Calcul de fermeture intégrale en dimension 1

Mes travaux tournent autour du calcul de fermeture intégrale en dimension 1. Seul le problème local est abordé ; l'aspect globalisation qui se résume la plupart du temps à de l'algèbre linéaire, n'est pas traité. Voici la situation locale à laquelle on s'intéresse : soit A un anneau de valuation discrète, v la valuation associée, K son corps des fractions, k son corps résiduel, π une de ses uniformisante ($v(\pi) = 1$), L une K-extension finie de degré n — ou plus généralement une K-algèbre réduite de dimension finie —, B la fermeture intégrale de A dans L dont l'anneau résiduel, i.e. le quotient de B par son radical de Jacobson, est noté l. Nous faisons les deux hypothèses suivantes : la K-extension L est supposée séparable (ou étale si c'est une K-algèbre) et la k-algèbre l est supposée étale. Sous ces hypothèses grâce à des théorèmes classiques d'algèbre commutative, on montre que B est un A module libre de rang n. C'est de surcroît un anneau de Dedekind semi-local (donc principal). Notons $P_1, \ldots, P_r$ les différents idéaux maximaux de B. Ils couvrent tous π, i.e. $P_i \cap A = \pi A$, et π se factorise ainsi dans B :

$$\pi B = P_1^{e_1} \cdots P_r^{e_r}$$

Notons pour finir f_i le degré résiduel de P_i sur A, c'est-à-dire la dimension $\dim_k B/P_i$, alors la célèbre relation $n = \sum_i e_i f_i$ est satisfaite. Les preuves modernes établissant cette structure ne se sont pas constructives. Nous développons un procédé de calcul permettant de déterminer explicitement la structure arithmétique de l'anneau B que nous venons de rappeler.

Concrètement, on dispose d'un algorithme de factorisation dans $k[X]$ ainsi que d'un algorithme de calcul de coefficients de Bezout dans $k[X]$ (en aucun cas nous aurons besoin de factoriser dans $K[X]$) ; étant donné $F \in A[X]$ un polynôme unitaire et séparable, on souhaite déterminer explicitement la structure arithmétique de B la fermeture intégrale de A dans $L = K[X]/\langle F\rangle$, c'est-à-dire une A-base de B, les idéaux maximaux de B et la relation $n = \sum_i e_i f_i$ sous-jacente. Concernant le polynôme F, cela permet de tester son irréductibilité dans $\widehat{K}[X]$ (où $\widehat{K}$ désigne le complété de K pour la valuation v) et de calculer une approximation π-adique de ses facteurs irréductibles dans $\widehat{K}[X]$.

On dit que $x \in B$ est un élément monogène de B sur A s'il vérifie $B = A[x]$ (et B est alors dite monogène). La connaissance d'un élément de ce type résout entièrement notre problème. En effet, dans ce cas, la famille $\{1, x, \ldots, x^{n-1}\}$ forme une A-base de B. Si $G \in A[X]$ le polynôme caractéristique (ou minimal) de x sur K se factorise modulo π sous la forme $G \equiv G_1^{e_1} \cdots G_r^{e_r} \pmod{\pi}$ alors, d'après le théorème de Kummer, l'anneau B compte exactement r idéaux maximaux respectivement engendrés par $P_i = \langle \pi, G_i(x)\rangle$ et la relation $\sum_i e_i f_i$ sous-jacente n'est rien d'autre que $n = \sum_i e_i \deg(G_i)$. Concernant le polynôme F, il est irréductible dans $\widehat{K}[X]$ si et seulement si G est la puissance d'un irréductible modulo π. Enfin, F se factorise en r facteurs irréductibles dans $\widehat{K}[X]$ dont on peut déterminer une approximation en remontant via Hensel la factorisation de G modulo π.

L'idée est donc de rechercher de la monogénéité coûte que coûte. On commence par donner une condition nécessaire et suffisante pour que B admette un élément monogène sur A. On s'aperçoit que la seule obstruction à la A-monogénéité est de nature résiduelle. Plus précisément, pour que B admette un élément monogène sur A, il faut il suffit que l admette un élément primitif sur k. En complétant, on se ramène à un produit cartésien d'algèbres admettant un élément monogène. Cependant, ce point de vue n'est pas satisfaisant en pratique. C'est pourquoi nous avons été amenés à introduire la notion de pseudo-isomorphisme. Si L et L' sont deux K-algèbres réduites de même dimension (finie), on dit que $\varphi : L \to L'$ est un pseudo-isomorphisme si c'est une application K-linéaire appliquant B dans B' et telle que $\overline{\varphi} : l \to l'$ induise un isomorphisme de k-algèbres. Remarquant, que la K-algèbre $B/\pi B$ porte toutes les quantités que l'on cherche à déterminer, on se ramène via un pseudo-isomorphisme à un produit d'algèbres admettant un élément monogène.

Finalement, s'inspirant de l'algorithme Round4 élaboré par H. Zassenhaus, nous avons obtenu un algorithme réalisant l'objectif fixé. Étant donné $F \in A[X]$ unitaire et séparable, on construit des triplets $(F_i, \varepsilon_i, g_i)_{1 \le i \le s}$ où $F_i \in A[X]$, $\varepsilon_i \in K[X]/\langle F\rangle$, $g_i \in K[X_i]/\langle F_i\rangle$, les éléments ε_i et g_i étant entiers sur A, de telle sorte que :

– chaque polynôme F_i est unitaire et séparable ;

– l'anneau des entiers de chacune des K-algèbres $K[X_i]/\langle F_i\rangle$ est une A-algèbre monogène et g_i en est un élément monogène ;

– enfin, les éléments $\varepsilon_i \in K[X]/\langle F\rangle$ forment un système fondamental d'idempotents orthogonaux de $B/\pi B$ et permettent de définir le pseudo-isomorphisme φ :

$$\varphi : K[X_1]/\langle F_1\rangle \times \cdots \times K[X_s]/\langle F_s\rangle \longrightarrow K[X]/\langle F\rangle, \qquad \varphi(X_i^j \bmod F_i) = (X^j \bmod F)\varepsilon_i$$

où $1 \leq i \leq s$ et $0 \leq j < \deg(F_i)$. Du calcul des cette suite de triplets découle facilement la détermination de toutes les quantités recherchées.