Université de Provence	2011–2012

Mathématiques Générales I

PARCOURS PEIP

COURS : POLYNÔMES

Sauf mention contraire, nous travaillerons, dans ce chapitre, avec $\mathbb{K}$ qui pourra être égal à $\mathbb{R}$ ou à $\mathbb{C}$.

1 Polynômes

Définition 1. On appelle polynôme en l'indéterminée X toute expression $P(X)$ de la forme

$$P(X) := a_0 + a_1X + a_2X^2 + \cdots + a_nX^n = \sum_{k=0}^{n} a_kX^k,$$

avec $n \in \mathbb{N}$ et, pour tout $k \in [\![0, n]\!]$, $a_k \in \mathbb{K}$.
On note $\mathbb{K}[X]$ l'ensemble des polynômes en l'indéterminée X.

Remarque 2. Ici, X est une indéterminée. Il s'agit d'une notation pour un polynôme élémentaire générateur de $\mathbb{K}[X]$. Il ne s'agit ni d'une inconnue dans une équation que nous souhaiterions résoudre, ni d'une variable vouée à prendre une quelconque valeur (voir Déf. 4). Lorsqu'il n'y a pas d'ambiguité sur l'indéterminé X, on pourra noter P pour $P(X)$.

Définition 3. Soit $P(X) = \sum_{k=0}^{n} a_kX^k \in \mathbb{K}[X]$. On dit que les a_k, pour $k \in [\![0, n]\!]$, sont les coefficients de $P(X)$.
On appelle monôme tout polynôme ne possédant qu'un unique coefficient non nul.

Définition 4. A tout $P(X) = \sum_{k=0}^{n} a_kX^k \in \mathbb{K}[X]$, on peut associer l'application polynomiale définie par

$$f_P : \begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K} \\ x & \longmapsto & \displaystyle\sum_{k=0}^{n} a_kx^k \end{array}.$$

Remarque 5. Les deux objets, $P(X)$ et f_P sont de nature très différentes. L'un, $P(X)$, est algébrique et permet toute une théorie arithmétique des polynômes ; tandis que l'autre, f_P, procède plus de l'analyse, permettant des études de type variationnel. Une grande partie de la richesse des polynômes vient de cette confluence des deux approches. Par abus de notation, l'application polynomiale peut être notée P et l'on pourra voir écrit, par exemple, $P(1)$ pour $f_P(1)$. Il ne faut cependant pas perdre de vue qu'il s'agit, en réalité, de l'évaluation en 1 de l'application polynomiale associée à $P(X)$.

Par analogie avec les applications polynomiales associées, on définit, sur $\mathbb{K}[X]$, les opérations suivantes.

Définition 6. Soit $P(X) = \displaystyle\sum_{k=0}^{n} a_kX^k$ et $Q(X) = \displaystyle\sum_{k=0}^{m} b_kX^k$ deux polynômes. Par convention, on pose $a_i = b_j = 0$ pour tout $i \notin [\![0, n]\!]$ et $j \notin [\![0, m]\!]$.

i. On définit $P(X) + Q(X) := \displaystyle\sum_{k=0}^{\max(n,m)} c_kX^k$ avec, pour tout $k \in [\![0, \max(n, m)]\!]$, $c_k := a_k + b_k$.

ii. On définit $P(X).Q(X) := \displaystyle\sum_{k=0}^{n+m} c_kX^k$ avec, pour tout $k \in [\![0, n + m]\!]$, $c_k := \displaystyle\sum_{i=0}^{k} a_ib_{k-i}$.

iii. On définit $P'(X) := \displaystyle\sum_{k=0}^{n-1} c_k X^k$ avec, pour tout $k \in [\![0, n-1]\!]$, $c_k := (k+1)a_{k+1}$.

Proposition 7. *Pour tous polynômes $P(X), Q(X), R(X) \in \mathbb{K}[X]$, on a*

i.	$P(X) + \big(Q(X) + R(X)\big) = \big(P(X) + Q(X)\big) + R(X)$;	*(associativité de +)*
ii.	$P(X) + Q(X) = Q(X) + P(X)$;	*(commutativité de +)*
iii.	$P(X).\big(Q(X).R(X)\big) = \big(P(X).Q(X)\big).R(X)$;	*(associativité de .)*
iv.	$P(X).Q(X) = Q(X).P(X)$;	*(commutativité de .)*
v.	$P(X).\big(Q(X) + R(X)\big) = P(X).Q(X) + P(X).R(X)$;	*(distributivité de + sur .)*
vi.	$\big(P(X) + Q(X)\big)' = P'(X) + Q'(X)$;	*(linéarité de la dérivation)*
vii.	$\big(P(X).Q(X)\big)' = P'(X).Q(X) + P(X).Q'(X)$;	*(identité de Leibniz).*

Démonstration. Chacune de ces propositions se démontre en prenant des notations pour les coefficients de $P(X)$, $Q(X)$ et, si nécessaire, $R(X)$. On utilise alors les définitions pour expliciter les coefficients des deux polynômes situés de chaque coté de l'égalité. On remarque enfin que ces coefficients sont les mêmes.

Traitons, par exemple, l'identité de Leibniz. On écrit $P(X) = \sum_{k=0}^{n} a_k X^k$ et $Q(X) = \sum_{k=0}^{m} b_k X^k$. On a alors $P'(X) = \sum_{k=0}^{n-1}(k+1)a_{k+1}X^k$ et $Q'(X) = \sum_{k=0}^{m-1}(k+1)b_{k+1}X^k$. On a donc $P'(X).Q(X) = \sum_{k=0}^{n+m-1} c_k X^k$ avec $c_k = \sum_{i=0}^{k}(i+1)a_{i+1}b_{k-i}$ et $P(X).Q'(X) = \sum_{k=0}^{n+m-1} c'_k X^k$ avec $c'_k = \sum_{i=0}^{k}(k-i+1)a_i b_{k-i+1}$.
On en déduit $P'(X).Q(X) + P(X).Q'(X) = \sum_{k=0}^{n+m-1} d_k X^k$ avec

$$\begin{aligned}
d_k = c_k + c'_k &= \sum_{i=0}^{k}(i+1)a_{i+1}b_{k-i} + \sum_{i=0}^{k}(k-i+1)a_i b_{k-i+1} \\
&= \sum_{i=1}^{k+1} i a_i b_{k-i+1} + \sum_{i=0}^{k}(k-i+1)a_i b_{k-i+1} \\
&= (k+1)a_{k+1}b_0 + \left(\sum_{i=1}^{k}(i a_i b_{k-i+1} + (k-i+1)a_i b_{k-i+1})\right) + (k+1)a_0 b_{k+1} \\
&= (k+1)a_{k+1}b_0 + \left(\sum_{i=1}^{k}((k+1)a_i b_{k-i+1}\right) + (k+1)a_0 b_{k+1} \\
&= (k+1)\sum_{i=0}^{k+1} a_i b_{k-i+1}.
\end{aligned}$$

De l'autre coté, on a $P(X).Q(X) = \sum_{k=0}^{n+m} e_k X^k$ avec $e_k = \sum_{i=0}^{k} a_i b_{k-i}$. Et donc $\big(P(X).Q(X)\big)' = \sum_{k=0}^{n+m-1} f_k X^k$ avec $f_k = (k+1)e_{k+1}$ et donc $f_k = (k+1)\sum_{i=0}^{k+1} a_i b_{k+1-i}$. On a donc $f_k = d_k$ et de fait $\big(P(X).Q(X)\big)' = P'(X).Q(X) + P(X).Q'(X)$. □

Remarque 8. Toutes les calculs "usuels" sont donc licites sur les polynômes. En particulier, les formules ne découlant que de la distributivité de l'addition sur la multiplication restent vraies.

Corollaire 9 (binôme de Newton)**.** *Soit $P(X), Q(X) \in \mathbb{K}[X]$ et $n \in \mathbb{N}$, alors*

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

Corollaire 10. *Avec les notations de la définition 4, on a, pour tous $P(X), Q(X) \in \mathbb{K}[X]$, $f_{P+Q} = f_P + f_Q$, $f_{P.Q} = f_P.f_Q$ et $f_{P'} = f'_P$.*

Remarque 11. Cette dernière proposition justifie l'amalgame entre les notations P et f_P.

2 Degré et valuation

Définition 12. On définit le degré de tout polynôme $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ non nul, noté $\deg(P)$, par $\max\{k \in [\![0, n]\!] | a_k \neq 0\}$. Par convention, le degré du polynôme nul vaut $-\infty$.
On appelle $a_{\deg(P)}$ le coefficient dominant de $P(X)$.
On dit que $P(X)$ est unitaire si son coefficient dominant est unitaire.

Proposition 13. *Soit $P(X), Q(X) \in \mathbb{K}[X]$ non nuls. Alors $\deg(P.Q) = \deg(P) + \deg(Q)$, $\deg(P + Q) \leq \max\big(\deg(P), \deg(Q)\big)$ et, si $\deg(P) \geq 1$, $\deg(P') = \deg(P) - 1$.*

Remarque 14. Concernant le degré d'une somme, l'inégalité peut être stricte si les polynômes sont de même degré avec des coefficients dominants opposés l'un à l'autre.

Démonstration. On pose $n := \deg(P)$ et $m := \deg(Q)$. On a alors $P(X) = \sum_{k=0}^{n} a_k X^k$ et $Q(X) = \sum_{k=0}^{m} b_k X^k$ avec $a_n, b_m \neq 0$. Il est clair, par définition de la somme, du produit et de la dérivation, que $\deg(P.Q) \leq \deg(P) + \deg(Q)$, $\deg(P + Q) \leq \max\big(\deg(P), \deg(Q)\big)$ et $\deg(P') \leq \deg(P) - 1$.

Or le coefficient de degré $n+m$ de $P(X).Q(X)$ vaut $\sum_{k=0}^{n+m} a_k b_{n+m-k}$. Pour $k \in [\![0, n-1]\!]$, on a $n+m-k > m$ et donc $b_{n+m-k} = 0$. Pour $k \in [\![n+1, n+m]\!]$, on a $a_k = 0$. Tous les termes de $\sum_{k=0}^{n+m} a_k b_{n+m-k}$ s'annulent donc sauf celui correspondant à $k = n$. Le coefficient de degré $n + m$ de $P(X).Q(X)$ vaut donc $a_n b_m \neq 0$ et $P(X).Q(X)$ est donc non nul, de degré $n + m$.

Si $n \geq 1$, alors le coefficient de degré $n - 1$ de $P'(X)$ vaut $n a_n \neq 0$. On a donc $\deg(P') = \deg(P) - 1$. □

Corollaire 15. *Soit $P(X), Q(X) \in \mathbb{K}[X]$. Si $P(X).Q(X) = 0$ alors soit $P(X) = 0$, soit $Q(X) = 0$.*

Définition 16. Pour tout $n \in \mathbb{N}$ on définit $\mathbb{K}_n[X] := \big\{P(X) \in \mathbb{K}[X] | \deg(P) \leq n\big\}$.

Proposition 17. *Pour tout $n \in \mathbb{N}$ l'ensemble $\mathbb{K}_n[X]$ est stable par addition et par dérivation. Il n'est par contre pas stable par multiplication dès que $n \geq 1$.*

Définition 18. On définit la valuation de tout polynôme $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ non nul, noté $\mathrm{val}(P)$, par $\min\{k \in [\![0, n]\!] | a_k \neq 0\}$. Par convention, la valuation du polynôme nul vaut $+\infty$.

3 Arithmétique des polynômes

Proposition 19 (division euclidienne)**.** *Soit $P(X), Q(X) \in \mathbb{K}[X]$ avec $Q(X)$ non nul. Il existe d'uniques polynômes $S(X), R(X) \in \mathbb{K}[X]$ tels que*

i. $P(X) = S(X).Q(X) + R(X)$;

ii. $\deg(R) < \deg(Q)$.

Démonstration. Montrons d'abord que de tels polynômes $S(X)$ et $R(X)$ existent.
Si $\deg(Q) = 0$, alors $Q(X) = a_0 \in \mathbb{K}^*$. On peut alors prendre $S(X) = \frac{1}{a_0} P(X)$ et $R(X) = 0$. On a de fait $\deg(R) = -\infty < 0 = \deg(Q)$.
Si $\deg(Q) > 0$, on raisonne par récurrence sur le degré de $P(X)$.

i. Si $\deg(P) < \deg(Q)$, on prend $S(X) = 0$ et $R(X) = P(X)$.

ii. Supposons le résultat vrai jusqu'au rang $n \geq \deg(Q) - 1$. Soit $P(X) \in \mathbb{K}[X]$ de degré $n + 1 \geq \deg(Q)$. On note a le coefficient dominant de $P(X)$ et b celui de $Q(X)$. Un calcul direct montre que $\frac{a}{b}X^{n+1-\deg(Q)}Q(X)$ est de degré $n + 1$ et que son coefficient dominant vaut a. Le polynôme $P(X) - \frac{a}{b}X^{n+1-\deg(Q)}Q(X)$ est donc de degré strictement plus petit que $n+1$ car les deux coefficients dominants s'annulent. Par hypothèse de récurrence, il existe deux polynômes $S(X)$ et $R(X)$ avec $\deg(R) < \deg(Q)$ et $P(X) - \frac{a}{b}X^{n+1-\deg(Q)}Q(X) = S(X).Q(X) + R(X)$. Mais alors $P(X) = \big(\frac{a}{b}X^{n+1-\deg(Q)} + S(X)\big).Q(X) + R(X)$.

iii. Par principe de raisonnement par récurrence, le résultat est donc vrai, quelque soit le degré de P.

Montrons maintenant que $S(X)$ et $R(X)$ sont uniques. Pour cela, on suppose qu'il existe deux autres polynômes $\widetilde{S}(X), \widetilde{R}(X) \in \mathbb{K}[X]$ vérifiant les mêmes propriétés. On a alors $\widetilde{S}(X).Q(X) + \widetilde{R}(X) = P(X) = S(X).Q(X)+R(X)$ et donc $\big(S(X)-\widetilde{S}(X)\big).Q(X) = \widetilde{R}(X)-R(X)$. Le polynôme $\big(S(X)-\widetilde{S}(X)\big).Q(X)$ est soit nul, soit de degré au moins égal à $\deg(Q)$. Or $\deg\big(\widetilde{R}(X)-R(X)\big) < \deg(Q)$. Donc $\big(S(X)-\widetilde{S}(X)\big).Q(X) = 0$, et puisque $Q(X) \neq 0$, on a $S(X) - \widetilde{S}(X) = 0$ en vertu de la proposition 15. On en déduit que $\widetilde{S}(X) = S(X)$ et donc que $\widetilde{R}(X) = P(X) - S(X).Q(X) = R(X)$. □

L'existence d'une division euclidienne permet de définir toute une arithmétique des polynômes. On a donc toutes les définitions et propositions suivantes, dont les preuves sont entièrement similaires aux preuves correspondantes en arithmétique sur $\mathbb{Z}$.

Définition 20. Un polynôme non nul $Q(X) \in \mathbb{K}[X]$ divise un autre polynôme $P(X) \in \mathbb{K}[X]$ si le reste de la division euclidienne de $P(X)$ par $Q(X)$ est nul. On dit aussi que $Q(X)$ est un diviseur de $P(X)$ ou encore que $P(X)$ est un multiple de $Q(X)$.

Remarque 21. Un polynôme $Q(X)$ divise un autre polynôme $P(X)$ s'il existe un troisième polynôme $S(X)$ tel que $P(X) = S(X).Q(X)$. Notamment, on a nécessairement $\deg(Q) \geq \deg(P)$.
Il est clair dans la preuve de la proposition 19 que tout polynôme de degré 0 (c'est-à-dire constant non nul) divise tous les autres polynômes.

Définition 22. Deux polynômes sont dits premiers entre eux si leurs seuls diviseurs communs sont les polynômes de degré 0.

Théorème 23 (de Bézout)**.** *Deux polynômes $P(X), Q(X) \in \mathbb{K}[X]$ sont premiers entre eux si et ssi il existe $U(X), V(X) \in \mathbb{K}[X]$ tels que $U(X).P(X) + V(X).Q(X) = 1$.*

Lemme 24 (de Gauss)**.** *Si $P(X), Q(X) \in \mathbb{K}[X]$ sont deux polynômes premiers entre eux et que $P(X)$ divise $Q(X).R(X)$ avec $R(X) \in \mathbb{K}[X]$, alors $P(X)$ divise $R(X)$.*

Corollaire 25. *Si $P(X), Q(X) \in \mathbb{K}[X]$ sont deux polynômes premiers entre eux et que chacun divise un troisième polynôme $R(X) \in \mathbb{K}[X]$, alors $P(X).Q(X)$ divise $R(X)$.*

Démonstration. Le polynôme $P(X)$ divise $R(X)$, il existe donc $\widetilde{R}(X)$ tel que $R(X) = P(X).\widetilde{R}(X)$. Or $Q(X)$ divise $R(X) = P(X).\widetilde{R}(X)$ et $Q(X)$ est premier avec $P(X)$, donc $Q(X)$ divise $\widetilde{R}(X)$. Il existe donc $\widehat{R}(X) \in \mathbb{K}[X]$ tel que $\widetilde{R}(X) = Q(X).\widehat{R}(X)$. Mais alors $R(X) = P(X).Q(X).\widehat{R}(X)$ et $P(X).Q(X)$ divise $R(X)$. □

4 Racines d'un polynôme

Définition 26. On dit que $\alpha \in \mathbb{K}$ est une racine de $P(X) \in \mathbb{K}[X]$ si $X - \alpha$ divise $P(X)$.
On dit qu'elle est d'ordre $k \in \mathbb{N}^*$ si $(X - \alpha)^k$ divise $P(X)$ mais que $(X - \alpha)^{k+1}$ ne divise pas $P(X)$.
Une racine d'ordre 1 est appelée racine simple. Les autres, de degré au moins 2, sont appelées racines multiples.

Remarque 27. D'après la remarque 21, un polynôme divisant $P(X)$ est de degré au plus égal à celui de $P(X)$. Le degré de toute racine de $P(X)$ est donc bien défini car il est majoré par le degré de $P(X)$.

Proposition 28. *Avec les notations de la définition 4, on a pour tout $\alpha \in \mathbb{K}$ et tout $P(X) \in \mathbb{K}[X]$*

$$\alpha \text{ racine de } P(X) \iff f_P(\alpha) = 0.$$

Démonstration. On fait la division euclidienne $P(X) = S(X).(X - \alpha) + R(X)$ de $P(X)$ par $X - \alpha$. Or $\deg(X - \alpha) = 1$, donc $R(X)$ est soit nul, soit de degré 0. Dans tous les cas, il existe $r \in \mathbb{K}$ tel que $R(X) = r$. Or $f_P(\alpha) = f_S(\alpha).f_{X-\alpha}(\alpha) + f_r(\alpha) = f_S(\alpha).(\alpha - \alpha) + r = r$. Donc α est racine de $P(X)$ si et ssi le reste $r = f_P(\alpha)$ est nul. □

Proposition 29. *Si un élément $\alpha \in \mathbb{K}$ est racine de multiple de $P(X) \in \mathbb{K}[X]$ alors α est également racine (éventuellement simple) de $P'(X)$.*

Remarque 30. Il est faux, en général, qu'une racine d'un polynôme soit également racine de sa dérivé. Par exemple, 1 est racine de $X - 1$, mais pas de sa dérivé.

Démonstration. Si α est racine multiple de $P(X)$, c'est qu'au moins $(X - \alpha)^2$ divise $P(X)$. Il existe donc $S(X)$ tel que $P(X) = (X - \alpha)^2.S(X)$. Mais alors $P'(X) = 2(X - \alpha).S(X) + (X - \alpha)^2.S'(X) = (X - \alpha).\big(2S(X) + (X - \alpha).S'(X)\big)$ et donc $X - \alpha$ divise $P'(X)$. □

Corollaire 31. *Si un élément $\alpha \in \mathbb{K}$ est racine multiple de $P(X) \in \mathbb{K}[X]$ alors, avec les notation de la définition 4, $f_P(\alpha) = f'_P(\alpha) = 0$.*

Théorème 32 (de D'Alembert–Gauss)**.** *Tout polynôme dans $\mathbb{C}[X]$ de degré au moins 1 admet une racine dans $\mathbb{C}$.*

Démonstration. Admis. □

5 Polynômes irréductibles

Définition 33. On dit que $P(X) \in \mathbb{K}[X]$ est irréductible si, pour toute décomposition $P(X) = S(X).R(X)$ avec $S(X), R(X) \in \mathbb{K}[X]$, on a $\deg(S) = 0$ ou $\deg(R) = 0$.

Proposition 34. *Tout polynôme $P(X) \in \mathbb{K}[X]$ de degré au moins 1 admet, à permutations des facteurs près, une unique décomposition de la forme*

$$P(X) = \alpha \prod_{k=1}^{n} P_k(X)$$

avec $\alpha \in \mathbb{K}$, $n \in \mathbb{N}^*$ et, pour tout $k \in [\![1, n]\!]$, $P_k(X) \in \mathbb{K}[X]$ unitaire et irréductible.

Démonstration. Montrons l'existence d'une telle décomposition par récurrence sur le degré de $P(X)$.

i. Si $\deg(P) = 1$ et que l'on a $P(X) = R(X).S(X)$, alors $\deg(R) + \deg(S) = \deg(P) = 1$. On a donc nécessairement $\deg(R) = 0$ et $\deg(S) = 1$, ou $\deg(R) = 1$ et $\deg(S) = 0$. Dans les deux cas, l'un des facteurs est de degré 0. Donc $P(X)$ est irréductible et en factorisant par son coefficient dominant α, on peut écrire $P(X) = \alpha\Big(\frac{1}{\alpha}P(X)\Big)$ avec $\frac{1}{\alpha}P(X)$ unitaire et irréductible.

ii. Supposons le résultat vrai jusqu'au rang n. Soit $P(X)$ un polynôme de degré $n + 1$. Si $P(X)$ est irréductible alors en factorisant par son coefficient dominant α, on peut écrire $P(X) = \alpha\Big(\frac{1}{\alpha}P(X)\Big)$ avec $\frac{1}{\alpha}P(X)$ unitaire et irréductible. Sinon, il existe $P(X) = R(X).S(X)$ avec $R(X)$ et $S(X)$ deux polynômes de degré au moins 1. Mais alors $\deg(R)+\deg(S) = \deg(P) = n+1$ et on a $\deg(R), \deg(S) \leq n$.

Par hypothèse de récurrence, il existe donc $\alpha, \beta \in \mathbb{K}$, $n, m \in \mathbb{N}^*$ et $R_1(X), \cdots, R_n(X), S_1(X), \cdots, S_m(X) \in \mathbb{K}[X]$ unitaires irréductibles tels que $R(X) = \alpha R_1(X).R_2(X).\cdots.R_n(X)$ et $S(X) = \beta S_1(X).S_2(X).\cdots.S_m(X)$. On a alors

$$P(X) = \alpha\beta R_1(X).R_2(X).\cdots.R_n(X).S_1(X).S_2(X).\cdots.S_m(X).$$

La propriété est donc vraie pour tout polynôme $P(X)$, quelque soit son degré.

L'unicité, à permutation des facteurs près, découle essentiellement du lemme de Gauss. Les détails sont laissés comme exercice au lecteur. □

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

Démonstration. Soit $P(X)$ un polynôme de degré $n \geq 2$. D'après le théorème de d'Alembert–Gauss, $P(X)$ admet au moins une racine dans $\mathbb{C}$. Il est donc divisible par un polynôme de degré 1. Mais alors le quotient est de degré $n-1 \geq 1$ et on a une factorization de $P(X)$ en deux polynômes de degré au moins 1. Le polynôme $p(X)$ n'est donc pas irréductible.

A contrario, nous avons prouvé, dans le cas initial de la récurrence prouvant la proposition 34, que tout polynôme de degré 1 est irréductible. □

Corollaire 36. *Tout polynôme de degré $d \in \mathbb{N}^*$ dans $\mathbb{C}[X]$ admet exactement d racines, éventuellement confondues.*

Démonstration. D'après la proposition 34, tout polynôme $P(X) \in \mathbb{C}[X]$ admet une décomposition en facteurs irréductibles. Or d'après la proposition 35, ceux-ci sont tous de degré 1. Le degré de $P(X)$ impose alors le nombre de ces facteurs. Or chaque facteur de degré 1 correspond à une racine, éventuellement multiple si le facteur apparait plusieurs fois, de $P(X)$. □

Proposition 37. *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et ceux de degré 2 dont le discriminant est strictement négatif, c'est à dire de la forme $aX^2 + bX + c$ avec $a, b, c \in \mathbb{R}$ tels que $b^2 - 4ac < 0$.*

Proposition 38. *Deux polynômes irréductibles unitaires sont soit égaux, soit premiers entre eux.*

Démonstration. Soit $P(X), Q(X) \in \mathbb{K}[X]$ irréductibles et unitaires. Supposons qu'ils ne soient pas irréductibles. Ils ont donc un diviseur commun $D(X) \in \mathbb{K}[X]$ de degré au moins 1 et il existe $\widetilde{P}(X), \widetilde{Q}(X) \in \mathbb{K}[X]$ tels que $P(X) = \widetilde{P}(X).D(X)$ et $Q(X) = \widetilde{Q}(X).D(X)$. Par irréducibilité de $P(X)$ et $Q(X)$, on a $\deg(\widetilde{P}) = \deg(\widetilde{Q}) = 0$. On a donc $\alpha, \beta \in \mathbb{K}$ tels que $P(X) = \alpha D(X)$ et $Q(X) = \beta D(X)$. Or, étant unitaires, $P(X)$ et $Q(X)$ ont le même coefficient dominant. On a donc $\alpha = \beta$ et donc $P(X) = Q(X)$. □

6 Fractions rationnelles

Définition 39. On appelle fraction de polynôme en l'indéterminé X toute expression de la forme $\frac{P(X)}{Q(X)}$ avec $P(X), Q(X) \in \mathbb{K}[X]$ et $Q(X) \neq 0$.
Pour tous $P(X), Q(X), R(X) \in \mathbb{K}[X]$, avec $Q(X), R(X) \neq 0$, on dit que $\frac{P(X)}{Q(X)}$ et $\frac{R(X).P(X)}{R(X).Q(X)}$ représente la même fraction rationnelle.
On note $\mathbb{K}(X)$ l'ensemble des fractions rationnelles en l'indéterminé X.

Définition 40. A l'instar des polynômes, on peut associer, à toute fraction rationnelle $\frac{P(X)}{Q(X)} \in \mathbb{K}(X)$ une application rationnelle

$$f_{\frac{P}{Q}} : \begin{array}{ccc} \mathbb{K} \setminus \{\text{racines de } Q(X)\} & \longrightarrow & \mathbb{K} \\ x & \longmapsto & \frac{f_P(x)}{f_Q(x)} \end{array}$$

avec f_P et f_Q les applications polynômiales associées à $P(X)$ et $Q(X)$.

Toujours par analogie avec les applications rationnelles associées, on définit sur $\mathbb{K}(X)$ les opérations suivantes.

Définition 41. Soit $\frac{P_1(X)}{Q_1(X)}, \frac{P_2(X)}{Q_2(X)} \in \mathbb{K}(X)$.

i. On définit $\frac{P_1(X)}{Q_1(X)} + \frac{P_2(X)}{Q_2(X)}$ par $\frac{P_1(X).Q_2(X)+P_2(X).Q_1(X)}{Q_1(X).Q_2(X)}$.

ii. On définit $\frac{P_1(X)}{Q_1(X)}.\frac{P_2(X)}{Q_2(X)}$ par $\frac{P_1(X).P_2(X)}{Q_1(X).Q_2(X)}$.

iii. On définit $\left(\frac{P_1(X)}{Q_1(X)}\right)'$ par $\frac{P_1'(X).Q_1(X)-P_1(X).Q_1'(X)}{Q_1^2(X)}$.

Proposition 42. *Les trois opérations définies ci-dessus sont bien définies. Cela signifie que le résultat d'une opération ne dépend pas du choix des fractions de polynômes choisies pour représenter chacune des fractions rationnelles.*

Proposition 43. *L'addition et la multiplication dans $\mathbb{K}(X)$ sont associatives et commutatives ; l'addition est distributive sur la multiplication ; la dérivation est linéaire et satisfait l'identité de Leibniz.*

Remarque 44. Toutes les techniques de calcul usuelles sont donc licites dans $\mathbb{K}(X)$, et toutes les opérations passent aux applications rationnelles associées.

Remarque 45. Les fractions rationnelles de la forme $\frac{P(X)}{1}$ peuvent être assimilées aux polynômes $P(X)$. On omet alors, en général, d'écrire la barre "$\frac{}{1}$".

Proposition 46. *Soit $\frac{P(X)}{Q(X)} \in \mathbb{K}(X)$, il existe d'uniques $E(X), R(X) \in \mathbb{K}[X]$ tels que $\frac{P(X)}{Q(X)} = E(X) + \frac{R(X)}{Q(X)}$.*

Démonstration. On fait la division euclidienne $P(X) = E(X).Q(X) + R(X)$ de $P(X)$ par $Q(X)$. On a alors $\frac{P(X)}{Q(X)} = \frac{E(X).Q(X)+R(X)}{Q(X)} = \frac{E(X).Q(X)+R(X).1}{Q(X).1} = \frac{E(X)}{1} + \frac{R(X)}{Q(X)} = E(X) + \frac{R(X)}{Q(X)}$.

Réciproquement, si $\frac{P(X)}{Q(X)} = E(X) + \frac{R(X)}{Q(X)}$, alors en multipliant par $Q(X)$, on trouve $E(X).Q(X) + R(X) = P(X)$. L'unicité de la division euclidienne assure donc l'unicité des polynômes $E(X), R(X) \in \mathbb{K}[X]$. ☐

Définition 47. Avec les notations de la proposition précédente, on appelle $E(X)$ partie entière de $\frac{P(X)}{Q(X)}$.

Proposition 48. *Soit $P(X), Q(X) \in \mathbb{K}[X]$ avec $Q(X)$ irréductible et $\deg(P) < \deg(Q^n)$. Alors il existe $P_1(X), \cdots, P_n(X) \in \mathbb{K}[X]$ avec $\deg(P_1), \cdots, \deg(P_n) < \deg(Q)$ tels que*

$$\frac{P(X)}{Q^n(X)} = \sum_{k=1}^{n} \frac{P_k(X)}{Q^k(X)}.$$

Démonstration. On raisonne par récurrence sur n.

i. Pour $n = 1$, le résultat est trivial.

ii. On suppose le résultat vrai au rang n. On considère la fraction rationnelle $\frac{P(X)}{Q^{n+1}(X)}$ avec $\deg(P) < \deg(Q^{n+1}) = (n+1)\deg(Q)$. On fait la division euclidienne $P(X) = Q^n(X).S(X) + R(X)$ de $P(X)$ par $Q^n(X)$. Une étude des degrés donne $S(X) = 0$ ou $\deg(S) = \deg(P) - n\deg(Q) < (n+1)\deg(Q) - n\deg(Q) = \deg(Q)$. Dans les deux cas, on a bien $\deg(S) < \deg(Q)$ De plus, $\deg(R) < n\deg(Q)$, donc par hypothèse de récurrence, il existe $R_1(X), \cdots, R_n(X) \in \mathbb{K}[X]$ tous de degré strictement inférieur à $\deg(Q)$, tels que

$$\frac{R(X)}{R^n(X)} = \sum_{k=1}^{n} \frac{R_k(X)}{Q^k(X)}.$$

Mais alors

$$\begin{aligned}\frac{P(X)}{Q^{n+1}(X)} &= \frac{Q^n(X).S(X)+R(X)}{Q^{n+1}(X)}\\ &= \frac{S(X)}{Q(X)}+\frac{1}{Q(X)}\frac{R(X)}{Q^n(X)}\\ &= \frac{S(X)}{Q(X)}+\frac{1}{Q(X)}\left(\sum_{k=1}^{n}\frac{R_k(X)}{Q^k(X)}\right)\\ &= \frac{S(X)}{Q(X)}+\sum_{k=2}^{n+1}\frac{R_{k-1}(X)}{Q^k(X)}.\end{aligned}$$

□

Proposition 49. *Soit* $P(X), Q_1(X), Q_2(X) \in \mathbb{K}[X]$ *avec* $Q_1[X], Q_2[X]$ *deux polynômes irréductibles unitaires distincts et* $\deg(P) < \deg(Q_1)+\deg(Q_2)$. *Il existe alors* $R_1(X), R_2(X) \in \mathbb{K}[X]$ *avec* $\deg(R_1) < \deg(Q_1)$ *et* $\deg(R_2) < \deg(Q_2)$ *tels que*

$$\frac{P(X)}{Q_1(X).Q_2(X)} = \frac{R_1(X)}{Q_1(X)}+\frac{R_2(X)}{Q_2(X)}.$$

Démonstration. D'après la proposition 38, $Q_1(X)$ et $Q_2(X)$ sont premiers entre eux. Donc, d'après le théorème de Bézout, il existe $S_1(X), S_2(X) \in \mathbb{K}[X]$ tels que $S_1(X).Q_1(X) + S_2(X).Q_2(X) = 1$. Mais alors

$$\begin{aligned}\frac{P(X)}{Q_1(X).Q_2(X)} &= \frac{P(X).\big(S_1(X).Q_1(X)+S_2(X).Q_2(X)\big)}{Q_1(X).Q_2(X)}\\ &= \frac{P(X).S_1(X).Q_1(X)}{Q_1(X).Q_2(X)}+\frac{P(X).S_2(X).Q_2(X)}{Q_1(X).Q_2(X)}\\ &= \frac{P(X).S_1(X)}{Q_2(X)}+\frac{P(X).S_2(X)}{Q_2(X)}.\end{aligned}$$

On écrit alors $\frac{P(X).S_2(X)}{Q_1(X)} = E_1(X)+\frac{R_1(X)}{Q_1(X)}$ et $\frac{P(X).S_2(X)}{Q_1(X)} = E_1(X)+\frac{R_1(X)}{Q_1(X)}$ avec $E_1(X), E_2(X), R_1(X), R_2(X) \in \mathbb{K}[X]$, $\deg(R_1) < \deg(Q_1)$ et $\deg(R_2) < \deg(Q_2)$. On a alors

$$\frac{P(X)}{Q_1(X).Q_2(X)} = E_1(X)+E_2(X)+\frac{R_1(X)}{Q_1(X)}+\frac{R_2(X)}{Q_2(X)}.$$

Mais par unicité de la partie entière de $\frac{P(X)}{Q_1(X).Q_2(X)}$, on a $E_1(X)+E_2(X) = 0$, ce qui permet de conclure. □

Théorème 50. *Soit* $\frac{P(X)}{Q(X)} \in \mathbb{K}(X)$. *On note* $Q(X) = \alpha\prod_{k=1}^{n} Q_k^{\alpha_k}(X)$, *avec* $Q_i(X) \neq Q_j(X)$ *si* $i \neq j$, *la décomposition de* $Q(X)$ *en facteurs irréductibles unitaires. Alors, il existe* $E(X) \in \mathbb{K}[X]$ *et, pour tout* $i \in [\![1, n]\!]$ *et tout* $j \in [\![1, \alpha_i]\!]$, $Q_{i,j}(X) \in \mathbb{K}[X]$ *avec* $\deg(Q_{i,j}) < \deg(Q_i)$ *tels que*

$$\frac{P(X)}{Q(X)} = E(X)+\sum_{k=1}^{n}\left(\sum_{i=1}^{\alpha_k}\frac{Q_{k,i}(X)}{Q_k^i(X)}\right).$$

C'est ce qu'on appelle décomposer une fraction rationnelle en éléments simples. Cela facilite l'étude des fractions rationnelles car cela permet de se rammener à des fractions plus simples n'ayant qu'une puissance d'un polynôme irréductible au dénominateur et avec un polynôme de puissance moindre au numérateur. Cela va permettre, notamment de calculer des primitives pour les applications rationnelles.

Démonstration. C'est un corollaire des propositions 46, 48 et 49. □

Corollaire 51. *Soit $\frac{P(X)}{Q(X)} \in \mathbb{C}(X)$ avec $a_1, \cdots, a_n \in \mathbb{C}$ les racines de $Q(X)$ d'ordre respectifs $\alpha_1, \cdots, \alpha_n \in \mathbb{N}^*$. Alors il existe $E(X) \in \mathbb{C}[X]$ et, pour tout $i \in [\![1, n]\!]$ et tout $j \in [\![1, \alpha_i]\!]$, $b_{i,j} \in \mathbb{C}$ tels que*

$$\frac{P(X)}{Q(X)} = E(X) + \sum_{k=1}^{n} \left(\sum_{i=1}^{\alpha_k} \frac{b_{k,i}}{(X - a_k)^i} \right).$$

Démonstration. C'est un corollaire du théorème 50 et de la proposition 35. □

En pratique, il existe plusieurs méthodes pour décomposer une fraction rationnelle en éléments simples. Bien entendu, on peut travailler par identification, mais cela nécessite beaucoup de calculs et la moindre erreur sur un des coefficients se répercute sur tous les autres coefficients. Le résultat suivant va permettre de trouver plus raisonablement les coefficients.

Proposition 52. *Avec les notations du théorème 50, si $Q_1 = X - a$ alors les $Q_{1,i}$, pour $i \in [\![1,]\!]$, sont des polynômes constants et on a*

$$Q_{1,\alpha_1} = \frac{P(a)}{\widetilde{Q}(a)}$$

avec $\widetilde{Q}(X) = \frac{Q(X)}{Q_1^{\alpha_1}(X)} \in \mathbb{K}[X]$.

Démonstration. D'après le théorème 50, les polynômes $Q_{1,i}$, pour $i \in [\![1, \alpha_1]\!]$, sont de degré plus petit que $\deg(X - a) = 1$. Ce sont donc des constantes $b_{1,i} \in \mathbb{K}$. De plus, on a

$$\frac{P(X)}{Q(X)} = E(X) + \sum_{i=1}^{\alpha_k} \frac{b_{1,i}}{(X - a)^i} + \sum_{k=2}^{n} \left(\sum_{i=1}^{\alpha_k} \frac{Q_{k,i}(X)}{Q_k^i(X)} \right)$$

avec $(X - a)$ premier avec $Q_k(X)$, pour tout $k \in [\![2, n]\!]$, c'est-à-dire $Q_k(a) \neq 0$. Or on a

$$\begin{aligned}
\frac{P(X)}{\widetilde{Q}(X)} &= (X - a)^{\alpha_1} \frac{P(X)}{Q(X)} \\
&= (X - a)^{\alpha_1}.E(X) + \sum_{i=1}^{\alpha_1} b_{1,i}(X - a)^{\alpha_1 - i} + (X - a)^{\alpha_1}.\sum_{k=2}^{n} \left(\sum_{i=1}^{\alpha_k} \frac{Q_{k,i}(X)}{Q_k^i(X)} \right).
\end{aligned}$$

et donc

$$\begin{aligned}
\frac{P(a)}{\widetilde{Q}(a)} &= (a - a)^{\alpha_1}.E(a) + b_{1,\alpha_1} + \sum_{i=1}^{\alpha_1 - 1} b_{1,i}(a - a)^{\alpha_1 - i} + (a - a)^{\alpha_1}.\sum_{k=2}^{n} \left(\sum_{i=1}^{\alpha_k} \frac{Q_{k,i}(a)}{Q_k^i(a)} \right) \\
&= b_{1,\alpha_1}.
\end{aligned}$$

□

Ce résultat permet de calculer rapidement tous les coefficients lorsque $Q(X) = \prod_{k=1}^{n}(X - a_k)$ avec $a_i \neq a_j$ pour tous $i \neq j$.
Si $Q(X)$ admet une racine multiple a, alors ce résultat permet de calculer le coefficient de degré maximal. En soustrayant l'élément simple ainsi obtenu à la fraction de départ, on obtient une nouvelle fraction rationnelle pour qui a est racine du dénominateur avec un ordre moindre. On peut donc réitérer le processus jusqu'à obtention du dernier coefficient lié à cette racine a.

Dans le cas d'une racine multiple, une autre technique consiste à considérer les évaluations en a des dérivés successives de $\frac{P(X)}{\widetilde{Q}(X)}$.