k}=\sum_{l=0}^{n}v_lu_{n-l}=(vu)_n$$

— Distributivité : Soit $(u,v,w)\in\left(\mathbb{K}^{\mathbb{N}}\right)^3$ et $n\in\mathbb{N}$.

$$(u(v+w))_n=\sum_{k=0}^{n}u_k(v+w)_{n-k}=\sum_{k=0}^{n}u_kv_{n-k}+\sum_{k=0}^{n}u_kw_{n-k}=(uv)_n+(uw)_n$$

Cela entraîne la distributivité à gauche. Celle à droite en découle par commutativité.

— Neutre : On pose $e:n\mapsto\delta_{n,0}$ la suite qui vaut 1 en 0 et 0 sinon. Vérifions qu'il s'agit du neutre pour le produit de Cauchy. Soit $u\in\mathbb{K}^{\mathbb{N}}$ et $n\in\mathbb{N}$.

$$(ue)_n=\sum_{k=0}^{n}u_k\delta_{n-k,0}=u_n$$

On en déduit que $eu=u$ par commutativité.

Passons à l'anneau des polynômes proprement dit :

Définition 3 *Soit $u\in\mathbb{K}^{\mathbb{N}}$ une suite à valeurs dans $\mathbb{K}$. On dit que u est à support fini (ou presque nulle) si elle stationne en 0, i.e*

$$\exists\mathrm{N}\in\mathbb{N},\forall n\geq\mathrm{N},u_n=0$$

Propriété 3 *L'ensemble des suites à support fini, noté $\mathbb{K}^{(\mathbb{N})}$, est stable par combinaison linéaire. C'est un sous-anneau de $(\mathbb{K}^{\mathbb{N}},+,\times)$.*

Démonstration. — Soit $(u,v)\in(\mathbb{K}^{(\mathbb{N})})^2,(\lambda,\mu)\in\mathbb{K}^2$. On note N_u un rang tel que $\forall n\geq\mathrm{N}_i,u_n=0$ et N_v un rang tel que $\forall n\geq\mathrm{N}_v,v_n=0$. Alors, on pose $\mathrm{N}=\max(\mathrm{N}_u,\mathrm{N}_v)$ ce qui entraîne $\forall n\geq\mathrm{N},(\lambda u+\mu v)_n=\lambda u_n+\mu v_n=0$.

— Rappelons que le neutre de $\mathbb{K}^{\mathbb{N}}$ est la suite $e:n\mapsto\delta_{n,0}$. Cette suite est à support fini puisque $\forall n\geq1,e_n=0$.

— D'après la stabilité par combinaison linéaire, on a en particulier $\forall(u,v)\in(\mathbb{K}^{\mathbb{N}})^2,u-v\in\mathbb{K}^{\mathbb{N}}$, ce qui en fait un sous-groupe de $(\mathbb{K}^{\mathbb{N}},+)$.

— Stabilité par produit : soit $(u,v)\in(\mathbb{K}^{\mathbb{N}})^2$. On note N_u un rang tel que $\forall n\geq\mathrm{N}_u,u_n=0$ et N_v un rang tel que $\forall n\geq\mathrm{N}_v,v_n=0$. On pose alors $\mathrm{N}=\mathrm{N}_u+\mathrm{N}_v$. Soit $n\geq\mathrm{N}$.

$$(uv)_n=\sum_{k=0}^{n}u_kv_{n-k}$$

Or pour tout entier k dans $[\![0,n]\!]$, $k\geq\mathrm{N}_u$ ou $n-k\geq\mathrm{N}_v$ (sinon, $n<\mathrm{N}_u+\mathrm{N}_v$). Par conséquent, $u_k=0$ ou $v_{n-k}0$ et tous les termes de la somme sont nuls et la suite uv est à support fini.

Définition 4 *On appelle indéterminée* X *la suite définie par* $\mathbb{N} \to \mathbb{K}, n \to \delta_{n,1}$*, i.e la suite qui vaut* 1 *en* 1 *et* 0 *partout ailleurs.*

Notation
On note 1 *le neutre du produit de Cauchy et on convient que* $X^0 = 1$*.*

Propriété 4 *Pour tout entier* m*,* $X^m : n \mapsto \delta_{n,m}$*. Pour toute suite à support fini* u*,*

$$u = \sum_{n=0}^{+\infty} u_n X^n$$

Démonstration. On prouve la première propriété par récurrence sur m. Pour $m = 0$, il s'agit d'une convention. Pour $m = 1$, il s'agit de la définition de X. Soit m un entier naturel tel que $X^m = n :\mapsto \delta_{n,m}$. Soit n un entier naturel, d'après l'hypothèse de récurrence,

$$(X^{m+1})_n = (X^m X)_n = \sum_{k=0}^{n} (X^m)_k X_{n-k} = \sum_{k=0}^{n} \delta_{k,m}\delta_{n-k,1} = \delta_{n-1,m} = \delta_{n,m+1}$$

Soit N un rang tel que $\forall n \geq N, u_n = 0$. Alors, il est clair que $\forall n \in \mathbb{N}, u_n = \sum_{k=0}^{N} u_k \delta_{k,n} = \sum_{k=0}^{N} u_k (X^k)_n$. Ainsi, on a l'égalité

$$u = \sum_{n=0}^{N} u_n X^n$$

Notation
On note dorénavant $\mathbb{K}[X]$ *cette structure. Ses éléments sont appelés polynômes à coefficients dans* $\mathbb{K}$ *à une indéterminée, typiquement notés* $P, Q, R, \ldots$*.*

☞ **Remarque**
Cette façon de noter les polynômes a l'avantage de faire apparaître les règles sur les puissances comme d'habitude, $X^r X^s = X^{r+s}$ *pour tous entiers naturels* r *et* s*.*

Définition 5 *Cette construction assure que pour tout polynôme* P*, il existe une unique suite à support fini* $(p_k)_{k\in\mathbb{N}}$ *telle que* $P = \sum_{k=0}^{+\infty} p_k X^k$*. En réalité, cette suite est le polynôme. On les appelle les coefficients de* P*.*

Définition 6 *Soit* $(P, Q) \in \mathbb{K}[X]^2$*. On note* $P = \sum_{k=0}^{n} p_k X^k$*. On définit alors la composée* $P \circ Q$ *comme le polynôme* $\sum_{k=0}^{n} p_k Q^k$

☞ **Remarque**
Cette définition est légitime, puisqu'il s'agit d'une combinaison linéaire de puissances d'un polynôme.

1.2 Degré

Définition 7 *Soit* $P \in \mathbb{K}[X]$*. Si* P *est non nul de coefficients* $(p_k)_{k\in\mathbb{N}}$*, l'entier* $\max\{n \in \mathbb{N}, p_n \neq 0\}$ *est appelé le degré de* P*. Si* $P = 0$*, on convient que son degré vaut* $-\infty$*.*

Notation
Il est noté deg(P) *ou* $d^\circ P$ *ou encore* d(P)*.*

Définition 8 *Soit* $P \in \mathbb{K}[X]$ *non nul. Alors son coefficient d'indice* d(P) *est appelé coefficient dominant de* P*. Si ce coefficient dominant vaut* 1*, on dit que* P *est un polynôme unitaire.*

Propriété 5 *Soit* $(P, Q) \in \mathbb{K}[X]^2$*. Alors*

- $d(P + Q) \leq \max(d(P), d(Q))$*. Il y a égalité si* $d(P) \neq d(Q)$*.*
- $d(PQ) = d(P) + d(Q)$*.*
- $d(P \circ Q) = d(P)d(Q)$*.*

Démonstration. Notons $P = \sum_{k=0}^{d(P)} p_k X^k$ et $Q = \sum_{k=0}^{d(Q)} q_k X^k$.

— Si l'un des polynômes est nul, l'inégalité est respectée. Sinon

$$P+Q=\sum_{k=0}^{\max(d(P),d(Q))}(p_k+q_k)X^k$$

Ainsi, pour le coefficient d'indice $\max(d(P),d(Q))+1$ de $P+Q$ est nul, donc son degré est inférieur ou égal à $\max(d(P),d(Q))$. Supposons que $d(P)\neq d(Q)$. On se place dans le cas où $d(P)>d(Q)$. Ainsi, le coefficient dominant $p_{d(P)}$ est non nul, tandis que $q_{d(P)}$ est nul, ainsi le coefficient de degré $d(P)$ de $P+Q$ vaut $p_{d(P)}$ et est non nul. Par conséquent, le degré de $P+Q$ vaut $d(P)=\max(d(P),d(Q))$. L'autre cas est symétrique.

⚠ **Attention**
Pour tout entier naturel n, X^n et $-X^n$ sont de degré n, mais $X^n-X^n=0$ est de degré $-\infty$.

— Si l'un des polynômes est nul, l'égalité est assurée avec la convention $n+(-\infty)=-\infty$. Sinon

$$PQ=\left(\sum_{k=0}^{d(P)}p_kX^k\right)\left(\sum_{m=0}^{d(Q)}q_mX^m\right)=\sum_{k=0}^{d(P)}\sum_{m=0}^{d(Q)}p_kq_mX^{m+k}$$

On regroupe alors les termes de même degré

$$PQ=\sum_{n=0}^{d(P)+d(Q)}\left(\sum_{\substack{m+k=n\\0\leq k\leq d(P)\\0\leq m\leq d(Q)}}p_kq_m\right)X^n$$

En particulier, le coefficient de degré $d(P)+d(Q)+1$ est nul, tandis que le coefficient de degré $d(P)+d(Q)$ vaut $p_{d(P)}q_{d(Q)}$ donc est non nul. Ainsi, $d(PQ)=d(P)+d(Q)$.

— Si l'un des polynômes est nul, on a égalité. Sinon, on écrit

$$P\circ Q=\sum_{k=0}^{d(P)}p_kQ^k$$

Or pour tout k dans $[\![0,d(P)]\!]$, $d(Q^k)=kd(Q)$ en généralisant l'égalité précédente par récurrence. Comme Q est non nul, tous ces degrés sont différents, donc la somme est du degré de $p_{d(P)}Q^{d(P)}$, puisque $p_{d(P)}$ est non nul. Comme $d(Q^{d(P)})=d(P)d(Q)$, le résultat s'ensuit.

Propriété 6 *L'anneau $\mathbb{K}[X]$ est intègre.*

Démonstration. On a déjà établi que cet anneau est commutatif. Soit $(P,Q)\in\mathbb{K}[X]^2$. On suppose que $PQ=0$ et $P\neq 0$. Alors, $d(PQ)=d(P)+d(Q)=-\infty$. Comme $d(P)\in\mathbb{N}$, on en déduit que $d(Q)=-\infty$, donc $Q=0$.

Définition 9 *Soit n un entier naturel. On note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré au plus n.*

Propriété 7 *Pour tout entier naturel n, l'espace $\mathbb{K}_n[X]$ est stable par combinaison linéaire.*

Démonstration. Soit $(P,Q)\in(\mathbb{K}_n[X])^2$, $(\lambda,\mu)\in\mathbb{K}^2$. Alors

$$d(\lambda P+\lambda d(Q))\leq\max(d(\lambda P),d(\mu Q))\leq\max(d(\lambda)+d(P),d(\mu)+d(Q))=\max(d(P),d(Q))\leq n$$

⚠ **Attention**
Pour $n\neq 0$, ce n'est pas un sous-anneau.

Propriété 8 *L'ensemble des éléments inversibles de $\mathbb{K}[X]$ est l'ensemble des polynômes de degré 0. C'est un groupe isomorphe à $\mathbb{K}^*$.*

Démonstration. Soit P un élément inversible de $\mathbb{K}[X]$. Alors il existe un polynôme Q tel que $PQ=1$. Alors $d(P)+d(Q)=d(1)=0$. D'autre part, P et Q ne sont pas nuls, donc $d(P)$ et $d(Q)$ sont des entiers. Par conséquent, $d(P)=0$. Réciproquement, soit P un polynôme de degré 0. Alors, P est un polynôme constant non nul p_0. Alors le polynôme constant $Q=1/p_0$ (puisque $\mathbb{K}$ est un corps) vérifie $QP=PQ=1$.

1.3 Divisibilité dans l'anneau $\mathbb{K}[X]$.

Définition 10 *Soit* $(P,Q) \in \mathbb{K}[X]^2$. *On dit que* P *divise* Q *lorsqu'il existe un polynôme* R *dans* $\mathbb{K}[X]$ *tel que* $Q = PR$. *On dit alors que* Q *est un multiple de* P.

Propriété 9 *Soit* $(P,Q) \in \mathbb{K}[X]^2$. *Alors, on a l'équivalence :* P *divise* Q *et* Q *divise* P *si et seulement s'il existe un scalaire* λ *non nul tel que* $P = \lambda Q$. *On dit qu'alors* P *et* Q *sont associés.*

Démonstration. On évacue le cas des polynômes nuls où tout fonctionne bien. Notons R un polynôme tel que $PR = Q$, alors $d(P) + d(R) = d(Q)$. Comme les degrés sont des entiers naturels, on en déduit que $d(P) \geq d(Q)$. L'autre relation de divisibilité fournit $d(P) \leq d(Q)$. On en déduit que $d(P) = d(Q)$, donc que $d(R) = 0$, i.e R est un polynôme constant non nul. Réciproquement, si P est de la forme λQ avec λ un scalaire non nul, alors les polynômes constants λ et $1/\lambda$ donnent les relations de divisibilité attendues.

☞ **Remarque**
Comme dans le cas de l'arithmétique de $\mathbb{Z}$, *la relation de divisibilité est à inversible près. Dans* $\mathbb{Z}$, *il s'agit du signe. Dans* $\mathbb{K}[X]$, *il s'agit d'un facteur scalaire non nul.*

Théorème 1 (Théorème de la division euclidienne) *Soit* $(A,B) \in \mathbb{K}[X] \times \mathbb{K}[X]^*$. *Alors il existe un unique couple* (Q,R) *de polynômes tel que*

$$A = BQ + R \quad et \quad [d(R) < d(B)]$$

Démonstration. Si A est nul, il suffit de choisir $(Q,R) = (0,0)$. On prouve l'existence par récurrence forte. Pour tout tout entier naturel n, on note $\mathcal{H}_n$ l'assertion : « $\forall A \in \mathbb{K}[X], d(A) = n, \exists (Q,R) \in \mathbb{K}[X], A = QB + R \wedge d(R) < d(B)$ ».
Initialisation : $n = 0$. Si $d(B) > 0$, on choisit $(Q,R) = (0,A)$. Si $d(B) = 0$, alors B est constant non nul et il suffit de choisir $(Q,R) = (A/B, 0)$.
Hérédité. Soit $n \in \mathbb{N}$ tel que $\forall k \in [\![0,n]\!], \mathcal{H}_k$. Soit $A \in \mathbb{K}[X]$ tel que $d(A) = n+1$, on note $A = aX^{n+1} + A'$ avec $a \neq 0$ et $A' \in \mathbb{K}_n[X]$. On écrit également $B = bX^p + B'$ avec $p = d(B)$, $b \neq 0$ et $B' \in \mathbb{K}_{p-1}[X]$. On pose alors $P = A - \frac{a}{b}X^{n+1-p}B = A' - \frac{a}{b}X^{n+1-p}B'$. Ce polynôme vérifie $d(P) < n+1$ car $d(A') \leq n$ et $d(X^{n+1-p}B') \leq n$. On lui applique alors l'hypothèse de récurrence : on dispose de (Q',R') tel que $P = Q'B + R'$ et $d(R') < d(B)$. On en déduit alors

$$A = P + \frac{a}{b}X^{n+1-p}B = Q'B + R' + \frac{a}{b}X^{n+1-p}B = (Q' + \frac{a}{b}X^{n+1-p})B + R'$$

En posant, $Q = Q' + \frac{a}{b}X^{n+1-p}$ et $R = R'$, on a alors $A = BQ + R$ et $d(R') = d(R) < d(B)$. L'existence est ainsi validée par récurrence forte.
Passons à l'unicité. Soit (Q_0,R_0) un autre couple satisfaisant ces critères. Alors $B(Q-Q_0) = R_0 - R$. On en déduit que $d(B) + d(Q-Q_0) = d(R-R_0)$. De plus, $d(R-R_0) \leq \max(d(R), d(R_0)) < d(B)$. On en déduit que $d(B) + d(Q-Q_0) < d(B)$. Comme B est non nul, $d(B) \neq -\infty$, de sorte qu'on peut soustraire $d(B)$ des deux côtés et obtenir $d(Q-Q_0) < 0$. Par conséquent, $Q - Q_0 = 0$ et $R - R_0 = B(Q-Q_0) = 0$. Finalement, $(Q,R) = (Q_0,R_0)$.

2 Racines d'un polynôme.

2.1 Fonction polynomiale

Définition 11 *Soit* $P \in \mathbb{K}[X]$ *tel que* $P = \sum_{k=0}^{n} p_k X^k$. *On appelle fonction polynomiale associée à* P, *l'application* $\mathbb{K} \to \mathbb{K}, x \mapsto \sum_{k=0}^{n} p_k x^k = P(x)$. *Elle est parfois notée* $\tilde{P}$

Propriété 10 *On note* $\mathcal{F}(\mathbb{K},\mathbb{K})$ *l'ensemble des applications de* $\mathbb{K}$ *dans* $\mathbb{K}$. *Muni des opérations* $+, \times$ *issues de celle de* $\mathbb{K}$, *c'est un anneau. Il est également muni d'une multiplication externe via* $\mathbb{K}$ *et d'une composition.*

Propriété 11 *Soit* $(A,B) \in \mathbb{K}[X]^2, \lambda \in \mathbb{K}$, *alors on a les égalités d'applications dans* $\mathcal{F}(\mathbb{K},\mathbb{K})$ *:*

$$\widetilde{A+B} = \widetilde{A} + \widetilde{B}, \quad \widetilde{\lambda A} = \lambda \widetilde{A}, \quad \widetilde{A \times B} = \widetilde{A} \times \widetilde{B}, \quad \widetilde{A \circ B} = \widetilde{A} \circ \widetilde{B}$$

✎ **Méthode (Algorithme de Horner)**
Plaçons-nous dans le cas réel. Soit x *un réel et* $P = \sum_{k=0}^{n} p_k X^k$ *un polynôme de degré* n. *Pour évaluer* $P(x)$, *l'expression* $\sum_{k=0}^{n} p_k x^k$ *nécessite de calculer* $n+1$ *additions et* $\sum_{k=0}^{n} k = n(n+1)/2$ *multiplications. C'est un coût quadratique sur le degré du polynôme, alors qu'on peut procéder avec une complexité linéaire en le degré de* P. *On pose* $u_0 = a_n x$ *et pour tout entier* k, $u_{k+1} = (u_k + a_{n-k})x$. *Alors* $u_n = P(x)$ *et le coût en opérations est* $2n$.

Définition 12 *Soit* $P \in \mathbb{K}[X]$ *et* $a \in \mathbb{K}$. *On dit que* a *est une racine (ou un zéro) de* P *lorsque* $P(a) = 0$.

Théorème 2 *Soit* $P \in \mathbb{K}[X]$ *et* $a \in \mathbb{K}$. *On a l'équivalence : a est racine de* P *si et seulement si* $X - a$ *divise* P.

Démonstration. Le polynôme $B = X - a$ est non nul car de degré 1. On effectue alors la division euclidienne de P par B sous la forme $P = BQ + R$ avec $R = 0$ ou $d(R) < d(B)$. Comme B est de degré 1, le polynôme R est constant (éventuellement nul). Pour évaluer cette constante, on évalue les fonctions polynomiales en a dans la division euclidienne : $P(a) = B(a)Q(a) + R(a)$. Comme $B(a) = 0$, on en déduit que R est constant égal à $P(a)$.
Si a est racine de P, alors R est nul et la division euclidienne $P = (X-a)Q$ assure que $X-a$ divise P. Réciproquement, si $X - a$ divise P, le reste dans cette division euclidienne est nul, donc $P(a) = 0$ et a est racine de P.

Propriété 12 *Soit* $P \in \mathbb{K}[X]$ *un polynôme non nul. Alors* $Z(P)$ *l'ensemble des racines est fini et* $|Z(P)| \leq d(P)$.

Démonstration. On en prouve la contraposée par récurrence sur le degré de P. Pour tout entier naturel n, on note $\mathcal{H}_n : \forall P \in \mathbb{K}_n[X], |Z(P)| \geq n+1 \Rightarrow P = 0$. Intialisation : pour $n = 0$. Soit $P \in \mathbb{K}_0[X]$ tel que $|Z(P)| \geq 1$. C'est donc un polynôme de degré au plus 0, il est donc constant. D'après l'hypothèse sur le nombre de ses racines, il en possède une, que l'on note a. Mais alors P est constant égal à $P(a)$, donc constant nul. Hérédité : Soit $n \in \mathbb{N}$ tel que $\mathcal{H}_n$ est vérifié. Démontrons que $\mathcal{H}_{n+1}$ est vérifiée. Soit $P \in \mathbb{K}_{n+1}[X]$ tel que $|Z(P)| \geq n+2$. Notons a un élément de $Z(P)$. D'après la propriété précédente, $X - a$ divise P. On note alors Q un polynôme tel que $P = (X-a)Q$ et on a l'égalité de degrés $d(P) = 1 + d(Q)$. De plus, on dispose de $a_1, \ldots, a_{n+1}$ $n+1$ scalaires distincts et distincts de a dans $Z(P)$ par hypothèse. Mais alors $\forall i [\![1, n+1]\!]$, $0 = P(a_i) = (a - a_i)Q(a_i)$. D'après l'intégrité de $\mathbb{K}$, on en déduit que $Z(Q) \supset \{a_1, \ldots, a_{n+1}\}$. On peut ainsi appliquer l'hypothèse de récurrence $\mathcal{H}_n$ au polynôme Q, ce qui assure que $Q = 0$, donc que $P = 0$.

☞ **Remarque**
On utilise souvent cette propriété via sa contraposée. Si on trouve un nombre de racines strictement supérieur au degré de P, *alors* P *est le polynôme nul.*

Propriété 13 *Soit* P *un polynôme. On suppose que* P *possède un nombre strictement plus grand que son degré de racines. Alors* P *est le polynôme nul.*

Propriété 14 *On suppose que* $\mathbb{K}$ *est un corps infini (typiquement un sous-corps de* $\mathbb{C}$*). Alors l'application* $\mathbb{K}[X] \to \mathbb{K}^{\mathbb{K}}, P \mapsto \widetilde{P}$ *est une injection. Autrement dit, un polynôme est uniquement déterminé par sa fonction polynomiale.*

Démonstration. Soit $(P, Q) \in (\mathbb{K}[X])^2$ tel que $\widetilde{P} = \widetilde{Q}$. Alors, $\widetilde{P - Q} = \widetilde{P} - \widetilde{Q} = 0$. Par conséquent, le polynôme $P - Q$ possède une infinité de racines, puisque $\mathbb{K}$ est infini. D'après la propriété précédente, $P - Q$ est le polynôme nul, donc $P = Q$.

Définition 13 *Soit* $P \in \mathbb{K}[X]$ *non nul et a une racine de* P. *Alors* $\max\{k \in \mathbb{N} | (X-k)^k \mid P\}$ *est appelé multiplicité de la racine a dans* P. *Si a n'est pas racine, on convient que sa multiplicité dans* P *vaut* 0.

Définition 14 *Soit* $P \in \mathbb{K}[X]$. *On dit que* P *est scindé lorsqu'il peut s'écrire comme produit de polynômes de degré* 1. *On dit que* P *est simplement scindé lorsque* P *est produit de polynômes de degré* 1 *tous distincts.*

Exemple 1 *Pour tout entier n non nul,* $X^n - 1$ *est simplement scindé car égal à* $\prod_{k=1}^{n}(X - \omega^k)$ *avec* $\omega = \exp(2i\pi/n)$.

Propriété 15 *Soit* $P \in \mathbb{K}[X]$, n *un entier naturel non nul,* $(a_1, \ldots, a_n) \in \mathbb{K}^n$ *un n-uplet de scalaires tous distincts. On suppose que* $\forall i \in [\![1, n]\!], P(a_i) = 0$. *Alors* $\prod_{i=1}^{n}(X - x_i)$ *divise* P

Démonstration. On établit cette propriété par récurrence sur n. Initialisation $n = 1$: il s'agit de la propriété $P(a) = 0 \iff X - a \mid P$. Hérédité : Soit n un entier naturel non nul tel que la propriété est vraie. Montrons-la au rang $n+1$. Soit $(a_1, \ldots, a_{n+1})$ un $n+1$-uplet de scalaires tous distincts tel que $\forall i [\![1, n+1]\!], P(a_i) = 0$. En particulier, $P(a_{n+1}) = 0$, donc $X - a_{n+1}$ divise P. On note alors Q tel que $P = (X - a_{n+1})Q$ et $\forall i [\![1, n]\!], (a_i - a_{n+1})Q(a_i) = 0$. Comme les $(a_i)_i$ sont distincts de a_{n+1}, on en déduit que $Q(a_i) = 0$. Par hypothèse de récurrence, $\prod_{i=1}^{n}(X - a_i)$ divise Q. Alors $\prod_{i=1}^{n+1}(X - a_i)$ divise P.

Définition 15 *Soit $(a_1,\dots,a_n)\in\mathbb{K}^n$ et $k\in\mathbb{N}$ tel que $k\leq n$. On note*

$$\sigma_k(a_1,\dots,a_n)=\sum_{1\leq i_1<i_2<\cdots<i_k\leq n} a_{i_1}a_{i_2}\dots a_{i_k}$$

On l'appelle fonction symétrique élémentaire d'ordre k en les $(a_i)_{1\leq i\leq n}$.

Exemple 2

$$\sigma_0(a_1,\dots,a_n)=1$$

$$\sigma_n(a_1,\dots,a_n)=a_1\dots a_n$$

$$\sigma_1(a_1,\dots,a_n)=a_1+\cdots+a_n$$

$$\sigma_2(a_1,\dots,a_n)=\sum_{1\leq i<j\leq n} a_ia_j$$

$$\sigma_2(a_1,a_2,a_3)=a_1a_2+a_1a_3+a_2a_3$$

$$\sigma_2(a_1,a_2,a_3,a_4)=a_1a_2+a_1a_3+a_1a_4+a_2a_4+a_3a_4$$

Propriété 16 (Relations coefficients-racines) *[Formules de Viète] Soit $(a_1,\dots,a_n)\in\mathbb{K}^n$.*

$$\prod_{i=1}^{n}(X-a_i)=\sum_{k=0}^{n}(-1)^{n-k}\sigma_{n-k}(a_1,\dots,a_n)X^k$$

☞ **Remarque**
Le plus important est de retenir

$$\prod_{i=1}^{n}(X-a_i)=X^n-\left(\sum_{i=1}^{n}a_i\right)X^{n-1}+\cdots+(-1)^n\prod_{i=1}^{n}a_i$$

Démonstration. Prouvons ce résultat par récurrence sur n. Initialisons en $n=1$.

$$\sum_{k=0}^{1}(-1)^{1-k}\sigma_{1-k}(a_1)X^k=-a_1+X$$

Supposons le résultat acquis en un rang $n\in\mathbb{N}^*$ et démontrons-le au rang $n+1$. On écrit

$$\begin{aligned}
\prod_{i=1}^{n+1}(X-a_i) &= (X-a_{n+1})\sum_{k=0}^{n}(-1)^{n-k}\sigma_{n-k}(a_1,\dots,a_n)X^k\\
&= \sum_{k=0}^{n}(-1)^{n-k}\sigma_{n-k}(a_1,\dots,a_n)X^{k+1}-\sum_{k=0}^{n}(-1)^{n-k}a_{n+1}\sigma_{n-k}(a_1,\dots,a_n)X^k\\
&= \sum_{l=1}^{n+1}(-1)^{n+1-l}\sigma_{n+1-l}(a_1,\dots,a_n)X^l+\sum_{k=0}^{n}(-1)^{n+1-k}a_{n+1}\sigma_{n-k}(a_1,\dots,a_n)X^k\\
&= X^{n+1}+(-1)^{n+1}a_1\dots a_{n+1}+\sum_{l=1}^{n}(-1)^{n+1-l}(\sigma_{n+1-l}(a_1,\dots,a_n)+a_{n+1}\sigma_{n-l}(a_1,\dots,a_n))X^l
\end{aligned}$$

Soit $k\in[\![1,n]\!]$, on étudie

$$\sigma_{k+1}(a_1,\dots,a_n)+a_{n+1}\sigma_k(a_1,\dots,a_n) = \sum_{1\leq i_1<i_2<\cdots<i_{k+1}\leq n} a_{i_1}a_{i_2}\dots a_{i_{k+1}}+a_{n+1}\sum_{1\leq i_1<i_2<\cdots<i_k\leq n} a_{i_1}a_{i_2}\dots a_{i_k}$$

Parmi les choix de $k+1$ d'indices croissants dans $[\![1,n+1]\!]$, il y a ceux qui ne contiennent pas $n+1$, ce qui correspond à la première somme, puis ceux qui contiennent $n+1$, ce qui correspond à la seconde somme. Ainsi,

$$\sigma_{k+1}(a_1,\dots,a_n)+a_{n+1}\sigma_k(a_1,\dots,a_n)=\sigma_{k+1}(a_1,\dots,a_{n+1})$$

On retrouve alors

$$\prod_{i=1}^{n+1}(X-a_i)=\sum_{k=0}^{n+1}(-1)^{n+1-k}\sigma_{n+1-k}(a_1,\dots,a_{n+1})X^k$$

et les formules de Viète sont établies par récurrence.

Propriété 17 *Soit* P *un polynôme de degré* n *non nul que l'on suppose scindé. On note* $P = \sum_{k=0}^{n} p_k X^k$ *et on liste* $(a_1, \dots, a_n)$ *ses racines (éventuellement répétées). Alors*

$$\forall k \in [\![0, n]\!], \quad \frac{p_k}{p_n} = (-1)^{n-k} \sigma_{n-k}(a_1, \dots, a_n)$$

Démonstration. Il suffit de factoriser en tenant compte du coefficient dominant de P : $P = p_n \prod_{i=1}^{n} (X - a_i)$ et d'appliquer les formules de Viète.

2.2 Interpolation de Lagrange

Théorème 3 (Interpolation de Lagrange) *Soit* n *un entier naturel non nul,* $(x_1, \dots, x_n)$ *des éléments* ***distincts*** *de* $\mathbb{K}$*,* $y_1, \dots, y_n$ *des éléments de* $\mathbb{K}$*. Alors il existe un unique polynôme* P *dans* $\mathbb{K}_{n-1}[X]$ *tel que* $\forall i \in [\![1, n]\!], P(x_i) = y_i$*.*

Démonstration. Pour tout entier j dans $[\![1, n]\!]$, on note

$$L_j = \prod_{\substack{i=1 \\ i \neq j}}^{n} \frac{X - x_i}{x_j - x_i}$$

Ce polynôme est de degré $n-1$, vérifie en particulier, $L_j(x_j) = 1$ et $\forall i \in [\![1, n]\!], i \neq j, L_j(x_i) = 0$. On synthétise le tout en écrivant

$$\forall j \in [\![1, n]\!], \quad L_j(x_i) = \delta_{i,j}$$

A l'aide de cette famille de n polynômes, on pose $P = \sum_{j=1}^{n} y_j L_j$, il s'agit d'un polynôme qui est somme de polynômes de degrés $n-1$, donc de degré au plus $n-1$. De plus,

$$\forall i \in [\![1, n]\!], P(x_i) = \sum_{j=1}^{n} y_j L_j(x_i) = \sum_{j=1}^{n} y_j \delta_{i,j} = y_i$$

Il satisfait tous les crtières attendus et l'existence est ainsi prouvée.
Soit à présent deux polynômes Q, R vérifiant tous ces critères. Alors $Q - R$ est un polynôme de degré au plus $n-1$ et $\forall i \in [\![1, n]\!], (Q-R)(x_i) = Q(x_i) - R(x_i) = y_i - y_i = 0$. Comme tous les x_i sont distincts, on a ainsi montré que $|Z(Q-R)| > d(Q-R)$. Cela entraîne que $Q - R = 0$, donc $Q = R$. L'unicité est ainsi acquise.

Définition 16 *Soit* $j \in [\![1, n]\!]$*. Si la famille* $(y_1, \dots, y_n)$ *est la famille* $(\delta_{i,j})_{1 \leq i \leq n}$*, le polynôme ainsi construit s'appelle le* j*-ième polynôme interpolateur de la famille* $(x_1, \dots, x_n)$*, souventé noté* L_j*.*

Propriété 18 *En gardant les notations précédentes, l'ensemble des polynômes* S *vérifiant* $\forall i \in [\![1, n]\!], S(x_i) = y_i$ *est l'ensemble*

$$\left\{ \prod_{i=1}^{n} (X - x_i) T + P \mid T \in K[X] \right\}$$

Voici une autre façon de décrire cet ensemble : il s'agit des polynômes dont le reste dans la division euclidienne par $\prod_{i=1}^{n} (X - x_i)$ *vaut* P

Démonstration. Soit S un polynôme tel que $\forall i \in [\![1, n]\!], S(x_i) = y_i$, alors $S - R$ admet tous les $(x_i)_{1 \leq i \leq n}$ pour racines. Comme ceux-ci sont tous distincts, $S - R$ est divisible par $\prod_{i=1}^{n} (X - x_i)$, ce qui donne la forme attendue. Réciproquement, soit $T \in \mathbb{K}[X]$ et $S = \prod_{i=1}^{n} (X - x_i) T + P$. Alors $\forall i \in [\![1, n]\!], S(x_i) = 0 + P(x_i) = y_i$. La remarque finale provient du fait que $d(\prod_{i=1}^{n} (X - x_i)) = n$ et $d(P) \leq n - 1$, donc P est bien un reste dans la division euclidienne annoncée.

3 Dérivation dans $\mathbb{K}[X]$.

C'est ici que se trouve un obstacle important à la généralité des corps utilisés. On va se limiter ici à des corps de caractéristique 0, cela signifie que $\forall n \in \mathbb{Z}, \forall a \in \mathbb{K}, na = 0 \Rightarrow a = 0$. C'est le cas de tous les sous-corps de $\mathbb{C}$.

Définition 17 *Soit* $P \in \mathbb{K}[X]$ *de degré* n*. Si* $n \in \mathbb{N}$*, on le note sous la forme* $P = \sum_{k=0}^{n} a_k X^k$*. Le polynôme* $\sum_{k=1}^{n} k a_k X^{k-1}$ *est appelé polynôme dérivé de* P*, il est noté* P'*. Si* $P = 0$*, on définit* $P' = 0$*.*

☞ **Remarque**
On dit parfois qu'il s'agit d'une dérivation formelle. Il n'est pas question de dérivabilité ici, on a simplement défini la dérivée formelle à l'aide de la liste de ses coefficients.

Propriété 19 *Soit* $(P,Q)\in\mathbb{K}[X]^2, (\lambda,\mu)\in\mathbb{K}^2$. *Alors*

— $P'=0 \iff d(P)\leq 0$.

— *Si* P *est non constant,* $d(P')=d(P)-1$. *Si* P *est constant,* $d(P')=-\infty$.

— $(\lambda P+\mu Q)=\lambda P'+\mu Q'$.

— $(PQ)'=P'Q+PQ'$.

— $(P\circ Q)=Q'(P'\circ Q)$.

Démonstration. — Si $P=0$, c'est évident. Sinon, $P'=0 \iff \forall n\in\mathbb{N}^*, p_n=0 \iff d(P)\leq 0$.

— Si P est non constant de degré n, le terme dominant de P' vaut np_nX^{n-1}. Comme $\mathbb{K}$ est de caractéristique 0, et $p_n\neq 0$, $np_n\neq 0$. Ainsi, $d(P')=n-1=d(P)-1$.

— Avec des notations évidentes,

$$\lambda P+\mu Q=\sum_{i=0}^{\max(d(P),d(Q))}(\lambda p_k+\mu q_k)X^k$$

La définition du polynôme entraîne

$$(\lambda P+\mu Q)'=\sum_{i=1}^{\max(d(P),d(Q))}k(\lambda p_k+\mu q_k)X^{k-1}=\lambda\sum_{k=1}^{d(P)}kp_kX^{k-1}+\mu\sum_{k=1}^{d(Q)}kq_kX^{k-1}=\lambda P'+\mu Q'$$

— Simplifions nous la vie en traitant d'abord le cas des monômes. Soit m et n deux entiers naturels. Si m ou n est nul, X^m ou X^n est de dérivée nulle, puisque constant. Supposons à présent m et n tous deux non nuls. Alors $(X^mX^n)'=(X^{m+n})'=(m+n)X^{m+n-1}=mX^{m-1}X^n+X^mnX^{n-1}=(X^m)'X^n+X^m(X^n)'$, ce qui établit la formule souhaitée par les monômes. Dans le cas général, on utilise la linéarité précédemment démontrée :

$$(PQ)'=\left(\sum_{m=0}^{+\infty}p_mX^m\sum_{n=0}^{+\infty}q_nX^n\right)'=\left(\sum_{(n,m)\in\mathbb{N}^2}p_mq_nX^{m+n}\right)'=\sum_{(n,m)\in\mathbb{N}^2}p_mq_n(X^{m+n})'$$

D'après la propriété sur les dérivations de produits de monômes, on en déduit que

$$(PQ)'=\sum_{(n,m)\in\mathbb{N}^2}p_mq_n\left[(X^m)'X^n+X^m(X^n)'\right]=\sum_{(n,m)\in\mathbb{N}^2}p_mq_n(X^m)'X^n+\sum_{(n,m)\in\mathbb{N}^2}p_mq_nX^m(X^n)'$$

On reconnaît des produits polynomiaux

$$(PQ)'=\sum_{m\in\mathbb{N}}p_m(X^m)'\sum_{n\in\mathbb{N}}q_nX^n+\sum_{m\in\mathbb{N}}p_mX^m\sum_{n\in\mathbb{N}}q_n(X^n)'$$

Toujours d'après la linéarité,

$$(PQ)'=P'Q+PQ'$$

— Si P est nul, $P'=0$, $P'\circ Q=0$ et $P\circ Q=0$, donc l'égalité est assurée. Sinon, on note $P=\sum_{k=0}^n p_kX^k$, ce qui entraîne $P\circ Q=\sum_{k=0}^n p_kQ^k$. En généralisant rapidement ce qui précède par récurrence,, on en déduit que $(P\circ Q)'=\sum_{k=1}^n p_kkQ'Q^{k-1}=Q'(P'\circ Q)$.

Définition 18 *On définit par récurrence les dérivées sucessives d'un polynôme* P, *elles sont notées* $P^{(k)}$. *On convient que* $P^{(0)}=P$.

Exemple 3 *Soit* $(k,n)\in\mathbb{N}^2$. *Alors*

$$(X^n)^{(k)}=\begin{cases}\frac{n!}{(n-k)!}X^{n-k} & \text{si } k<n\\ k! & \text{si } k=n\\ 0 & \text{si } k>n\end{cases}$$

Propriété 20 (Formule de Leibniz) *Soit* $(P,Q)\in\mathbb{K}[X]^2$ *et* $n\in\mathbb{N}$. *Alors*

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

Démonstration. Calquer la preuve dans le cas des fonctions réelles. Il s'agit d'une récurrence se basant sur la formule de Pascal.

Théorème 4 (Formule de Taylor polynomiale) *Soit* $P \in K[X]$ *de degré* n, $a \in \mathbb{K}$ *Alors*

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

En particulier, le coefficient d'indice k *de* P *n'est autre que* $P^{(k)}(0)/k!$.

Démonstration. On note $P = \sum_{j=0}^{n} p_j X^j$. Soit $k \in [\![0, n]\!]$. D'après la linéarité de la dérivation et la formule sur les dérivées itérées des monômes, on a

$$P^{(k)} = \sum_{j=0}^{n} p_j \left(X^j\right)^{(k)} = \sum_{j=k}^{n} p_j \frac{k!}{(k-j)!} X^{k-j}$$

L'évaluation en 0 donne alors

$$P^{(k)}(0) = k! p_k$$

On retrouve alors la formule indiquée pour $a = 0$. Dans le cas général, on applique ce qui précède à $Q = P(X + a)$. Cela entraîne

$$Q = \sum_{k=0}^{n} \frac{Q^{(k)}(0)}{k!} X^k$$

Or pour tout entier r, $Q^{(r)} = P^{(r)}(X + a)$ (récurrence facile puisque $(X + a)' = 1$), et $P = Q(X - a)$. On en déduit que

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

Propriété 21 *Soit* $P \in \mathbb{K}[X]$ *non nul et a une racine de* P. *Alors la multiplicité de a dans* P *vaut*

$$1 + \max\{k \in \mathbb{N} | P^{(k)}(a) = 0\}$$

Démonstration. Soit k un entier non nul. Via la formule de Taylor polynomiale, on écrit la division euclidienne de P par $(X - a)^k$:

$$P = (X-a)^k \sum_{j=k}^{n} \frac{P^{(j)}(a)}{j!}(X-a)^{j-k} + \sum_{j=0}^{k-1} \frac{P^{(j)}(a)}{j!}(X-a)^j$$

ce qui est valide puisque le degré de $\sum_{j=0}^{k-1} \frac{P^{(j)}(a)}{j!}(X-a)^j$ vaut au plus $k-1 < k = d((X-a)^k)$. On a alors l'équivalence

$$(X-a)^k \mid P \iff \sum_{j=0}^{k-1} \frac{P^{(j)}(a)}{j!}(X-a)^j = 0 \iff \forall j \in [\![0, k-1]\!], P^{(j)}(a) = 0$$

On a alors l'égalité annoncée.

Propriété 22 *Soit* $P \in \mathbb{K}[X]$ *non nul et a une racine de* P. *Alors la multiplicité de a dans* P *vaut* n *si et seulement si*

$$P(a) = 0, \quad P'(a) = 0, \quad \ldots, \quad P^{(n-1)}(a) = 0, \quad P^{(n)}(a) \neq 0$$

Démonstration. Il s'agit d'une refomulation du maximum précédent.

4 Arithmétique dans $\mathbb{K}[X]$.

L'exposé est ici abrégé, car extrêmement similaire au chapitre sur l'arithmétique de $\mathbb{Z}$. On ne peut pas toutefois adapter les notions de sous-groupes de $(\mathbb{Z},+)$ à $(\mathbb{K}[X],+)$. Les structures sous-jacentes à l'arithmétique dans le cas général s'appellent des idéaux. Vous les aborderez l'année prochaine.

4.1 L'anneau euclidien $\mathbb{K}[X]$.

Théorème 5 (Théorème de la division euclidienne) *Soit* $(A,B) \in \mathbb{K}[X]\times\mathbb{K}[X]^*$. *Alors il existe un unique couple* (Q,R) *de polynômes tel que*

$$A = BQ + R \quad \textit{et} \quad [R = 0 \textit{ ou } d(R) < d(B)]$$

✎ **Méthode**
Pour déterminer le reste R, *il suffit d'évaluer l'égalité en les racines de* B *si elles sont toutes simples. On dérive si certaines racines sont multiples.*

Exemple 4 *On pose* $B = X^2+X+1$. *Soit* $n \in \mathbb{N}$. *On cherche le reste dans la division euclidienne de* X^n *par* B. *Ce reste est de degré au plus* 1, *on écrit alors* R *sous la forme* $a_nX + b_n$. *On exploite les racines de* B *pour trouver les coefficients* a_n *et* b_n. *En évaluant* $X^n = BQ_n + a_nX + b_n$ *en* j *et* j^2, *on obtient* $a_nj + b_n = j^n$ *et* $a_nj^2 + b_n = j^{2n}$. *On s'est ainsi ramené à un système linéaire* 2×2 *qui fournit*

$$a_n = \frac{j^{2n}-j^n}{j^2-j} = \begin{cases} 0 & \textit{si } n \equiv 0[3] \\ 1 & \textit{si } n \equiv 1[3] \\ -1 & \textit{si } n \equiv 2[3] \end{cases}$$

puis

$$b_n = \frac{j^{2n}-j^{n+1}}{1-j} = \begin{cases} 1 & \textit{si } n \equiv 0[3] \\ 0 & \textit{si } n \equiv 1[3] \\ -1 & \textit{si } n \equiv 2[3] \end{cases}$$

Exemple 5 *Soit* $B = (X+1)^2$ *et* $n \in \mathbb{N}^*$. *On cherche le reste dans la division euclidienne de* X^n *par* B. *Ce reste est de degré au plus* 1 *et on l'écrit sous la forme* $\alpha_nX + \beta_n$. *L'égalité* $(-1)^n = B(-1)Q_n(-1) + R_n(-1)$ *fournit* $-\alpha_n + \beta_n = (-1)^n$. *Pour obtenir davantage d'informations, on dérive* $nX^{n-1} = 2(X+1)Q_n + (X+1)^2Q_n' + R_n'$, *ce qui fournit* $n(-1)^{n-1} = \alpha$. *On en déduit que*

$$R_n = n(-1)^{n-1}X + (-1)^n - n(-1)^{n-1} = n(-1)^{n-1}X + (n+1)(-1)^n$$

4.2 Pgcd, ppcm dans $\mathbb{K}[X]$.

Propriété 23 *Soit* $P \in \mathbb{K}[X]$ *non nul. L'ensemble des degrés des diviseurs de* P *est majoré.*

Démonstration. Si Q divise P, alors on écrit $QR = P$, donc $d(Q) + d(R) = d(P)$. Comme P est non nul, R est non nul, et on peut minorer $d(R)$ par 0. On en déduit $d(Q) \leq d(P)$.

Définition 19 *Soit* $(P,Q) \in \mathbb{K}[X]^2$. *Si* P *et* Q *sont nuls, on définit leur pgcd comme* 0. *Sinon, on définit leur pgcd comme leur diviseur commun unitaire de plus grand degré. Si* P *ou* Q *est nul, on définit leur ppcm comme* 0. *Sinon, on définit leur ppcm comme leur multiple commun unitaire de plus petit degré.*

Théorème 6 *Soit* $(P,Q) \in \mathbb{K}[X]^2$. *Alors* $P\mathbb{K}[X] + Q\mathbb{K}[X] = (P \wedge Q)\mathbb{K}[X]$ *et* $P\mathbb{K}[X] \cap Q\mathbb{K}[X] = (P \vee Q)\mathbb{K}[X]$.

Lemme 1

$$\exists W \in \mathbb{K}[X], P\mathbb{K}[X] + Q\mathbb{K}[X] = W\mathbb{K}[X], \quad \exists Y \in \mathbb{K}[X], P\mathbb{K}[X] \cap Q\mathbb{K}[X] = Y\mathbb{K}[X].$$

Démonstration (preuve du lemme). Si P et Q sont tous deux nuls, il suffit de choisir W = 0. Sinon, on pose $\Delta = \{d(U)|U \in (P\mathbb{K}[X]+Q\mathbb{K}[X])\backslash\{0\}\}$. Comme P ou Q est non nul, Δ est non vide, donc il possède un minimum. On dispose alors d'un polynôme non nul de degré minimal dans $P\mathbb{K}[X]+Q\mathbb{K}[X]$. Soit $V \in P\mathbb{K}[X]+Q\mathbb{K}[X]$. On effectue la division euclidienne de V par W : V = WS + R avec $d(R) < d(W)$. Mais alors R = V − WS appartient clairement à $P\mathbb{K}[X]+Q\mathbb{K}[X]$ puisque V et W en font partie. Par minimalité du degré de W, R = 0. On en déduit que $P\mathbb{K}[X]+Q\mathbb{K}[X] \subset W\mathbb{K}[X]$. L'inclusion réciproque est claire puisque $W \in P\mathbb{K}[X]+Q\mathbb{K}[X]$.
L'autre construction se réplique à l'identique, en utilisant une division euclidienne par un polynôme non nul de degré minimal dans $P\mathbb{K}[X] \cap Q\mathbb{K}[X]$.

Démonstration (preuve du théorème). Dans le cas où P ou Q est nuls, l'égalité est claire. On suppose que P et Q sont tous deux non nuls. Soit D un diviseur commun à P et Q. Alors D divise tout polynôme de la forme PU + QV avec U et V dans $\mathbb{K}[X]$. Ainsi, $P \wedge Q$ qui est un diviseur commun à P et Q divise tous les éléments de $P\mathbb{K}[X]+Q\mathbb{K}[X]$, donc $P\mathbb{K}[X]+Q\mathbb{K}[X] \subset (P \wedge Q)\mathbb{K}[X]$. Réciproquement, on considère le polynôme unitaire de plus petit degré dans $P\mathbb{K}[X]+Q\mathbb{K}[X]$ que l'on note W. Par division euclidienne, $W\mathbb{K}[X] = P\mathbb{K}[X]+Q\mathbb{K}[X]$. Donc il existe U, V des polynômes tels que $W = PU+QV = (P \wedge Q)(P_1U+Q_1V)$, ainsi W est multiple de $P \wedge Q$ et $(P \wedge Q)\mathbb{K}[X] \subset W\mathbb{K}[X] = P\mathbb{K}[X]+Q\mathbb{K}[X]$. L'égalité est alors prouvée.
Pour le ppcm, on remarque que $P\mathbb{K}[X] \cap Q\mathbb{K}[X]$ est l'ensemble des multiples communs à P et Q. En considérant le polynôme unitaire de plus petit degré dans cet ensemble Y, on trouve $P\mathbb{K}[X] \cap Q\mathbb{K}[X] = Y\mathbb{K}[X]$. Y est alors multiple commun à $\mathbb{K}[X]$, et parmi les polynômes non nuls, c'est celui de plus petit degré, donc c'est le ppcm $P \vee Q$.

Propriété 24 *Soit* $(P,Q) \in \mathbb{K}[X]^2$, $A \in \mathbb{K}[X]$

- $D(P) \cap D(Q) = D(P \wedge Q)$
- $D(P) \cap D(Q+AP) = D(P) \cap D(Q)$
- $\exists (P_1,Q_1) \in \mathbb{K}[X]^2, P = (P \wedge Q)P_1, Q = (P \wedge Q)Q_1, P_1 \wedge Q_1 = 1$.

Démonstration.
- D'après l'égalité précédente, être diviseur commun à P et Q équivaut à être diviseur de $P \wedge Q$, d'où l'égalité.
- D'après l'égalité précédente, $P\mathbb{K}[X]+(Q+AP)\mathbb{K}[X] = P\mathbb{K}[X]+Q\mathbb{K}[X] = (P \wedge Q)\mathbb{K}[X]$. Ainsi, être diviseur commun de P et Q équivaut à être diviseur commun de P et Q + AP, puisqu'il s'agit d'être diviseur de $P \wedge Q$.
- Le polynôme $P \wedge Q$ divise P et Q, donc on peut écrire $P = (P \wedge Q)P_1$ et $Q = (P \wedge Q)Q_1$. Mais alors par intégrité de $\mathbb{K}[X]$, l'égalité d'ensembles $(P \wedge Q)\mathbb{K}[X] = P\mathbb{K}[X]+Q\mathbb{K}[X] = (P \wedge Q)P_1\mathbb{K}[X]+(P \wedge Q)Q_1\mathbb{K}[X]$ se simplifie en $P_1\mathbb{K}[X]+Q_1\mathbb{K}[X] = \mathbb{K}[X]$, donc P_1 et Q_1 sont premiers entre eux.

Propriété 25 *Soit* $(P,Q) \in (\mathbb{K}[X])^2$. *Alors* $\exists (U,V) \in (\mathbb{K}[X])^2, P \wedge Q = UP+VQ$.

Démonstration. Cf plus haut

Théorème 7 (Bezout) *Soit* $(P,Q) \in \mathbb{K}[X]$. *Alors* $P \wedge Q = 1 \iff \exists (U,V) \in (\mathbb{K}[X])^2, 1 = UP+VQ$.

Démonstration. La réciproque vient du fait que les seuls diviseurs unitaires de 1 sont 1.

☞ **Remarque**
On détermine les relations de Bezout par l'algorithme d'Euclide étendu comme dans le cas de $\mathbb{Z}$.

Propriété 26 (Lemme de Gauss) *Soit* $(P,Q,R) \in \mathbb{K}[X]^2$. *On suppose que* P *divise* QR *et* $P \wedge Q = 1$. *Alors* P *divise* R.

Démonstration. On écrit une relation de Bezout : PU + QV = 1. Alors P divise PUR + QVR = R.

On étend toutes ces propriétés à des familles finies de polynômes.

Propriété 27 *Soit* $(P,Q) \in \mathbb{K}[X]^2$, $A \in \mathbb{K}[X]$. *On suppose que* $P \wedge A = 1$ *et* $Q \wedge A = 1$. *Alors* $(PQ) \wedge A = 1$.

Démonstration. On écrit deux relations de Bezout issues des hypothèses : 1 = AU + PV et 1 = AS + QT, On en déduit que

$$PVQT = (1-AU)(1-AS) = 1-A(U+S+AUS)$$

Exemple 6 *Soit* $(a,b) \in \mathbb{K}^2$, $a \neq b$, $(p,q) \in (\mathbb{N}^*)^2$. *Alors* $(X-a)^p \wedge (X-b)^q = 1$. *Dans le cas* $p = q = 1$, *on constate que* $(X-a)1+(-1)(X-b) = b-a \neq 0$, *donc que* $(X-a)\frac{1}{b-a}+(X-b)\frac{1}{a-b} = 1$. *On en déduit par récurrence via la propriété précédente que* $(X-a)^p \wedge (X-b)^q = 1$.

Propriété 28 *Soit* $P \in \mathbb{K}[X]$. *On suppose que* P *est scindé. Alors* P *est simplement scindé si et seulement si* $P \wedge P' = 1$.

Démonstration. On regroupe toutes les racines de P, ce qui permet d'écrire

$$P = \lambda \prod_{i=1}^{n} (X - a_i)^{k_i}$$

avec $\lambda \in \mathbb{K}^*$ et $(a_1, \dots, a_n)$ n scalaires tous distincts, $(k_1, \dots, k_n)$ des entiers naturels tous non nuls. On établit alors l'expression de la dérivée de P

$$P' = \lambda \sum_{i=1}^{n} k_i (X - a_i)^{k_i - 1} \prod_{\substack{j=1 \\ j \neq i}}^{n} (X - a_j)^{k_j}$$

Comme tous les a_i sont distincts, on en déduit que

$$P \wedge P' = \prod_{j=1}^{n} (X - a_j)^{k_j - 1}$$

On en déduit que $P \wedge P' = 1 \iff \forall j \in [\![1, n]\!], k_j = 1 \iff$ P simplement scindé.

4.3 L'anneau factoriel $\mathbb{K}[X]$.

Définition 20 *Soit* $P \in \mathbb{K}[X]$. *Le polynôme* P *est dit irréductible lorsqu'il est non constant et*

$$\forall (Q, R) \in \mathbb{K}[X]^2, P = QR \Rightarrow [d(Q) = 0 \vee d(R) = 0]$$

Autrement dit, P *ne possède pas d'autres factorisations qu'en facteurs constants et associés à* P.

Propriété 29 *Soit* $P \in \mathbb{K}[X]$ *non constant.* P *est irréductible si et seulement si les seuls diviseurs de* P *sont les polynômes constants et les polynômes associés à* P.

Exemple 7 *Tout polynôme de degré* 1 *est irréductible. Soit* P *un polynôme de degré supérieur ou égal à* 2 *tel que* P *admet une racine, alors* P *n'est pas irréductible. En effet, en notant a une telle racine,* $X - a$ *divise* P *et* $d(X - a) < d(P)$ *puisque* $d(P) \geq 2$*, ce qui fournit une factorisation non triviale de* P. *La réciproque est fausse en général : le polynôme* $X^4 + 1$ *n'a pas de racine dans* $\mathbb{R}$*, pourtant,* $X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$ *est une factorisation non triviale de* P. *La réciproque est vraie dans le cas* $n = 2$ *et* $n = 3$. *Soit* P *un polynôme de degré* 2 *ou* 3 *sans racines. Soit* $P = QR$ *une factorisation de* P. *Alors* Q *et* R *sont sans racines, sinon* P *en aurait. Par conséquent,* Q *et* R *ne sont pas de degré* 1. *Si* P *est de degré* 2*, cela indique que* $d(Q) = 2$ *ou* $d(R) = 2$ *donc qu'il s'agit d'une factorisation triviale. Ainsi,* P *est irrréductible. Si* P *est de degré* 3*,* $d(Q) + d(R) = 3$*, donc* Q *et* R *ne sont pas de degré* 2. *Ainsi,* $d(Q) = 3$ *ou* $d(R) = 3$*, et la factorisation est triviale et* P *est irréductible.*

Propriété 30 *Soit* $P \in \mathbb{K}[X]$ *non constant.* P *est irréductible si et seulement si* $\forall Q \in \mathbb{K}_{d(P)-1}[X], Q \wedge P = 1$.

Démonstration. Si P est irréductible, on considère $Q \in \mathbb{K}_{d(P)-1}[X]$ non constant. Pour tout diviseur D de P et Q, D est constant, sinon il fournit une factorisation non triviale de P puisque de degré inférieur à $d(P) - 1$. Par conséquent, $P \wedge Q = 1$. Supposons $\forall Q \in \mathbb{K}_{d(P)-1}[X], Q \wedge P = 1$. Alors $D(P) \backslash P\mathbb{K}[X] \subset \bigcup_{Q \in \mathbb{K}_{d(P)-1}} D(P) \cap D(Q) \subset \mathbb{K}[X]$. Par conséquent, les seuls diviseurs de P non associés à P sont constants et P est irréductible.

Propriété 31 *Soit* $P \in \mathbb{K}[X]$ *irréductible,* $(A, B) \in \mathbb{K}[X]^2$*. On suppose que* P *divise* AB*. Alors* P *divise* A *ou* P *divise* B*. Autrement dit, tout polynôme irréductible est premier.*

Démonstration. Comme P divise AB, $d(P) \leq d(AB)$, donc $d(P) \leq d(A)$ ou $d(P) \leq d(B)$. Dans le cas où $d(P) \leq d(A)$, si P ne divise pas A, alors $P \wedge A = 1$. On en déduit par le lemme de Gauss, que P divise B.

Propriété 32 *Soit* P *un polynôme non constant. Alors* P *possède un diviseur irréductible. En particulier, si* P *n'est pas irréductible,* P *possède un diviseur irréductible de degré strictement inférieur à* $d(P)$.

Démonstration. On note $A = \{Q \in D(P) | d(Q) \geq 1\}$, puis $\Delta = \{d(R) | R \in A\}$. Comme P est non constant, A contient P, donc est non vide. On en déduit que Δ est une partie non vide de $\mathbb{N}^*$. Elle possède donc un minimum r et il existe un polynôme R non constant de degré r minimal qui divise P. Montrons que R est irréductible. Soit D un diviseur de R, par transitivité de la relation de divisibilité, D divise P. Si D n'est pas constant, alors D appartient à A. Par minimalité de r, $d(D) \geq r$. D'autre part, D divise R, donc $d(D) \leq r$. Ainsi, D et R sont associés. Ainsi, les seuls factorisations de R sont triviales et R est irréductible.

Théorème 8 *Soit* $P \in \mathbb{K}[X]$ *non constant. Alors* P *se décompose de manière unique à l'ordre près en produit d'un scalaire non nul et de polynômes irréductibles unitaires.*

Démonstration. Existence par récurrence forte sur le degré. Soit P un polynôme de degré 1. Il est de la forme $\alpha(X-\beta)$ avec α non nul et $X-\beta$ unitaire irréductible. Soit n un entier naturel non nul tel que la propriété est vraie pour tous les polynômes de degré inférieur à n. Soit P un polynôme de degré $n+1$. Alors si P est irréductible, c'est fini, sinon P admet un diviseur irréductible Q unitaire de degré strictement plus petit d'après la propriété précédente. Écrivons alors $P = QR$ avec $d(R) < d(P)$. On applique la propriété de récurrence à R. On regroupe alors les facteurs irréductibles pour obtenir une factorisation de P adéquate.
Unicité par récurrence forte sur le nombre de termes. S'il n'y a qu'un terme irréductible dans la factorisation, il est unique car égal à P divisé par son coefficient dominant. Supposons qu'on ait $P = \alpha Q_1 \dots Q_k = \beta R_1 \dots R_m$. Si R_1 était premier avec tous les Q_i, alors il serait premier avec leur produit P, ce qui est absurde. Quitte à appliquer une permutation des Q_i, on peut supposer que R_1 n'est pas premier avec Q_1. Mais alors R_1 et Q_1 sont associés car l'un divise l'autre et ils sont tous deux non constants. Comme ils sont unitaires, ils sont égaux. Par intégrité, on est ramené à $Q_2 \dots Q_k = R_2 \dots R_m$.

☞ **Remarque**
On dit que l'anneau $\mathbb{K}[X]$ *est factoriel.*

Notation
Je note l'ensemble des polynômes irréductibles unitaires de $\mathbb{K}[X]$, $\mathcal{I}(\mathbb{K})$

Propriété 33 *Soit* $P \in \mathbb{K}[X]$ *non nul. Alors, il existe un unique scalaire non nul* λ*, une unique famille* $(\nu_R(P))_{R\in\mathcal{I}(\mathbb{K})}$ *à support fini telle que*

$$P = \lambda \prod_{R\in\mathcal{I}(\mathbb{K})} R^{\nu_R(P)}$$

Démonstration. Le scalaire λ n'est rien d'autre que le coefficient dominant de P. Pour tout irréductible unitaire R, $\nu_R(P)$ est l'exposant du polynôme R dans la décomposition de P en produit d'irréductibles unitaires (0 s'il n'y apparaît pas).

Théorème 9 (Théorème de D'Alembert-Gauss) *Soit* $P \in \mathbb{C}[X]$ *non constant. Alors* P *admet une racine.*

Démonstration. Admis pour l'instant. On pourra le démontrer avec quelques outils supplémentaires d'analyse.

Propriété 34 *Soit* $P \in \mathbb{C}[X]$ *non constant. Alors* P *est scindé*

Démonstration. On établit ce résultat par récurrence sur le degré de P. Soit P de degré 1. Alors il est clair que P est scindé. Soit n un entier naturel non nul tel que le résultat est vrai. Soit P un polynôme de degré $n+1$. D'après le théorème de D'Alembert-Gauss, P admet une racine a, donc $X-a$ divise P. On écrit alors $P = (X-a)Q$, ce qui implique que $d(Q) = n$. On lui applique l'hypothèse de récurrence. Q est alors produit de polynômes de degré 1. En regroupant avec $X-a$, P s'écrit comme produit de polynômes de degré 1.

Propriété 35 *Les polynômes irréductibles de* $\mathbb{C}[X]$ *sont les polynômes de degré* 1*.*

Démonstration. Soit P un polynôme irréductible de $\mathbb{C}[X]$. Il est non constant par définition des irréductibles. D'après le théorème de D'Alembert-Gauss, il possède une racine a. Mais alors $X-a$ divise P et $X-a$ n'est pas constant. Par conséquent, P est associé à $X-a$ et P est de degré 1. La réciproque a déjà été mentionnée.

Propriété 36 *Soit* $P \in \mathbb{C}[X]$ *non constant. On note* $Z(P) = \{a_1, \dots, a_n\}$ *l'ensemble de ses racines sans répétition et pour tout entier* i *dans* $[\![1, n]\!]$, α_i *la multiplicité de* a_i *dans* P*, puis* λ *le coefficient dominant de* P*. Alors*

$$P = \lambda \prod_{i=1}^{n} (X-a_i)^{\alpha_i}$$

Démonstration. On connaît la liste des irréductibles unitaires dans $\mathbb{C}[X]$: il s'agit des polynômes $(X-a)_{a\in\mathbb{C}}$. Or $X-a$ divise P ssi a est racine de P. Donc les polynômes apparaissant dans la décomposition en produits d'unitaires irréductibles sont les $(X-a_i)_{1\leq i\leq n}$. D'après la définition de la multiplicité des racines, pour tout i dans $[\![1, n]\!]$, $(X-a_i)^{\alpha_i}$ divise P et non $(X-a_i)^{\alpha_i+1}$. Il reste alors simplement à reconnaître le coefficient dominant de P en facteur.

Propriété 37 *Soit* $(P, Q) \in \mathbb{C}[X]^2$ *tous deux non nuls. On note* $Z(P)$ *et* $Z(Q)$ *les ensembles de leurs racines respectives. Alors* P *divise* Q *si et seulement si* $Z(P) \subset Z(Q)$ *et pour tout racine* a *de* P*, sa multiplicité dans* P *est inférieure ou égale à sa multiplicité dans* Q*.*

Démonstration. Si P divise Q, soit $a \in Z(P)$ de multiplicité α alors $(X-a)^\alpha$ divise P donc divise Q par transitivité. Ainsi, a est une racine de Q de mutliplicité au moins α. Réciproquement, si l'on a la condition sur les racines, comme on travaille dans $\mathbb{C}[X]$, on peut factoriser les polynômes P et Q comme précédemment, on dispose alors de complexes $(a_1,\dots,a_p,a_{p+1},\dots,a_n)$, d'entiers naturels non nuls $\alpha_1,\dots,\alpha_p$, $\beta_1,\dots\beta_n$ tels que $\forall i[\![1,p]\!], \alpha_i \leq \beta_i$, de complexes non nuls λ et μ tels que

$$P = \lambda \prod_{i=1}^{p} (X-a_i)^{\alpha_i} \quad \text{et} \quad Q = \mu \prod_{i=1}^{n} (X-a_i)^{\beta_i}$$

Mais alors

$$Q = \prod_{i=p+1}^{n} (X-a_i)^{\beta_i} \prod_{i=1}^{p} (X-a_i)^{\beta_i-\alpha_i} P$$

donc P divise Q.

Propriété 38 *Soit* $(P,Q) \in \mathbb{C}[X]^2$ *tous deux non nuls. On a l'équivalence*

$$P \wedge Q = 1 \iff Z(P) \cap Z(Q) = \emptyset$$

Autrement dit, P *et* Q *sont premiers entre eux si et seulement si ils n'ont aucune racine commune.*

Démonstration. Si P et Q ont une racine commune, alors la propriété précédente, montre qu'ils possèdent un diviseur de la forme $X-a$, donc P et Q ne sont pas premiers entre eux. Réciproquement, s'ils n'ont aucune racine commune, alors comme $\forall (a,b) \in \mathbb{C}^2, \forall (p,q) \in \mathbb{N}^2, (X-a)^p \wedge (X-b)^q = 1$, on en déduit via la propriété 27 et l'exemple 6 que P et Q sont premiers entre eux.

Propriété 39 *Les polynômes irréductibles de* $\mathbb{R}[X]$ *sont les polynômes de degré* 1 *et les polynômes de degré* 2 *de discriminant strictement négatif.*

Démonstration. Soit $P \in \mathbb{R}[X]$ irréductible. Supposons $d(P) \geq 2$. On peut voir P comme élément de $\mathbb{C}[X]$. Alors P admet une racine complexe α d'après le théorème de D'Alembert-Gauss. Mais alos comme P est à coefficients réels, $\overline{P(\alpha)} = P(\overline{\alpha}) = 0$, donc $\overline{\alpha}$ est une racine de P. D'autre part, α n'est pas réel car sinon P n'est pas irréductible, donc $\alpha \neq \overline{\alpha}$. On en déduit que $(X-\alpha)(X-\overline{\alpha})$ divise P, ce que l'on écrit

$$P = (X - 2\mathfrak{Re}(\alpha) + |\alpha|^2)Q$$

avec $Q \in \mathbb{C}[X]$. On reconnaît toutefois la division euclidienne de P de $(X - 2\mathfrak{Re}(\alpha) + |\alpha|^2)$ dans $\mathbb{R}[X]$, donc Q est à coefficients réels. Cette factorisation de P irréductible dans $\mathbb{R}[X]$ implique que Q est constant non nul. Ainsi, P est un polynôme de degré 2, et son discriminant vaut $Q^2(4\mathfrak{Re}(\alpha)^2 - 4|\alpha|^2) < 0$.

5 Corps des fractions rationnelles à une indéterminée.

L'objectif de cette section est moins algébrique et plus calculatoire.

5.1 Opérations dans $\mathbb{K}(X)$.

On « définit » le corps des fractions de $\mathbb{K}[X]$ comme l'ensemble quotient de $\mathbb{K}[X] \times \mathbb{K}[X]^*$ par la relation d'équivalence

$$(P,Q)\mathcal{R}(S,T) \iff PT = RS$$

La classe de (P,Q) est alors noté P/Q ou $\frac{P}{Q}$. Vous êtes priés de bien vouloir croire que cela fournit un corps qui prolonge toutes les opérations de $\mathbb{K}[X]$. Il est noté $\mathbb{K}(X)$.

Propriété 40 *Soit $F \in \mathbb{K}(X)$. Alors il existe un unique couple $(P,Q) \in \mathbb{K}[X] \times \mathbb{K}[X]^*$ avec Q unitaire tel que $F = P/Q$ et $P \wedge Q = 1$. Cette écriture unique est appelée forme irréductible de F.*

Démonstration. D'après la définition d'une fraction rationnelle, il existe $(A,B) \in \mathbb{K}[X]\times\mathbb{K}[X]^*$ tel que $F = A/B$. On pose alors $D = A \wedge B$, ce qui permet d'écrire $A = DA_1$, $B = DB_1$ et $A_1 \wedge B_1 = 1$. Comme B est non nul, D et B_1 sont non nuls, on simplifie alors $F = A_1/B_1$. On pose alors $Q = B_1/b_1$ avec b_1 le coefficient dominant de B_1 et $P = A_1/b_1$, ce qui fournit un couple convenable puisque b_1 est non nul. Soit (P_1,Q_1) un autre couple convenable. Alors $Q_1P = P_1Q$. D'après le lemme de Gauss, Q_1 divise Q et Q divise Q_1. Ils sont alors associés et tous deux unitaires, donc égaux. Par intégrité de $\mathbb{K}[X]$, on en déduit que $P = P_1$.

Définition 21 *Soit $F \in \mathbb{K}(X)$ et P/Q sa forme irréductible. Alors les zéros de P sont appelés les zéros de F, tandis que les zéros de Q sont appelés les pôles de F. La multiplicité d'un pôle de F est la multiplicité de ce réel comme racine de Q.*

Définition 22 *Soit $F \in \mathbb{K}(X)$ et P/Q sa forme irréductible. Alors $\tilde{F} : \mathbb{K}\backslash Z(Q), x \mapsto P(x)/Q(x) = F(x)$ est appelée fonction rationnelle associée à F.*

Définition 23 *Soit $F \in \mathbb{K}(X)$ et P/Q sa forme irréductible. Alors $d(P) - d(Q)$ est appelé le degré de F, noté $d(F)$ (avec la convention $-\infty - n = -\infty$.)*

Propriété 41 *Soit $(F,G) \in K(X)^2$. Alors*

- *Le degré de F est indépendant des polynômes P,Q tels que $F = P/Q$.*
- *$d(FG) = d(F) + d(G)$*
- *Si G est non nul, $d(F/G) = d(F) - d(G)$.*

Démonstration.
- Soit P_1,Q_1,P_2,Q_2 des polynômes tels que $F = P_1/Q_1 = P_2/Q_2$. Alors $P_1Q_2 = P_2Q_1$ et d'après les propriétés sur les degrés de polynômes, on a $d(P_1) + d(Q_2) = d(P_2) + d(Q_1)$. Comme Q_1 et Q_2 sont non nuls, on peut soustraire $d(Q_1)$ et $d(Q_2)$, donc $d(P_1) - d(Q_1) = d(P_2) - d(Q_2)$. Ainsi, le degré de F est indépendant des représentants polynomiaux de F.
- On écrit $F = P/Q$ et $G = A/B$ avec des polynômes. Cela implique $FG = (PA)/(QB)$ avec PA et QB des polynômes. On en déduit que $d(FG) = d(PA) - d(QB) = d(P) + d(A) - d(Q) - d(B) = d(P) - d(Q) + d(A) - d(B) = d(F) + d(G)$.
- Il suffit de constater que $\frac{F}{G}G = F$, donc que $d(F/G) + d(G) = d(F)$ d'après ce qui précède. On en déduit puisque $d(G) \neq -\infty$ que $d(F/G) = d(F) - d(G)$.

Définition 24 *Soit $F \in \mathbb{K}(X)$ de forme irréductible P/Q. On définit alors la dérivée (formelle) de F via $\frac{P'Q-PQ'}{Q^2}$.*

Propriété 42 *La dérivée formelle est indépendante des représentants polynomiaux de F*

Démonstration. On note $F = A/B = P/Q$ deux formes de F. Alors, $AQ = PB$, et la dérivation des polynômes implique $A'Q + AQ' = P'B + PB'$. On en déduit que

$$(A'B-B'A)Q^2 = (A'Q)(BQ)-(B'Q)(AQ) = (P'B+PB'-AQ')(BQ)-(B'Q)(BP) = BQ(P'B-AQ') = B^2QP'-PBBQ' = B^2(P'Q-Q'P)$$

Propriété 43 *Soit* $(F,G) \in (\mathbb{K}[X])^2, \lambda \in \mathbb{K}[X]$.

- *Linéarité :* $(F+\lambda G)' = F' + \lambda G'$
- *Leibniz :* $(FG)' = F'G + FG'$.
- *Si* F *est non nul,* $\left(\frac{1}{F}\right)' = -\frac{F'}{F^2}$.
- *Si* G *est non nul,* $\left(\frac{F}{G}\right)' = \frac{F'G - FG'}{G^2}$.
- $d(F') \leq d(F) - 1$.

Démonstration. Laissée à titre d'exercice.

5.2 Décomposition en éléments simples

Définition 25 *Soit* $F \in \mathbb{K}(X)$ *et* P/Q *sa forme irréductible. On appelle partie entière de* F*, le quotient dans la division euclidienne de* P *par* Q.

Propriété 44 *Soit* $F \in \mathbb{K}(X)$ *et* P/Q *sa forme irréductible. On note* $P = EQ + R$ *la division euclidienne de* P *par* Q. *Alors*

$$F = E + \frac{R}{Q}$$

avec $d(E) \geq 0$ *et* $d(R/Q) < 0$.

Démonstration. Il suffit d'écrire la division euclidienne de P par Q, $P = QE + R$. Alors $F = E + R/Q$. De plus, $d(R) < d(Q)$ comme c'est un reste de diviseur Q, donc $d(R/Q) = d(R) - d(Q) < 0$.

Notre objectif est de décomposer la fraction R/Q en somme de fraction rationnelles les plus simples possibles, cela s'appelle effectuer la décomposition en éléments simples de F.

Définition 26 *On appelle élément simple toute fraction rationnelle de la forme* Q/P^k *avec* $Q \in \mathbb{K}[X]$, $P \in \mathbb{K}[X]$ *irréductible,* $k \in \mathbb{N}^*$ *et* $d(Q) < d(P)$.

Exemple 8 *Dans* $\mathbb{R}[X]$*, les éléments simples sont de la forme* $a/(X-\lambda)^k$ *et* $(bX+c)/(X^2+\alpha X+\beta)^k$ *avec* $\alpha^2 - 4\beta < 0$. *Dans* $\mathbb{C}[X]$*, les éléments simples sont de la forme* $\mu/(X-\nu)^k$.

Théorème 10 (Division par puissances croissantes) *Soit* $(A,B) \in \mathbb{K}[X]^2$ *tel que* $B(0) \neq 0$*, puis* $n \in \mathbb{N}$. *Alors*

$$\exists!(Q,R) \in (\mathbb{K}[X])^2, \quad A = BQ + X^{n+1}R, \quad d(Q) \leq n$$

Démonstration. On note $A = \sum_{k=0}^{+\infty} a_k X^k$ et $B = \sum_{k=0}^{+\infty} b_k X^k$. Prouvons l'existence par récurrence sur l'entier n. Pour $n = 0$, on pose $Q = a_0/b_0$, ce qui est possible puisque $b_0 = B(0) \neq 0$. Dans ce cas, $A - BQ_0$ est divisible par X puisque nul en 0, il suffit d'écrire $A - BQ_0 = XR_0$. Soit n un entier naturel tel que (Q_n, R_n) est construit comme souhaité. Construisons un couple (Q_{n+1}, R_{n+1}) satisfaisant. On applique la division par puissances croissantes à l'ordre 0 au couple (R_n, B), ce qui est possible puisque $B(0) \neq 0$, cela fournit un couple (k, T) avec k un scalaire (un polynôme constant) et T un polynôme tels que $R_n = kB + XT$. On en déduit que

$$A = BQ_n + X^{n+1}(kB + XT) = B(Q_n + kX^{n+1}) + X^{n+2}T$$

On pose alors $Q_{n+1} = Q_n + kX^{n+1}$ qui vérifie bien $d(Q_{n+1}) \leq \max(n, n+1) \leq n+1$ et $R_{n+1} = T$.
Unicité. Soit $(Q_1, R_1), (Q_2, R_2)$ deux couples satisfaisants. On a alors $B(Q_1 - Q_2) + X^{n+1}(R_1 - R_2) = 0$, donc X^{n+1} divise $B(Q_1 - Q_2)$. Or comme $B(0) \neq 0$, B n'est pas divisible par X. Comme X est irréductible, X est premier avec B. D'après le lemme de Gauss, X^{n+1} divise $Q_1 - Q_2$. Or $d(Q_1 - Q_2) \leq n$, donc $Q_1 - Q_2 = 0$. Comme X^{n+1} n'est pas le polynôme nul, on en déduit par intégrité que $R_1 = R_2$.

Exemple 9 *Il suffit d'utiliser la disposition classique de la division euclidienne en renversant l'ordre des coefficients en s'arrêtant à l'ordre indiqué.*

$$1 + X = (1 + X^2)(1 + X - X^2) + X^3(X - 1)$$

Théorème 11 (décomposition en éléments simples) *Soit* $F \in \mathbb{K}(X)$ *et* P/Q *sa forme irréductible. On note* E *la partie entière de* F *et* $Q = Q_1^{\alpha_1} \dots Q_n^{\alpha_n}$ *la décomposition de* Q *en facteurs irréductibles unitaires dans* $K[X]$. *Alors il existe une unique famille de polynômes* $(P_{i,j})_{1 \leq i \leq n, 1 \leq j \leq k_i}$ *telle que*

$$F = E + \sum_{i=1}^{n} \sum_{j=1}^{\alpha_i} \frac{P_{i,j}}{Q_i^j} \quad et \quad \forall (i,j) \in [\![1,n]\!] \times [\![1,\alpha_i]\!], d(P_{i,j}) < d(Q_i).$$

La démonstration est hors-programme, je vais la décomposer en trois morceaux. Je note $\mathcal{I}$ l'ensemble des polynômes unitaires irréductibles dans $\mathbb{K}[X]$

Lemme 2 *Soit* $P \in \mathcal{I}$, *d son degré et* $n \in \mathbb{N}^*$. *Soit* $Q \in \mathbb{K}[X]$, *alors il existe un unique n-uplet de polynômes* $(R_0, R_1, \dots, R_{n-1}) \in (\mathbb{K}[X])^n$, *tel que* $\forall i \in [\![0, n-1]\!], d(R_i) < d$ *et* $R_0 + R_1 P + \dots R_{n-1} P^{n-1}$ *est le reste dans la division euclidienne de* Q *par* P^n.

Démonstration. Si des polynômes (R_i) vériifent ces conditions, $d(R_0 + R_1 P + \dots R_{n-1} P^{n-1}) < d(P^n)$. Alors si un autre couple vérifie ces conditions, leur différence est muliple de P^n de degré strictement inférieur à $d(P^n)$, donc est nulle. L'existence est prouvée par récurrence sur n. Si $n = 1$, on choisit R_0 le reste dans la division euclidienne de Q par P. Sinon, on fixe $n \geq 2$. On dispose de l'écriture $Q = (R_0 + R_1 P + \dots R_{n-2} P^{n-2}) + S P^{n-1}$. On effectue alors la division euclidienne de S par P, ce qui fournit $S = PT + R_{n-1}$ avec $d(R_{n-1}) < d$.

Lemme 3 *Soit* $A \in \mathbb{K}[X], n \in \mathbb{N}^*, P \in \mathcal{I}$ *premier avec* A. *Il existe une unique suite* $(R_0, R_1, \dots, R_n) \in \mathbb{K}[X] \times (K_{n-1}[X])^{n-1}$ *telle que*

$$\frac{A}{P^n} = R_0 + \frac{R_1}{P} + \dots + \frac{R_n}{P^n} \quad et \quad R_n \neq 0$$

Démonstration. Cette condition équivaut à

$$A = R_0 P^n + R_1 P^{n-1} + R_{n-1} P + R_n$$

Or A est premier avec P donc R_n est non nul.

Lemme 4 *Soit* $F \in \mathbb{K}(X)$. *Il existe une partie finie* $\mathcal{H}$ *de* $\mathcal{I}$, $E \in \mathbb{K}[X]$, *des entiers strictement positifs* n_P *et des polynômes* A_P, *non divisibles par* P *pour* $P_i n \mathcal{H}$, *tels que :*

$$A = E + \sum_{P \in \mathcal{H}} \frac{A_P}{P^{n_P}}$$

L'ensemble $\mathcal{H}$ *et les entiers* n_P *sont uniquement déterminés par ces conditions.*

Démonstration. Existence : si $F \in \mathbb{K}[X]$, $E = F$ et $\mathcal{H} = \emptyset$ conviennent. Supposons $F \notin \mathbb{K}[X]$, A/B une forme irréductible de F. D'après la factorialité de $\mathbb{K}[X]$, il existe un entier non nul s, $P_1, \dots, P_s) \in \mathcal{I}^s$, des entiers strictement positifs $n_1, \dots, n_s$ tels que $B = P_1^{n_1} \dots P_s^{n_s}$. Si $s = 1$, c'est clair en effectuant la division euclidienne de A par B. Supposons $s > 1$. Pour $1 \leq i \leq s$, on pose $Q_i = \prod_{j \neq i} P_j^{n_j}$. Ces polynômes sont premiers dans leur ensemble. Il existe donc s polynômes $(S_i)_i$ tels que $S_1 Q_1 + \dots + S_s Q_s = 1$. Il est clair que, pour tout entier i, S_i et P_i sont premiers entre eux. On a alors

$$F = \frac{S_1 A}{P_1^{n_1}} + \dots + \frac{S_s A}{P_s^{n_s}}$$

On en déduit imméditamat par division euclidienne de $S_i A$ par $P_i^{n_i}$ une décomposition du type souhaité.
Unicité : Supposons que F s'écrit sous la forme écrite et A/B la forme irréductible de F. On pose Δ le produit des P^{n_P} pour $P \in \mathcal{H}$ et Δ_P le produit des Q^{n_Q} pour $Q \in \mathcal{H} \backslash \{P\}$. Il vient

$$\Delta A = \Delta E + \sum_{P \in \mathcal{H}} A_P B \Delta_P$$

Les diviseurs irréductibles sont les $P \in \mathcal{H}$. D'autre part, si $P \in \mathcal{H}$, les polynômes $\Delta_P A_P$ et P sont premiers entre eux. On en déduit que P^{n_P} divise B, puis que Δ divise B. De même, A et B sont premiers entre eux, on voit que B divise Δ. Comme ils sont tous deux unitaires, $\Delta = B$. Ceci prouve que $\mathcal{H}$ et les n_P sont uniquement déterminés.

On arrive enfin à la démonstration du théorème :

Démonstration. L'existence vient d'être prouvée d'après les deux résultats précédentes. Pour l'unicité, la preuve du résultat précédent indique que Q est le produit des $Q_i^{\alpha_i}$, ce qui établit l'unicité des Q_i et des α_i. Cela établit l'unicité des Q_i et des α_i. Il est alors clair que E est le quotient dans la division euclidienne de P/Q. Ainsi E est uniquement déterminé. Fixons $i \in [\![1,n]\!]$, soit Q le produit des $Q_j^{\alpha_j}$ pour $j \neq i$. On mutliplie deux telles décompositions par Q, il résulte alors du second lemme l'unicité des $P_{i,j}$.

Exemple 10 *En utilisant la division par puissances croissantes,*

$$\frac{1+X}{X^3(1+X^2)} = \frac{(1+X^2)(1+X-X^2)+X^3(X-1)}{X^3(1+X^2)} = \frac{1}{X^3}+\frac{1}{X^2}-\frac{1}{X}+\frac{X-1}{X^2+1}$$

Exemple 11 *Quelques exemples de décompositions en éléments simples dans* $\mathbb{R}[X]$ *et* $\mathbb{C}[X]$.

1.

$$\frac{1}{1-X^2} = \frac{1/2}{1-X}+\frac{1/2}{1+X}$$

2.

$$\frac{X}{1-X^2} = \frac{1/2}{1-X}-\frac{1/2}{1+X}$$

3.

$$F = \frac{1}{(X-1)(X+3)^2} = \frac{a}{X-1}+\frac{b}{X+3}+\frac{c}{(X+3)^2}$$

On évalue $(F(X-1))(1) = \frac{1}{4^2} = a$, $(F(X+3)^2)(-3) = \frac{1}{-4} = c$. *Si l'on note* $G = \frac{1}{X-1} = F(X+3)^2 = a\frac{(X+3)^2}{X-1} + b(X+3)+c$, *la dérivée de* G *donne*

$$G' = -\frac{1}{(X-1)^2} = a(X+3)R+b$$

On évalue cette dernière fraction rationnelle en -3, *ce qui donne* $b = -1/16$. *Au final, on a*

$$\frac{1}{(X-1)(X+3)^2} = \frac{1/16}{X-1}+\frac{-1/16}{X+3}+\frac{-1/4}{(X+3)^2}$$

4. Dans $\mathbb{R}[X]$,

$$F = \frac{X^2+4}{(X^2+1)^2} = \frac{aX+b}{X^2+1}+\frac{cX+d}{(X^2+1)^2}$$

On remarque que F *est paire, i.e* $F(-X) = F(X)$. *Mais alors, on a*

$$F = \frac{-aX+b}{X^2+1}+\frac{-cX+d}{(X^2+1)^2}$$

Par unicité de la décomposition en éléments simples, $a = -a$ *et* $c = -c$, *donc* $a = 0$ *et* $c = 0$. *De plus, on évalue* $F(X^2+1)^2$ *en i ce qui entraîne* $d = -1+4 = 3$. *On écrit de plus la limite de* X^2F *quand* X *tend vers* $+\infty$, *ce qui entraîne* $1 = b$. *En conclusion,*

$$F = \frac{1}{X^2+1}+\frac{3}{(X^2+1)^2}$$

Propriété 45 *Soit* $F \in \mathbb{K}(X)$ *et* P/Q *sa forme irréductible. Soit* λ *un pôle simple de* F, *i.e une racine simple de* Q. *Alors le coefficient de l'élément simple* $\frac{1}{X-\lambda}$ *dans la décomposition en éléments simples de* F *vaut* $P(\lambda)/Q'(\lambda)$.

Démonstration. On écrit la décomposition en éléments simples $F = \frac{\alpha}{X-\lambda}+R$ avec $\mathbb{R} \in \mathbb{K}(X)$ de pôles distincts de λ et $\alpha \in \mathbb{K}$. Après multiplication par $X-\lambda$ et B on obtient,

$$P(X-\lambda) = \alpha Q + R(X-\lambda)Q$$

Après dérivation, on a

$$P+P'(X-\lambda) = \alpha Q' + RQ + (X-\lambda)R'Q + (X-\lambda)RQ'$$

On évalue le tout en λ. Comme R ne possède pas λ comme pôle et $Q(\alpha) = 0$, cela entraîne

$$P(\lambda)+0 = \alpha Q'(\lambda)+0$$

D'autre part, $Q'(\lambda)$ est non nul car λ est pôle simple de F. Ainsi, $\alpha = P(\lambda)/Q'(\lambda)$.

Propriété 46 *Soit* $P \in \mathbb{K}[X]$ *non nul scindé. On l'écrit sous la forme* $P = \lambda(X-\alpha_1)^{k_1}\dots(X-\alpha_n)^{k_n}$. *Alors*

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

Démonstration. On a déjà vu la dérivée de ce genre de polynômes :

$$P' = \sum_{i=1}^{n} k_i (X-a_i)^{k_i-1} \prod_{\substack{j=1 \\ j\neq i}}^{n} (X-a_j)^{k_j} = \sum_{i=1}^{n} k_i \frac{P}{X-a_i} = P \sum_{i=1}^{n} \frac{k_i}{X-a_i}$$

On en déduit

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

Les physiciens parlent parfois de dérivée logarithmique.

Exercice 1 (Théorème de Gauss-Lucas) *Soit* $P \in \mathbb{C}[X]$ *non constant. Montrer que les racines de* P' *sont des combinaisons linéaires convexes de racines de* P*, en exploitant la décomposition en éléments simples de* P'/P.