

Algèbre tome I - groupes, corps et théorie de Galois

erratum

D. Guin & Th. Hausberger

17 novembre 2009

– p. 395 l. 13¹ :

– le polynôme $v = \sum_{i \in I} e_i \beta^i \prod_{j \in I \setminus \{i\}} (1 - \beta^j x)$ *évaluateur d'erreur*.

Les polynômes u et v vérifient $\deg u \leq t$ et $\deg v < t$. Ils déterminent à eux deux l'emplacement et la valeur des erreurs : il suffit d'évaluer en β^{-i} pour obtenir I ; on calcule e_i à l'aide de $u' = \sum_{i \in I} -\beta^i \prod_{j \in I \setminus \{i\}} (1 - \beta^j x)$, d'où

$$v(\beta^{-i}) = e_i \beta^i \prod_{j \in I \setminus \{i\}} (1 - \beta^{j-i}) = -e_i u'(\beta^{-i})$$

puis $e_i = -v(\beta^{-i})/u'(\beta^{-i})$.

Il existe différentes façons de calculer u et v . On peut, par exemple, formuler le problème en terme d'équations linéaires à résoudre. On va donner une autre méthode, plus performante en pratique.

On définit

$$w = \frac{v}{u} = \sum_{i \in I} \frac{e_i \beta^i}{1 - \beta^i x} = \sum_{i \in I} x^{-1} \sum_{j \geq 1} e_i (\beta^i x)^j = \sum_{j \geq 1} x^{j-1} \sum_{i \in I} e_i \beta^{ji} = \sum_{j \geq 1} e(\beta^j) x^{j-1}.$$

Comme $c(\beta^j) = 0$ pour $1 \leq j \leq \delta - 1$, on a $e(\beta^j) = m'(\beta^j)$ pour $1 \leq j \leq \delta - 1$. On connaît donc w modulo $x^{\delta-1}$: c'est $S(x) = \sum_{j=1}^{\delta-1} m'(\beta^j) x^{j-1}$, appelé parfois *polynôme syndrôme*.

– p. 396 l. 18 :

$$\begin{pmatrix} r_i & u_i \\ r_{i+1} & u_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} r_{i-1} & u_{i-1} \\ r_i & u_i \end{pmatrix}$$

¹On pourrait également corriger l'erreur en gardant la définition de v et S donnée, donc avec $\deg v < t + 1$, mais en remplaçant x^{2t} par x^{2t+1} à partir de l. 28, sachant que la congruence $v(x) \equiv u(x)S(x) \pmod{x^{2t+1}}$ est vérifiée