

# Constructions cachées en algèbre abstraite (1) Relations de dépendance intégrale

Henri Lombardi <sup>1</sup>

Décembre 99

## Résumé

Nous donnons une méthode élémentaire, cachée dans un théorème d'algèbre abstraite, pour construire des relations de dépendance intégrale. Nous appliquons cette méthode pour donner une preuve constructive d'un théorème de Kronecker.

Classification AMS : 13B21, 03F65, 13F30

Mots clés : Anneau de valuation, Relation de dépendance intégrale, Mathématiques constructives.

## Introduction

Dans cet article, tous les anneaux considérés sont commutatifs, sauf mention expresse du contraire.

Rappelons le théorème suivant dû à Kronecker (cf. [5, 3]).

**Théorème** (théorème de Kronecker) *Soit  $A$  un anneau commutatif et dans  $A[X]$*

$$f(X) = \sum_i f_i X^i = g(X)h(X) = \left( \sum_j g_j X^j \right) \left( \sum_k h_k X^k \right)$$

*Alors chaque  $g_j h_k$  est entier sur l'anneau engendré par les  $f_i$ .*

Citons aussi les corollaires suivants.

### Corollaires

- a) *Soit  $A$  un anneau normal,  $K$  son anneau total des fractions, et  $f(X) \in A[X]$  unitaire. On suppose que  $f(X) = g(X)h(X)$  dans  $K[X]$ , avec  $g$  unitaire. Alors  $g(X) \in A[X]$*
- b) *Soit  $A$  un anneau de Prüfer,  $g(X), h(X) \in A[X]$  et  $f(X) = g(X)h(X)$ . Le produit des idéaux engendrés respectivement par les coefficients de  $g$  et ceux de  $h$  est l'idéal engendré par les coefficients de  $f$ .*

---

<sup>1</sup> Equipe de Mathématiques, UMR CNRS 6623, UFR des Sciences et Techniques, Université de Franche-Comté, 25030 BESANCON cedex, FRANCE, email : lombardi@math.univ-fcomte.fr

Le théorème de Kronecker, (ou certaines variantes), est à la base d'exposés constructifs de la théorie des diviseurs (cf. [5, 12]). Une preuve constructive de Hurwitz est donnée dans [5]. Il serait également intéressant de récupérer une preuve constructive d'après les variantes contenues dans [12].

Dans [3], ce théorème est démontré de manière explicite en utilisant une preuve abstraite non constructive et en lui faisant subir une transformation adéquate. En utilisant le corollaire 4.7 dans [4], on pourrait également faire une utilisation constructive de la preuve abstraite. Dans les deux cas, cette transformation d'une preuve abstraite en un calcul explicite est directement inspirée de la logique. Malgré son élégance, elle peut rebuter.

Nous présentons ici une méthode apparentée aux deux précédentes, mais qui n'utilise pas la logique. Purement algébrique, elle devrait provoquer moins de maux de têtes.

## 1 Le principe de la méthode

On considère un anneau  $A$ , sous-anneau d'un anneau  $B$  et un élément  $x$  de  $B$ . On veut construire une relation de dépendance intégrale qui signifie que  $x$  est entier sur  $A$ . L'argument classique abstrait usuel utilise un critère valuatif. On considère un homomorphisme arbitraire  $\varphi : B \rightarrow K$  où  $K$  est un corps valué,  $V$  étant l'anneau de valuation, avec  $\varphi(A) \subset V$ , et on montre que sous ces hypothèses  $\varphi(x) \in V$ . Le critère valuatif permet de conclure que  $x$  est entier sur  $A$ .

Dans le cas où  $B$  est intègre, le critère valuatif peut s'exprimer en disant que l'intersection des anneaux de valuation de  $\text{Frac}(B)$  qui contiennent  $A$  est égal à la clôture intégrale de  $A$  dans  $\text{Frac}(B)$ .

L'idée de notre méthode est à très peu près la suivante. Nous examinons avec un peu d'attention la preuve classique, en considérant que l'anneau de valuation  $V$  n'est qu'un objet idéal qui guide nos pas. Nous remplaçons les calculs dans  $V$  par les calculs dans des extensions convenablement construites de  $A$ . Nous voyons en effet dans la preuve classique certains calculs qui sont faisables dans  $V$  en vertu du principe :  $\forall \alpha, \beta \in K$  tels que  $\alpha\beta = 1$ ,  $\alpha$  est dans  $V$  ou  $\beta$  est dans l'idéal maximal de  $V$ . Principe qui est appliqué à des éléments  $\alpha, \beta$  provenant de la preuve elle-même.

Nous répétons la même preuve, en remplaçant chaque disjonction

“ $\alpha$  est dans  $V$  ou  $\beta$  est dans le radical (l'idéal maximal) de  $V$ ”,

par la considération des deux anneaux  $C_1 = C[\alpha]$  et  $C_2 = C[\beta]_{1+\beta C[\beta]}$ , où  $C$  est l'extension “courante” de l'anneau  $A$  de départ, à l'endroit de la preuve où on se trouve. Ainsi

“ $\alpha$  est dans  $C_1$  et  $\beta$  est dans le radical de  $C_2$ ”.

Lorsque la preuve initiale est ainsi déployée de manière arborescente, on a construit à la fin un certain nombre, fini parce que la preuve est finie, d'extensions  $A_i$ , sur chacune desquelles la relation de dépendance intégrale est construite. Et la manière dont les  $A_i$  sont construits implique que ces relations de dépendance intégrale peuvent se recoller en une relation de dépendance intégrale sur  $A$ .

En fait, pour que tout se passe bien lors de nos extensions successives de l'anneau  $A$ , nous avons besoin d'une catégorie légèrement différente de la catégorie des anneaux commutatifs, de manière qu'un élément qu'on a forcé à rentrer dans le radical d'une extension n'en sorte pas lors d'une nouvelle extension. La “bonne catégorie” (pour les calculs) sera celle dont les objets sont les couples  $(A, J)$  où  $A$  est un anneau commutatif et  $J$  un idéal contenu dans le radical de  $A$ , et les flèches de  $(A, J)$  vers  $(A', J')$  sont les homomorphismes  $f : A \rightarrow A'$  tels que  $f(J) \subset J'$ .

On retrouve les anneaux usuels en prenant  $J = 0$  et les anneaux locaux (avec la notion de morphisme local) en prenant  $J$  égal à l'idéal maximal.

Notons que cette méthode consiste pour l'essentiel à mettre à plat les calculs explicites qui sont impliqués par la mise en oeuvre de la méthode de l'évaluation dynamique donnée dans [4].

## 2 Recollement de relations de dépendance intégrale

L'usage de la "bonne catégorie" conduit à la définition suivante.

**Définition 1** Soit  $J$  un idéal d'un sous anneau  $A$  d'un anneau  $B$  et  $x \in B$ . On dit que  $x$  est entier sur  $(A, J)$  si on a une relation de dépendance intégrale

$$(1 + j)x^{n+1} = a_1x^n + a_2x^{n-1} + \cdots + a_nx + a_{n+1}$$

où  $j \in J$  et les  $a_i \in A$ .

Notez que  $x$  est entier sur  $A$  au sens usuel si et seulement si il est entier sur  $(A, \{0\})$  (ou encore sur  $(A, \text{Rad}(A))$ ) au sens de la définition ci-dessus.

Le contenu concret du critère valuatif, qui peut être débusqué dans toute preuve de ce critère (voir par exemple [11]), est donné par le théorème suivant, qui permet de mettre en oeuvre la méthode expliquée à la section 1.

La preuve utilise le résultant de deux polynômes en une variable, ce qui montre une fois de plus qu'il ne faut surtout pas éliminer l'élimination.

**Théorème 2** Soit  $J$  un idéal d'un sous anneau  $A$  d'un anneau  $B$  et  $x \in B$ . Soient  $\alpha, \beta \in B$  tels que  $\alpha\beta = 1$ , si  $x$  est entier sur  $(A[\alpha], JA[\alpha])$  et sur  $(A[\beta], \beta A[\beta] + JA[\beta])$  alors  $x$  est entier sur  $(A, J)$ .

**Preuve** On écrit les hypothèses, et on trouve la conclusion en éliminant  $\alpha$  et  $\beta$ . Voyons cela plus précisément. Le fait que  $x$  est entier sur  $(A[\alpha], JA[\alpha])$  correspond à une relation de dépendance intégrale

$$a(\alpha, x) = (1 + j_1(\alpha))x^n + a_{n-1}(\alpha)x^{n-1} + \cdots + a_1(\alpha)x + a_0(\alpha) = 0 \quad (1)$$

avec  $j_1$  à coefficients dans  $J$  et  $a_0, \dots, a_{n-1}$  à coefficients dans  $A$ , tous de degrés  $\leq s$ .

Le fait que  $x$  est entier sur  $(A[\beta], \beta A[\beta] + JA[\beta])$  correspond à une relation de dépendance intégrale

$$b(\beta, x) = (1 + j_2 + \beta b_m(\beta))x^m + b_{m-1}(\beta)x^{m-1} + \cdots + b_1(\beta)x + b_0(\beta) = 0 \quad (2)$$

avec  $j_2 \in J$  et  $b_0, \dots, b_{m-1}, \beta b_m$  polynômes en  $\beta$  de degrés  $\leq r$  à coefficients dans  $A$ .

On multiplie (1) par  $\beta^s$  de manière à chasser les  $\alpha$  et on obtient

$$c(\beta, x) = (\beta^s + j_3(\beta))x^n + c_1(\beta)x^{n-1} + \cdots + c_{n-1}(\beta)x + c_n(\beta) = 0 \quad (3)$$

avec  $j_3$  de degré  $\leq s$  à coefficients dans  $J$  et  $c_1, \dots, c_n$  de degrés  $\leq s$  à coefficients dans  $A$ .

On regarde maintenant le premier membre dans (2) et (3) comme un polynôme en  $\beta$  ayant pour coefficients des polynômes en  $x$ . Ainsi (2) se réécrit

$$d(x, \beta) = d_r(x)\beta^r + d_{r-1}(x)\beta^{r-1} + \cdots + d_1(x)\beta + d_0(x) = 0 \quad (4)$$

avec  $d_0, \dots, d_r$  de degrés  $\leq m$  à coefficients dans  $A$  et

$$d_0(x) = (1 + j_2)x^m + d_{0,m-1}x^{m-1} + \dots + d_{0,0}$$

De même (3) se réécrit

$$e(x, \beta) = e_s(x)\beta^s + e_{s-1}(x)\beta^{s-1} + \dots + e_1(x)\beta + e_0(x) = 0 \quad (5)$$

avec  $e_0, \dots, e_s$  de degrés  $\leq n$  à coefficients dans  $A$ ,

$$e_s(x) = (1 + j_{3,s})x^n + e_{s,n-1}x^{n-1} + \dots + e_{s,0}$$

et pour  $\ell < s$

$$e_\ell(x) = j_{3,\ell}x^n + e_{\ell,n-1}x^{n-1} + \dots + e_{\ell,0}$$

Dans l'anneau  $A$  les polynomes (en  $T$ )  $d(x, T)$  et  $e(x, T)$  admettent la racine commune  $\beta$ , donc le résultant (en  $T$ ) est nul (car il annule le vecteur  $(1, \beta, \dots, \beta^{r+s})$ ). Le résultant est le déterminant de la matrice de Sylvester de format  $(r + s + 1) \times (r + s + 1)$ , où les  $r$  premières colonnes sont remplies avec les coefficients de  $e(x, T)$  et les  $s$  dernières avec ceux de  $d(x, T)$ .

$$\begin{pmatrix} e_s(x) & 0 & \dots & \dots & 0 & d_r(x) & 0 & \dots & 0 \\ \vdots & e_s(x) & \ddots & & \vdots & \vdots & d_r(x) & & \vdots \\ & & \ddots & & & & & & \\ \vdots & & & & & & & \ddots & 0 \\ e_1(x) & & & & & & & & d_r(x) \\ e_0(x) & & & \ddots & & \vdots & & & \vdots \\ & \ddots & & & e_s(x) & d_1(x) & & & \\ \vdots & \ddots & & & \vdots & d_0(x) & & & \\ & & & & & 0 & \ddots & & \\ & & & & & \vdots & \ddots & & \\ \vdots & & \ddots & \ddots & \vdots & & & \ddots & \vdots \\ 0 & \dots & & 0 & e_0(x) & 0 & \dots & 0 & d_0(x) \end{pmatrix}$$

Lorsqu'on développe ce déterminant on obtient un polynome  $h(x)$  de degré  $rn + sm$  à coefficients dans  $A$ . Le coefficient  $h_{rn+sm}$  en degré  $rn + sm$  peut être analysé comme la somme de deux termes. Tout d'abord le coefficient dominant dans le produit  $e_s(x)^r d_0(x)^s$  des éléments diagonaux de la matrice. Ensuite une somme provenant des autres produits. Comme le seul produit non nul qui utilise tous les  $e_s(x)$  sur la diagonale est le produit de tous les éléments diagonaux, chacun des autres produits non nuls contient au moins un  $e_\ell(x)$  avec  $\ell < s$ , et cet  $e_\ell(x)$  a son coefficient de degré  $n$  dans  $J$ .

Ce coefficient  $h_{rn+sm}$  est donc égal à

$$h_{rn+sm} = (1 + j_{3,s})^r \cdot (1 + j_2)^s + j_4 = 1 + j$$

avec  $j_4, j \in J$ . Ceci termine la preuve, qui ne demande donc aucun effort d'imagination.  $\square$

### 3 Relecture constructive de la preuve abstraite du théorème de Kronecker

Hurwitz a donné une preuve constructive du théorème de Kronecker (cf. [5]). Nous sommes intéressés ici par le décryptage constructif de la preuve abstraite qui est usuelle aujourd'hui.

Cette preuve abstraite est la suivante. On considère le cas où les  $g_j$  et  $h_k$  dans le théorème de Kronecker sont des indéterminées, les degrés de  $g$  et  $h$  étant fixés ( $m$  et  $n$ ). On considère  $A = \mathbb{Z}[f_i]$ ,  $B = \text{Frac}(\mathbb{Z}[g_j, h_k])$ . On montre que chaque  $g_j h_k$  est entier sur  $A$  en montrant qu'il est dans tout anneau de valuation  $V$  de  $B$  qui contient  $A$ .

Pour cela on considère l'indice  $j_0$  défini comme suit :  $g_{j_0}$  divise tous les  $g_j$ , mais aucun  $g_\ell$  avec  $\ell > j_0$  ne divise  $g_{j_0}$ . Autrement dit

$$\forall j \leq m \quad g_j/g_{j_0} \in V, \quad \forall \ell > j_0 \quad g_\ell/g_{j_0} \in m_V$$

De même on considère l'indice  $k_0$  tel que

$$\forall k \leq n \quad h_k/h_{k_0} \in V, \quad \forall \ell > k_0 \quad h_\ell/h_{k_0} \in m_V$$

On obtient donc  $g_j h_k \in g_{j_0} h_{k_0} V$  pour tous  $j, k$ . On écrit alors en posant  $i_0 = j_0 + k_0$

$$f_{i_0} = g_{j_0} h_{k_0} + \sum_{j_0 < \ell \leq m} g_\ell h_{i_0 - \ell} + \sum_{k_0 < \ell \leq n} h_\ell g_{i_0 - \ell} = g_{j_0} h_{k_0} (1 + \mu)$$

où  $\mu \in m_V$ , ce qui implique que  $(1 + \mu)$  est unité. Comme  $f_{i_0} \in V$  on obtient  $g_{j_0} h_{k_0} \in V$ , ce qui termine la preuve.

Il est maintenant facile de décrypter constructivement cette preuve en utilisant le théorème 2. Nous voulons montrer que  $g_j h_k$  est entier sur  $(A, \{0\})$ . Dans la preuve abstraite, la détermination des indices  $j_0$  et  $k_0$  se fait au moyen d'un usage répété de l'axiome

$$\text{si } \alpha\beta = 1, \text{ alors } \alpha \text{ est dans } V \text{ ou } \beta \text{ est dans } m_V$$

avec pour  $\alpha$  un  $g_j/g_{j'}$  ou un  $h_k/h_{k'}$ .

Par exemple avec  $n = 3$  pour trouver le bon  $g_{j_0}$ , et en notant  $x \preceq y$  pour  $x$  divise  $y$  ( $y/x \in V$ ) et  $x \prec y$  pour  $x$  divise strictement  $y$  ( $y/x \in m_V$ ), on fera les disjonctions suivantes.

Première disjonction. 0 :  $g_0 \prec g_1$  ou 1 :  $g_1 \preceq g_0$

Branche 0. 00 :  $g_0 \prec g_2$  ou 01 :  $g_2 \preceq g_0$

Branche 00. 000 :  $g_0 \prec g_3$  (résultat final  $g_0$ ) ou 001 :  $g_3 \preceq g_0$  (résultat final  $g_3$ )

Branche 01. 010 :  $g_2 \prec g_3$  (résultat final  $g_2$ ) ou 011 :  $g_3 \preceq g_2$  (résultat final  $g_3$ )

Branche 1. 10 :  $g_1 \prec g_2$  ou 11 :  $g_2 \preceq g_1$

Branche 10. 100 :  $g_1 \prec g_3$  (résultat final  $g_1$ ) ou 101 :  $g_3 \preceq g_1$  (résultat final  $g_3$ )

Branche 11. 110 :  $g_2 \prec g_3$  (résultat final  $g_2$ ) ou 111 :  $g_3 \preceq g_2$  (résultat final  $g_3$ )

Nous mettons ainsi à plat cette recherche des indices  $j_0$  et  $k_0$ , et chaque fois que l'axiome est utilisé, nous passons d'un couple (anneau, idéal) du type

$$(A[\gamma_1, \dots, \gamma_r], \langle \gamma_{i_1}, \dots, \gamma_{i_s} \rangle)$$

à deux couples de la forme

$$(A[\gamma_1, \dots, \gamma_r, \alpha], \langle \gamma_{i_1}, \dots, \gamma_{i_s} \rangle) \quad \text{et} \quad (A[\gamma_1, \dots, \gamma_r, \beta], \langle \gamma_{i_1}, \dots, \gamma_{i_s}, \beta \rangle).$$

Ceci produit un arbre d'extensions de  $(A, \{0\})$  ayant à sa racine  $(A, \{0\})$  et dont chaque feuille est (une extension d') un couple du type

$$(A[(g_j/g_{j_0})_{0 \leq j \leq m}, (h_k/h_{k_0})_{0 \leq k \leq n}], \langle (g_\ell/g_{j_0})_{j_0 < \ell \leq m}, (h_\ell/h_{k_0})_{k_0 < \ell \leq n} \rangle)$$

Pour un couple  $(A', J)$  correspondant à une telle feuille, on a

$$f_{i_0} = g_{j_0} h_{k_0} + \sum_{j_0 < \ell \leq m} g_\ell h_{i_0 - \ell} + \sum_{k_0 < \ell \leq n} h_\ell g_{i_0 - \ell} = g_{j_0} h_{k_0} (1 + \mu)$$

où  $\mu \in J$ , ce qui constitue bien une relation de dépendance intégrale (particulièrement simple) de  $g_{j_0}h_{k_0}$  sur  $(A', J)$  puisque  $\mathbb{Z}[f_{i_0}] \subset A \subset A'$ . Comme tous les  $g_jh_k$  sont dans  $g_{j_0}h_{k_0}A'$  ils sont tous entiers sur  $(A', J)$ .

Maintenant, si on fixe deux indices  $(j, k)$  on voit qu'on a construit une relation de dépendance intégrale de  $g_jh_k$  sur chaque couple (anneau, idéal) à toute feuille de l'arbre. L'utilisation systématique du théorème 2 nous permet alors de recoller petit à petit ces relations de dépendance intégrale jusqu'à obtenir celle de  $g_jh_k$  sur  $(A, \{0\})$ .

## 4 Recollement de relations de dépendance intégrale et critère valuatif

Nous montrons maintenant que le théorème 2, que nous rappelons ci-dessous, est étroitement relié, en mathématiques classiques, au critère valuatif que nous écrivons juste après dans le théorème 3.

**Théorème 2** *Soit  $J$  un idéal d'un sous anneau  $A$  d'un anneau  $B$  et  $x \in B$ . Soient  $\alpha, \beta \in B$  tels que  $\alpha\beta = 1$ , si  $x$  est entier sur  $(A[\alpha], JA[\alpha])$  et sur  $(A[\beta], \beta A[\beta] + JA[\beta])$  alors  $x$  est entier sur  $(A, J)$ .*

**Théorème 3** *Soit  $J$  un idéal d'un sous anneau  $A$  d'un anneau  $B$  et  $x \in B$ . Alors  $x$  est entier sur  $(A, J)$  si et seulement si pour tout homomorphisme  $\varphi : B \rightarrow K$  dans un corps valué  $K$  tel que  $\varphi(A) \subset V$  et  $\varphi(J) \subset m_V$  on a  $\varphi(x) \in V$ .*

Ce critère valuatif est en mathématiques classiques une conséquence immédiate (via le théorème de complétude de Gödel qui peut se démontrer en utilisant le lemme de Zorn) de la proposition 4.14 (c) dans [4]. Cette proposition admet en effet comme cas particulier le fait suivant : l'évaluation dynamique du triplet  $(J, A, B)$  sous forme  $(m_V, V, K)$  (dans un corps valué) prouve que  $x \in A$  si et seulement si  $x$  est entier sur  $(A, J)$ .

**Preuve que 3 implique 2** Supposons que  $x$  est entier sur  $(A[\alpha], JA[\alpha])$  et sur  $(A[\beta], \beta A[\beta] + JA[\beta])$  comme dans les hypothèses du théorème 2. Soit  $\varphi : B \rightarrow K$  un homomorphisme arbitraire dans un corps valué  $K$  tel que  $\varphi(A) \subset V$  et  $\varphi(J) \subset m_V$ .

On a  $\varphi(\alpha)\varphi(\beta) = 1$  dans  $K$ , donc  $\varphi(\alpha) \in V$  ou  $\varphi(\beta) \in m_V$ .

Dans le premier cas, puisque  $x$  est entier sur  $(A[\alpha], JA[\alpha])$ ,  $\varphi(x)$  est entier sur  $(\varphi(A[\alpha]), \varphi(J)\varphi(A[\alpha]))$  donc a fortiori sur  $(V, m_V)$ .

Dans le deuxième cas, le même raisonnement montre que  $\varphi(x)$  est entier sur  $(\varphi(A[\beta]), \varphi(\beta)\varphi(A[\beta]) + \varphi(J)\varphi(A[\beta]))$  donc a fortiori sur  $(V, m_V)$ .

Donc le critère valuatif s'applique, et  $x$  est entier sur  $(A, J)$ .  $\square$

Nous aurons évidemment besoin du lemme de Zorn dans la réciproque.

**Preuve que 2 implique 3 lorsque  $B$  est intègre** Il suffit de considérer le cas où  $B$  est un corps. Soit  $x$  dans  $B$  qui n'est pas entier sur  $(A, J)$ . Considérons les couples  $(A', J')$  où  $A'$  est un sous anneau de  $B$  contenant  $A$ ,  $J'$  un idéal de  $A'$  contenant  $J$  et  $x$  non entier sur  $(A', J')$ . L'ensemble de ces couples n'est pas vide puisqu'il contient  $(A, J)$ . Il est ordonné par la relation  $\leq$  définie par

$$(A', J') \leq (A'', J'') \text{ si et seulement si } A' \subset A'' \text{ et } J' \subset J''$$

Par le lemme de Zorn, il existe un couple maximal  $(V, m)$  dans cet ensemble. Montrons que  $V$  est un anneau de valuation de  $B$  et  $m$  son idéal maximal. Soit  $\alpha \in B$ ,  $\beta = 1/\alpha$ . Nous voulons

montrer que  $\alpha \in V$  ou  $\beta \in m$ .

Puisque  $x$  n'est pas entier sur  $(V, m)$ , le théorème 2 donne :

$x$  n'est pas entier sur  $(V[\alpha], mV[\alpha])$  ou  $x$  n'est pas entier sur  $(V[\beta], \beta V[\beta] + mV[\beta])$

Puisque le couple  $(V, m)$  est maximal, il est égal à l'un des deux précédents. Ceci signifie bien que  $\alpha \in V$  ou  $\beta \in m$ .  $\square$

Remarquons que l'utilisation du lemme de Zorn et du tiers exclu dans la preuve précédente pourrait être remplacée par celle du théorème de complétude de Gödel, qui, dans le cas de théories formelles ayant une présentation dénombrable, apparaît comme une conséquence de l'axiome du choix dénombrable et du principe non constructif **LLPO** (lequel signifie que tout nombre réel est  $\geq 0$  ou  $\leq 0$ , cf. par exemple [1]).

## Conclusion

Notre preuve constructive est obtenue par une “simple relecture” des arguments contenus dans une preuve classique abstraite. Elle n'a par contre aucune raison a priori de donner une construction *efficace* du résultat. Notre méthode n'a pas pour but de produire de bonnes bornes pour des algorithmes, mais de produire automatiquement des algorithmes par décryptage des preuves classiques. Nous montrons ainsi que les méthodes d'algèbre abstraite sont, très souvent, en fait constructives.

Ainsi nous pensons réaliser une sorte de programme de Hilbert pour de larges pans de l'algèbre abstraite : donner une sémantique constructive pour les objets abstraits et obtenir de manière plus ou moins automatique des preuves constructives pour les résultats concrets obtenus par les méthodes abstraites. Faisant partie de ce programme de travail, on peut citer [2, 4, 7, 6, 8, 9, 10].

Dans l'article présent, les arbres d'extensions de  $(A, \{0\})$  sont la sémantique constructive du discours abstrait sur les anneaux de valuation du corps des fractions de  $A$  qui contiennent  $A$ . Le décryptage des preuves abstraites basées sur le critère valuatif est fourni par le théorème 2, qui constitue la forme constructive du critère valuatif abstrait. De plus la preuve constructive du théorème 2 est en fait cachée dans toute preuve usuelle du critère valuatif. Ainsi la preuve constructive était bel et bien cachée dans la preuve abstraite.

## Références

- [1] Bishop E., Bridges D. : *Constructive Analysis*. Springer-Verlag (1985). 7
- [2] Coquand T., Lombardi H. *Constructions cachées en algèbre abstraite (3) Dimension de Krull, Going Up, Going Down*. Preprint 2001. 7
- [3] Coquand T., Persson H. *Valuations and Dedekind's Prague Theorem*. J. Pure Appl. Algebra **155** (2001), no. 2-3, 121–129. 1, 2
- [4] Coste M., Lombardi H., Roy M.-F. *Dynamical method in algebra : Effective Nullstellensätze* Annals of Pure and Applied Logic. sous presse 2, 3, 6, 7
- [5] Edwards H. M. : *Divisor theory*. Birkhäuser. Boston MA. 1990. 1, 2, 4
- [6] Lombardi H. *Le contenu constructif d'un principe local-global avec une application à la structure d'un module projectif de type fini*. Publications Mathématiques de Besançon. Théorie des nombres. Fascicule 94–95 & 95–96, (1997). 7
- [7] Lombardi H. *Relecture constructive de la théorie d'Artin-Schreier*. Annals of Pure and Applied Logic **91**, (1998), 59–92. 7

- [8] Lombardi H. *Dimension de Krull, Nullstellensätze et Évaluation dynamique*. Math. Zeitschrift. Sous presse. [7](#)
- [9] Lombardi H. Platitude, localisation et anneaux de Prfer, une approche constructive. Preprint 1999 [7](#)
- [10] Lombardi H., Quitté C. *Constructions cachées en algèbre abstraite (2) Théorème de Horrocks, du local au global*). Preprint 1999 [7](#)
- [11] Matsumura H. : *Commutative ring theory*. Cambridge studies in advanced mathematics n°8. Cambridge University Press. 1989 [3](#)
- [12] Weyl H. *Algebraic Theory of Numbers*. Princeton landmarks in mathematics, (1998). (édition originale 1940) [2](#)