Théorème de Rothstein-Trager

Référence : [SP99] p.153-155.

1 Travail préparatoire

Définition 1.1 (Fraction rationnelle propre) *Soit* $\frac{P}{Q}$ *une fraction rationnelle de* $\mathbb{Q}(X)$ *telle que* $pgcd(P,Q) = 1$, Q *n'est pas réduit à* 1, *est unitaire et que* $\deg(P) < \deg(Q)$. *Une telle fraction rationnelle est dite propre.*

Remarque : On peut toujours se ramener à cette situation, quitte à effectuer une division de P par Q et un calcul de *pgcd*.

But : On souhaite déterminer une primitive de $\frac{P}{Q}$.

Remarque : Si $\alpha_1, \ldots, \alpha_d$ désignent les racines distinctes de Q dans $\mathbb{C}$, on sait qu'une primitive s'écrit alors sous la forme :

$$\int \frac{P}{Q} = \frac{G}{Q} + c_1 \log(X - \alpha_1) + \ldots + c_d \log(X - \alpha_d)$$

où $G \in \mathbb{Q}[X]$ et où les $c_i \in \mathbb{C}$.

Définition 1.2 (log d'un polynôme) *Soit* $R \in \mathbb{Q}[X]$, *on désigne par* $\log(R)$ *un élément d'une extension de* $\mathbb{Q}(X)$ *dont la dérivée vaut* $\frac{R'}{R}$.

Remarque : Avec cette définition du logarithme, on a toujours la propriété :

$$\log(UV) = \log(U) + \log(V)$$

Remarque : Cette définition doit être prise "formellement". La construction et le calcul de ces fonctions logarithme en un point particulier ne nous concernent pas ici mais seulement leurs propriétés de dérivation sus-mentionnées qui les caractérisent.

Pour en revenir à notre problème, il suffit a priori de décomposer le dénominateur en facteurs du premier degré dans $\mathbb{C}$ puis d'utiliser l'écriture en somme d'éléments simples. Cependant, on remarque que cette décomposition de Q en facteurs du premier degré n'est pas indispensable, par exemple :

$$\int \frac{X}{X^2-3} dX = \int \frac{dX}{2(X-\sqrt{3})} + \int \frac{dX}{2(X+\sqrt{3})} = \frac{1}{2}\log(X-\sqrt{3}) + \frac{1}{2}\log(X+\sqrt{3}) = \frac{1}{2}\log(X^2-3)$$

On voit donc que l'introduction de $\sqrt{3}$ lors des calculs s'est résorbée au moment d'écrire le résultat final de sorte que l'on peut se demander si cette situation est fréquente et si l'on pourrait, dans ce type de situation, se passer complètement de la factorisation du dénominateur en facteurs du premier degré. C'est l'objet des résultats qui suivent.

Proposition 1.1 (Décomposition sans facteur carré d'un polynôme) *Pour tout $Q \in \mathbb{Q}[X]$, il existe $Q_1, \ldots, Q_r \in \mathbb{Q}[X]$ premiers entre eux deux à deux et n'ayant que des racines simples tels que :*

$$Q = Q_1 Q_2^2 \ldots Q_r^r$$

C'est ce qu'on appelle la décomposition de Q sans facteur carré.

Grâce à cette décomposition, on peut écrire notre fraction rationnelle sous la forme :

$$\frac{P}{Q} = G_0 + \frac{G_{1,1}}{Q_1} + \frac{G_{2,1}}{Q_2} + \frac{G_{2,2}}{Q_2^2} + \frac{G_{3,1}}{Q_3} + \ldots + \frac{G_{r,r}}{Q_r^r}$$

où les polynômes $G_{i,j}$ sont à coefficients rationnels et tels que $\deg(G_{i,j}) < \deg(Q_i)$.
On est donc ramené à des calculs de primitive de la forme $\frac{u}{v^n}$ où v est sans facteur carré et premier avec u et $n \geq 0$.
Lorsque $n \geq 2$, on peut exprimer $\int \frac{u}{v^n}$ en fonction de $\int \frac{u}{v^{n-1}}$ par des méthodes élémentaires. En effet, comme v est sans facteur carré, il est premier avec sa dérivée et il existe deux polynômes c et d de $\mathbb{Q}[X]$ tels que $cu + dv' = 1$, polynômes qu'on obtient via l'algorithme d'Euclide étendu. On peut donc écrire pour $n \geq 2$:

$$\begin{aligned}
\int \frac{u}{v^n} &= \int \frac{ucv + udv'}{v^n} = \frac{cu}{v^{n-1}} + \int \frac{udv'}{v^n} \\
&= \int \frac{cu}{v^{n-1}} - \frac{ud}{(n-1)v^{n-1}} + \int \frac{(ud)'}{(n-1)v^{n-1}} \quad \text{via une intégration par parties ;} \\
&= -\frac{ud}{(n-1)v^{n-1}} + \frac{1}{n-1} \int \frac{(n-1)cu + (ud)'}{v^{n-1}} \quad \text{en rassemblant les termes.}
\end{aligned}$$

De proche en proche, on voit donc qu'on pourra écrire :

$$\int \frac{P}{Q} = \frac{U}{V} + \int \frac{P_1}{Q_1} + \int \frac{P_2}{Q_2} + \ldots + \int \frac{P_r}{Q_r}$$

avec $\frac{U}{V} \in \mathbb{Q}(X)$.
En regroupant les intégrales qu'ils nous restent à évaluer, on obtient :

$$\int \frac{P}{Q} = \frac{U}{V} + \int \frac{\tilde{P}}{Q_1 \ldots Q_r}$$

Le numérateur de la partie à intégrer peut être rendu de degré plus petit que le dénominateur en effectuant une division euclidienne et la fraction pourra être réduite, de sorte que nous sommes ramenés au problème suivant : calculer $\int \frac{P}{Q}$ avec $P, Q \in \mathbb{Q}[X]$, $pgcd(P, Q) = 1$, $\deg(P) < \deg(Q)$ et Q sans facteur carré unitaire.

2 Le théorème de Rothstein-Trager

Théorème 2.1 (Rothstein-Trager) *Soient $P, Q \in \mathbb{Q}[X]$ tels que $pgcd(P, Q) = 1$, $\deg(P) < \deg(Q)$ et Q sans facteur carré unitaire. Soit $\mathbb{K}$ une extension de $\mathbb{Q}$ (au sens où $\mathbb{Q} \subset \mathbb{K} \subset \mathbb{C}$) dans laquelle on peut écrire :*

$$\int \frac{P}{Q} = \sum_{i=1}^{n} c_i \log(P_i) \tag{1}$$

où les c_i sont des constantes non nulles de $\mathbb{K}$ qu'on suppose différentes (sinon on regroupe les log*) et où les P_i sont des polynômes unitaires non constants, sans facteur carré et premiers entre eux deux à deux dans $\mathbb{K}[X]$.*
Alors les c_i sont les racines distinctes du polynôme :

$$R(Y) = Res_X(P - YQ', Q) \in \mathbb{K}[Y]$$

et pour tout $1 \leq i \leq n$, $P_i = pgcd(P - c_i Q', Q)$.

Démonstration

Étape 1 Qui divise qui ?
On pose pour tout $1 \leq i \leq n$:

$$U_i = \frac{\prod_{j=1}^{n} P_j}{P_i}$$

Si on dérive la relation (1), on obtient :

$$\frac{P}{Q} = \sum_{i=1}^{n} c_i \frac{P_i'}{P_i}$$

D'où :

$$P \times \prod_{i=1}^{n} P_i = Q \times \sum_{i=1}^{n} c_i \frac{P_i'}{P_i} \times \prod_{i=1}^{n} P_i = Q \times \sum_{i=1}^{n} c_i P_i' U_i$$

On en déduit que Q divise $\prod_{i=1}^{n} P_i$ dans $\mathbb{K}[X]$ d'après le théorème de Bézout et que P_i divise $\sum_{i=1}^{n} c_i Q P_i' U_i$.
Mais, comme par définition, P_i divise déjà tous les U_j pour $j \neq i$, alors P_i divise $c_i Q P_i' U_i$.
Or on sait que P_i est sans facteur carré, par suite, $pgcd(P_i, P_i') = 1$; de plus P_i est aussi premier avec tous les P_j pour $j \neq i$, par suite P_i est premier avec U_i ; donc d'après le théorème de Bézout, pour tout $1 \leq i \leq n$, P_i divise Q.
Or les P_i sont premiers entre eux, donc on a :

$$\prod_{i=1}^{n} P_i | Q$$

On s'aperçoit donc que ces deux polynômes se divisent mutuellement l'un l'autre dans $\mathbb{K}[X]$ et sont donc associés (ie ne diffèrent que d'un facteur constant près).
Or ils sont tous les deux unitaires, donc ils sont égaux. On a alors :

$$Q = \prod_{i=1}^{n} P_i \quad \text{et} \quad P = \sum_{i=1}^{n} c_i P_i' U_i$$

Étape 2 Montrons que pour tout $1 \leq i \leq n$, P_i divise $P - c_i Q'$.
Comme :

$$Q = \prod_{i=1}^{n} P_i$$

On a :

$$Q' = \sum_{i=1}^{n} P_i' U_i$$

Et par suite :

$$P - c_i Q' = \sum_{j=1}^{n} c_j P_j' U_j - \sum_{j=1}^{n} c_i P_j' U_j = \sum_{j=1}^{n} (c_j - c_i) P_j' U_j$$

Et dans cette dernière égalité, le terme d'indice $j = i$ s'annule et pour tous les autres indices j, P_i divise U_j, de sorte que P_i divise bien $P - c_i Q'$.

Étape 3 Montrons que $P_i = pgcd(P - c_i Q', Q)$.
On a :

$$pgcd(P - c_i Q', Q) = pgcd(P - c_i Q', \prod_{j=1}^{n} P_j) = \prod_{j=1}^{n} pgcd(P - c_i Q', P_j)$$

car les P_j sont premiers entre eux deux à deux.
Or :

$$pgcd(P - c_i Q', P_j) = pgcd(\sum_{k=1}^{n} (c_k - c_i) P_k' U_k, P_j) = pgcd((c_j - c_i) P_j' U_j, P_j) = 1$$

car $pgcd(P_j, P_j') = 1$ (P_j étant sans facteur carré) et $pgcd(U_j, P_j) = 1$, c_i étant distinct de c_j par définition.
D'où :

$$pgcd(P - c_iQ', Q) = pgcd(P - c_iQ', P_i) = P_i$$

puisque nous avons vu que P_i divise $P - c_iQ'$.
Le coefficient c_i est donc tel que les polynômes $P - c_iQ'$ et Q ont un pgcd non trivial et on a ainsi $Res_X(P - c_iQ', Q) = 0$; ce qui montre bien que les coefficients c_i sont des racines distinctes du polynôme $R(Y) = Res_X(P - YQ', Q)$.

Étape 4 La réciproque.
Soit c une racine de R dans une extension $\widehat{\mathbb{K}}$ de $\mathbb{K}$ et supposons qu'elle n'apparaisse pas parmi les c_i de la relation (1).
Alors $pgcd(P - cQ', Q) = S \in \widehat{\mathbb{K}}[X]$ est un polynôme de degré non nul.
Si T désigne un facteur irréductible de S, T divise à la fois $P - cQ'$ et Q.
Comme $Q = \prod_{i=1}^{n} P_i$ et que les P_i sont premiers entre eux, alors T divise un seul des P_i, notons-le P_{i_0}.
Comme $P - cQ' = \sum_{j=1}^{n}(c_j - c)P_j'U_j$ et T divise P_{i_0}, et donc tous les U_j pour $j \neq i_0$ et qu'il divise aussi $P - cQ'$, alors :

$$T|(c_{i_0} - c)P_{i_0}'U_{i_0}$$

Le polynôme T ne divise pas U_{i_0} car il est facteur de P_{i_0}. Comme $c_{i_0} \neq c$, il en découle que T divise P_{i_0}' et ainsi P_{i_0} ne sera pas sans facteur carré, ce qui contredit l'hypothèse.

Remarque : Si on reprend l'exemple vu précédemment, on a :

$$R(Y) = Res_X(X - 2YX, X^2 - 3) = -3(1 - 2Y)^2$$

Donc $Y = \dfrac{1}{2}$ est la seule racine de R d'ordre 2, la primitive recherchée s'écrira alors sous la forme (1) avec une somme réduite à un élément. Le polynôme correspondant vaut :

$$P = pgcd(X - \frac{1}{2}2X, X^2 - 3) = X^2 - 3$$

et on retrouve le résultat. On remarque qu'ici la racine de R est dans $\mathbb{Q}$ et qu'on n'a pas besoin de considérer une extension de $\mathbb{Q}$.

Références

[SP99] Philippe Saux-Picart. *Cours de calcul formel, algorithmes fondamentaux.* Ellipses, 1999.