Théorème de Rothstein–Trager

Arnaud Girand

17 juin 2012

Référence :
- [SP99], p. 153–155

Proposition 1 (Rothstein–Trager)
Soient $P, Q \in \mathbb{Q}[X]$ premiers entre eux tels que $\deg(P) < \deg(Q)$.
On suppose de plus Q unitaire et sans facteur carré.
Soit $\mathbb{K}/\mathbb{Q}$ une extension dans laquelle on puisse écrire[1] *:*

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

Quitte à regrouper, on peut supposer les $c_i \in \mathbb{K}^*$ deux à deux distincts. La nature de Q nous permet également[2] *de supposer les P_i unitaires sans facteurs carrés, non constants*[3] *et premiers entre eux* deux à deux.
Alors :

(i) pour tout $i \in [n]$ on a :

$$P_i = (P - c_i Q') \wedge Q$$

(ii) les c_i sont exactement les racines du polynôme suivant :

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

Démonstration :

(i) Commençons par poser, pour $i \in [n]$:

$$U_i := \prod_{j \neq i} P_j$$

Ensuite, si on dérive (formellement) la relation (1) on obtient :

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

D'où :

$$P \prod_{j=1}^{n} P_j = Q \sum_{j=1}^{n} c_j P_j' U_j$$

On déduit de cette dernière relation que, dans $\mathbb{K}[X]$:

$$Q \mid \prod_{i=1}^{n} P_i \text{ et } \forall i \in [n], \quad P_i \mid \sum_{j=1}^{n} c_j P_j' U_j$$

Soit $i \in [n]$; alors pour tous les $j \neq i$, $P_i | U_j$ et donc on déduit de la seconde relation ci–avant que :

$$P_i \mid c_i Q P_i' U_i$$

1. On a existence d'une telle extension par théorème de décomposition en éléments simples.
2. Toujours par décomposition en éléments simples.
3. car $\deg(P) < \deg(Q)$.

Or P_i est sans facteur carré donc $P_i \wedge P_i' = 1$. En sus, $P_i \wedge P_j = 1$ si $j \neq 1$ donc $P_i \wedge U_i = 1$: le théorème de Gauss nous permet alors de conclure que $P_i | Q$, ergo (comme les P_i sont premiers entre eux *deux à deux*) :

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

Les polynômes $\prod_{i=1}^{n} P_i$ et Q sont donc unitaires associés, d'où in fine :

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

Soit $i \in [n]$; on se propose à présent de démontrer que $P_i | P - c_i Q'$. On déduit du résultat que l'on vient de démontrer sur Q que :

$$Q' = \sum_{j=1}^{n} P_j' U_j$$

Ergo :

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

Or la quantité $(c_i - c_j) P_j' U_j$ est nulle si $i = j$ et divisible par P_i sinon d'où le résultat attendu :

$$P_i \mid P - c_i Q'$$

Remarquons à présent que, si $i \in [n]$:

$$\begin{aligned} (P - c_i Q') \wedge Q &= (P - c_i Q') \wedge \prod_{j=1}^{n} P_j \\ &= \prod_{j=1}^{n} ((P - c_i Q') \wedge P_j) \text{ car les } P_j \text{ sont premiers entre eux deux à deux} \end{aligned}$$

Or, si $j \neq i$:

$$\begin{aligned} (P - c_i Q') \wedge P_j &= \left(\sum_{k=1}^{n} (c_k - c_i) P_k' U_k \right) \wedge P_j \\ &= (c_j - c_i) P_j' U_j \wedge P_j \text{ car } P_j \text{ divise les termes pour} \\ &= 1 \text{ car } P_j' \wedge P_j = U_j \wedge P_j = 1 \end{aligned}$$

D'où :

$$\begin{aligned} (P - c_i Q') \wedge Q = (P - c_i Q') \wedge P_i \\ = P_i \text{ car } P_i \mid P - c_i Q' \end{aligned}$$

(*ii*) On déduit du point (*i*) que pour tout $i \in [n]$ c_i est tel que $P - c_i Q'$ et Q ont un pgcd non trivial ; il est de fait racine du résultant R.
Réciproquement, si c est une racine de R dans une extension $\mathbb{L}/\mathbb{K}$, alors $S := (P - cQ') \wedge Q \in \mathbb{L}[X]$ est de degré strictement positif. Si on se donne T un facteur irréductible de S dans $\mathbb{L}[X]$ on a alors :

$$T \mid P - cQ' \text{ et } T \mid Q$$

Comme $Q = \prod_i P_i$ avec les P_i premiers entre eux deux à deux, T doit alors nécessairement diviser un et un seul des P_i, soit P_{i_0}. Mais :

$$P - cQ' = \sum_{i=1}^{n} (c_i - c) P_i' U_i$$

Comme T divise P_{i_0} donc tous les U_i pour $i \neq i_0$ et que $T|P - cQ'$ on a alors :

$$T \mid (c_{i_0} - c)P'_{i_0}U_{i_0}$$

Mais $T \nmid U_{i_0}$, ainsi si on suppose que c est distinct de tous les c_i on trouve $T|P'_{i_0}$ et donc P_{i_0} admet un facteur carré, ce qui est absurde et, accessoirement, conclut la preuve.

Références

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