Journées Nationales de Calcul Formel

CIRM, Luminy, 3-7 Novembre 2014

Algèbre constructive

premier exposé 3 Novembre

H. Lombardi, Besançon

Henri.Lombardi@univ-fcomte.fr, http://hlombardi.free.fr

Le tutoriel écrit en détail :
http://hlombardi.free.fr/publis/JNCF2014.pdf
Version imprimable de ces transparents :
http://hlombardi.free.fr/publis/JNCF-LectDoc1-2.pdf

Je vais essayer de vous convaincre que l'Algèbre abstraite contemporaine est **pour l'essentiel** constructive **si l'on prend la peine de « bien lire » les démonstrations usuelles**.

Lorsque l'on veut examiner le contenu concret d'un théorème d'algèbre et que l'on regarde sa démonstration en détail, si celle-ci ne se laisse pas traduire en un algorithme, on se heurte usuellement à deux obstacles :

– **l'utilisation du principe du tiers exclu**, qui permet de démontrer l'existence d'un objet concret au moyen d'une preuve par l'absurde : si l'objet n'existait pas, bla bla bla, on trouverait une contradiction dans les mathématiques,

– **l'utilisation du lemme de Zorn**, qui permet de mimer le raisonnement par récurrence même dans le cas où l'ensemble considéré n'est pas dénombrable.

van der Waerden, Brouwer

Par exemple, le Moderne Algebra de **van der Waerden** évite le deuxième obstacle en ne considérant que des structures algébriques dénombrables.

En fait, il s'avère que c'est l'utilisation du principe du tiers exclu qui constitue l'obstacle principal dans les démonstrations classiques pour les transformer en algorithmes.

Nous avons été avertis par **Brouwer** que le principe du tiers exclu est problématique lorsque l'on considère des objets infinis auxquels on prétend appliquer la logique du vrai et du faux usuelle valable pour les objets finis.

L'évaluation paresseuse

Or **le moyen de contourner l'obstacle du tiers exclu est fourni par une pratique courante en Calcul Formel**, connue sous le nom de **l'évaluation paresseuse.**

Le paradigme est fourni par la méthode **D5** qui permet de calculer dans la clôture algébrique d'un corps explicite, sans jamais se tromper, même si aucune clôture algébrique de ce corps ne peut être construite (au sens usuel de la chose).

1 - Théorème de la base adaptée

cohérence, noethérianité

Théorème 1. (Théorème de la base adaptée)
Soit G un sous-groupe de $(\mathbb{Z}^n, +)$. Alors **il existe** *une $\mathbb{Z}$-base $(e_1, \ldots, e_n)$ de $\mathbb{Z}^n$, un entier $r \in [\![0..n]\!]$, et des entiers $a_1, \ldots, a_r > 0$ qui vérifient :*

– *a_i divise a_{i+1} $(i \in [\![1..r]\!])$,*

– *$(a_1 e_1, \ldots, a_r e_r)$ est une $\mathbb{Z}$-base de G.*

Dans ces conditions, la liste des entiers a_i est déterminée de manière unique. En outre le sous-groupe $\tilde{G} = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_r$ de $\mathbb{Z}^n$ ne dépend que de G : c'est l'ensemble des x tels qu'il existe $k \neq 0$ avec $kx \in G$. Enfin $(\tilde{G} : G) = a_1 \cdots a_r$.

Nous allons faire une analyse du contenu constructif de ce théorème.

Le contenu concret du théorème dépend de la réponse à la question : « comment le sous-groupe G nous est-il donné ? »

Le théorème de la base adaptée pour un sous-groupe de type fini de $\mathbb{Z}^n$

Théorème 2. (Théorème de réduction de Smith pour $\mathbb{Z}$)
Soit M une matrice $\in \mathbb{Z}^{n\times m}$, alors elle admet une **réduction de Smith** *: il existe deux matrices inversibles $C \in \mathbb{Z}^{m\times m}$ et $L \in \mathbb{Z}^{n\times n}$ telles que la matrice $D = LMC$ est sous* forme de Smith, *i.e., tous les coefficients $d_{i,j}$ avec $i \neq j$ sont nulles, et $d_{i,i}$ divise $d_{i+1,i+1}$ $(1 \leqslant i \leqslant \min(m,n) - 1)$.*
En outre si l'on choisit les $d_{i,i}$ positifs ou nuls, ils sont déterminés de manière unique par M (en fait le produit $d_{1,1} \cdots d_{k,k}$ est égal au pgcd des mineurs $k \times k$ de M).

Le théorème de la base adaptée pour un sous-groupe de type fini de $\mathbb{Z}^n$

Corollaire 3. *Soit $\varphi : \mathbb{Z}^m \to \mathbb{Z}^n$ une application $\mathbb{Z}$-linéaire (c'est-à-dire un homomorphisme de groupes).*

1. *Le théorème de la base adaptée s'applique à* $\operatorname{Ker}\varphi$ *et* $\operatorname{Im}\varphi$.
2. *En outre $\mathbb{Z}^m = \operatorname{Ker}\varphi \oplus N$ avec un sous-$\mathbb{Z}$-module N libre, autrement dit une $\mathbb{Z}$-base de* $\operatorname{Ker}\varphi$ *se prolonge en une $\mathbb{Z}$-base de $\mathbb{Z}^m$.*

Une autre conséquence du théorème 2 est que *les systèmes d'équations linéaires avec coefficients et inconnues dans $\mathbb{Z}$ peuvent être résolus et discutés d'une manière simple et systématique.*
Ceci ne ressortait pas clairement du théorème 1.

Définition 4.

- *Un anneau commutatif* $\mathbf{A}$ *est appelé un* **anneau de Smith** *si toute matrice admet une réduction de Smith.*
- *Un anneau est dit* **zéro-dimensionnel** *lorsqu'il vérifie l'axiome suivant :*

$$\forall x \in \mathbf{A}\ \exists y \in \mathbf{A}\ \exists k \in \mathbb{N} \qquad x^k = yx^{k+1}. \tag{1}$$

- *Un anneau intègre* $\mathbf{A}$ *est dit* **de dimension** $\leqslant 1$ *si, pour tout élément* $a \neq 0$*, le quotient* $\mathbf{A}/\langle a \rangle$ *est zéro-dimensionnel.*

Théorème 5. *Tout anneau de Bezout intègre de dimension* $\leqslant 1$ *est un anneau de Smith.*

Intersections de sous-groupes de type fini
Cohérence

Une autre manière de décrire en termes finis un sous-groupe de $\mathbb{Z}^n$ est de le donner comme *une intersection finie de sous-groupes de type fini* de $\mathbb{Z}^n$.

Théorème 6. *Le théorème de la base adaptée est valable pour toute intersection finie de sous-groupes de type fini de* $\mathbb{Z}^n$.

Plus généralement, le « calcul » de l'intersection de sous-modules de type fini est étroitement lié à la notion de cohérence.

Intersections de sous-groupes de type fini, cohérence

Définition 7.
– Un anneau $\mathbf{A}$ *est dit* **cohérent** *si toute forme linéaire* $\mathbf{A}^n \to \mathbf{A}$ *admet pour noyau un sous-module de type fini de* $\mathbf{A}^n$.
– Un $\mathbf{A}$*-module* M *est dit* **cohérent** *si toute application linéaire* $\varphi : \mathbf{A}^n \to M$ *a pour noyau un sous* $\mathbf{A}$*-module de type fini de* $\mathbf{A}^n$.

Proposition 8. *Un* $\mathbf{A}$*-module* M *est cohérent si, et seulement si, il vérifie les deux propriétés suivantes :*
– l'intersection de deux sous-module de type fini est de type fini ;
– l'annulateur $(0 : a) = \{\, x \in \mathbf{A} \mid ax = 0 \,\}$ *de tout élément* $a \in M$ *est de type fini.*

Ainsi tout anneau de Bezout intègre est cohérent.

Noethérianité

Le théorème 1 (théorème de la base adaptée classique) peut être décomposé en deux parties.

– Tout sous-groupe *de type fini* de $\mathbb{Z}^n$ admet une base adaptée (corollaire 3).

– Tout sous-groupe de $\mathbb{Z}^n$ est de type fini.

Noethérianité

Pour analyser constructivement la seconde assertion, on analyse les cinq propriétés suivantes pour un $\mathbf{A}$-module M, équivalentes lorsque l'on admet le principe du tiers exclu.

– [N1] Tout sous-module de M est de type fini.
– [N2] Toute suite croissante de sous-modules de M,
$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \ldots$, est constante après un certain rang.
– [N3] Toute suite croissante de sous-modules **de type fini** de M est constante après un certain rang.
– [N4] Toute suite croissante de sous-modules de type fini de M **admet deux termes consécutifs égaux**.
– [N5] Une suite strictement croissante de sous-modules de type fini de M est impossible.

Noethérianité

La définition [N4] possède les avantages suivants :

- Elle a un contenu constructif assez clair.
- Elle est équivalente en mathématiques classiques à la définition usuelle.
- Elle s'applique à la plupart des anneaux usuellement étudiés lorsque les mathématiques classiques les considèrent noethériens.
- Elle permet de rendre algorithmiques la plupart des démonstrations en mathématiques classiques qui utilisent la noethérianité dans leurs hypothèses.
- En particulier, les anneaux noethériens cohérents vérifient constructivement le théorème de la base de Hilbert.

Noethérianité

En définitive, **tout le monde est d'accord** !

Si l'on donne une suite croissante d'idéaux de type fini $(\mathfrak{a}_n)$ dans $\mathbb{Z}[X_1, \ldots, X_m]$, il est absurde de supposer que tous ses termes sont distincts.

Cela signifie que $\mathbb{Z}[X_1, \ldots, X_m]$ est un anneau noethérien.

La démonstration donnée par Richman donne **mieux** que la démonstration classique usuelle : elle explicite l'existence d'une borne pour le premier n tel que $\mathfrak{a}_n = \mathfrak{a}_{n+1}$.

2 - Nullstellensatz sans clôture algébrique

La méthode D5

Clôture algébrique à la D5

Le logiciel D5 calcule dans la clôture algébrique d'un **corps discret explicite** $\mathbf{K}$ même lorsque la clôture algébrique n'existe pas en tant qu'objet crédible d'un point de vue constructif.

La clôture algébrique apparaît ainsi comme un **objet dynamique constructif** qui évolue en fonction des problèmes qu'il doit (aider à) résoudre.

Question : faire pour introduire formellement un zéro d'un polynôme unitaire lorsque l'on ne dispose pas d'algorithme de factorisation des polynômes sur le corps où l'on travaille. Ou simplement si un tel algorithme coûte trop cher ?

/...

Algorithme de factorisation partielle

Réponse : remplacer la factorisation absolue (trop difficile) par des factorisations partielles (faciles).

Proposition 1. *On dispose d'un algorithme de factorisation partielle pour les familles finies de polynômes unitaires dans* $\mathbf{K}[X]$ *:*
une **factorisation partielle** *pour une famille finie* $(f_1, \ldots, f_r)$ *est donnée par une famille finie* $(g_1, \ldots, g_s)$ *de polynômes unitaires deux à deux étrangers et par l'écriture de chaque* f_i *sous la forme*

$$f_i = \prod_{k=1}^{s} g_k^{m_{k,i}} \ (m_{k,i} \in \mathbb{N}).$$

La famille $(g_1, \ldots, g_s)$ *s'appelle alors une* **base de factorisation partielle** *pour la famille* $(f_1, \ldots, f_r)$.

Rajouter un zéro d'un polynôme unitaire et calculer avec

Au départ, on a un corps $\mathbf{K}$, pour lequel :
– on connaît 0, 1 et -1,
– on dispose des opérations $+$ et $\times$ de façon explicite, et
– l'axiome CDI (tout élément est nul ou inversible) est réalisé par un algorithme.

On rajoute lorsque cela est nécessaire un zéro x_p d'un polynôme unitaire $p \in \mathbf{K}[X]$. Le calcul qui s'ensuit se passe désormais dans l'algèbre $\mathbf{K}[x_p] = \mathbf{K}[X]/\langle p \rangle$, du moins tant qu'il ne s'agit pas de mettre en œuvre l'axiome CDI.

À un certain moment du calcul, il peut se produire que l'on ait besoin d'expliciter l'axiome CDI pour un élément $a = q(x_p)$ de $\mathbf{K}[x_p]$. On peut supposer que $\deg(q) < \deg(p)$.

Rajouter un zéro d'un polynôme unitaire et calculer avec

On commence par calculer $r = \text{pgcd}(p, q)$.
Si $r = 1$ ou $r = p$ (i.e. $q = 0$), l'algorithme donne la réponse facilement.
Sinon, on calcule une base de factorisation partielle $(g_1, \ldots, g_s)$ pour (p, q). On obtient ainsi une partition de $[\![1..s]\!]$ en trois ensembles I, J, K :

- les g_i pour $i \in I$ divisent p et q,
- les g_i pour $i \in J$ divisent p mais ne divisent pas q,
- les g_i pour $i \in K$ divisent q mais ne divisent pas p.

Notons que I ne peut être vide (dans ce cas $\text{pgcd}(p, q) = 1$). Une inspection détaillée de l'algorithme de factorisation partielle pour (p, q) montre que J et K ont chacun au plus un élément. Plusieurs éventualités pour la suite selon que J est vide ou pas.

Rajouter un zéro d'un polynôme unitaire et calculer avec

cas où $J = \emptyset$

Alors a est nilpotent dans $\mathbf{K}[x_p]$, on a la réponse $a = 0$. Le polynôme $\boxed{p_1 = \prod_{i \in I} g_i}$ a les mêmes zéros que p dans toute $\mathbf{K}$-algèbre réduite.

– A priori, on remplace p par p_1 (qui peut être égal à p). On est désormais dans l'algèbre $\mathbf{K}[X]/\langle p_1 \rangle$.

– Si I contient plusieurs indices, on a parfois intérêt à ouvrir plusieurs branches, dans chacune d'entre elles p est remplacé par l'un des g_i pour $i \in I$. Dans la branche i on travaille modulo g_i, i.e. on est dans l'algèbre $\mathbf{K}[X]/\langle g_i \rangle$.

cas où $J \neq \emptyset$

On écrit $p_1 = \prod_{i \in I} g_i$ et $p_2 = g_j$ où $J = \{j\}$. Comme $p_1 p_2$ divise p et p divise une puissance de $p_1 p_2$, on peut déjà remplacer p par $p_1 p_2$. Mais la réponse à la question relative à l'élément a est différente selon que $p_1 = 0$ ou $p_2 = 0$. En conséquence, **on ouvre deux branches de calcul pour l'avenir**.

- Dans la première branche, a est nul et p est remplacé par p_1 ; en outre si I contient plusieurs éléments, on a parfois intérêt à ouvrir des branches de calcul séparées, pour chaque $i \in I$.
- Dans la seconde branche, a est inversible et p est remplacé par p_2.

Rajouter des zéros en cascade

Examinons maintenant ce qui se passe lorsque l'on veut introduire, après un zéro x_1 de $p_1 \in \mathbf{K}[X_1]$, un zéro d'un polynôme unitaire $p_2(X_2) \in \mathbf{K}_1[X_2]$, où $\mathbf{K}_1 = \mathbf{K}[x_1]$.

Dans chaque branche du calcul ouverte précédemment, $\mathbf{K}[X]/\langle g_i \rangle$, on va faire comme si l'algèbre était un corps discret et procéder de la même manière que lors du rajout du premier zéro.

Si l'on trouve un obstacle (par exemple dans le calcul d'un pgcd dans la branche où l'on se trouve) c'est que le polynôme g_i correspondant n'est pas irréductible. Cependant, cela n'est pas grave, car il suffit de raffiner l'étude de la situation en introduisant des branches correspondant à des facteurs de g_i deux à deux étrangers. Dans chacune d'elle le calcul voulu pourra aboutir.

Traiter les systèmes polynomiaux à la D5

Sur une clôture algébrique d'un corps discret $\mathbf{K}$ on peut construire (de façon élémentaire ou de façon savante) une décomposition cylindrique algébrique pour n'importe quel système polynomial pris dans $\mathbf{K}[X_1, \ldots, X_n]$.

En l'absence de clôture algébrique, la construction fonctionne encore « à la D5 ».
On en déduit alors une version explicite pour le théorème de Chevalley : la projection d'un constructible (défini sur $\mathbf{K}$) sur un sous-espace de coordonnées est un constructible (défini sur $\mathbf{K}$).

On peut aussi en déduire des versions constructives du Nullstellensatz.

Nullstellensatz faible

Ne cherchez pas les zéros bien loin !

Théorème 2. (Nullstellensatz faible)
Soit $\mathbf{K}$ *un corps discret et* $(f_1, \ldots, f_s)$ *un système polynomial dans l'algèbre* $\mathbf{K}[\underline{X}] = \mathbf{K}[X_1, \ldots, X_n]$ $(n \geqslant 1)$.
Notons $\mathfrak{f} = \langle f_1, \ldots, f_s \rangle_{\mathbf{K}[\underline{X}]}$ *et* $\mathbf{A} = \mathbf{K}[\underline{X}]/\mathfrak{f}$.

Énoncé classique

Si le système n'admet aucun zéro dans une clôture algébrique de $\mathbf{K}$, *alors* $\mathbf{A} = \{0\}$, *c'est-à-dire* $1 \in \langle f_1, \ldots, f_s \rangle$, *et le système n'admet de zéro dans aucune* $\mathbf{K}$*-algèbre non nulle.*

Énoncé constructif

- *Ou bien* $\mathbf{A} = \{0\}$, *c'est-à-dire on construit une égalité* $1 \in \langle f_1, \ldots, f_s \rangle$.
- *Ou bien on construit un quotient de* $\mathbf{A}$ *qui est une* $\mathbf{K}$*-algèbre strictement finie non nulle.*

Nullstellensatz usuel, version constructive

La notation $h \#_{\mathbf{C}} 0$ signifie que h est inversible dans l'anneau $\mathbf{C}$.

Théorème 3. (Nullstellensatz usuel, version constructive générale)
Soit $\mathbf{K}$ un corps discret et $f_1, \ldots, f_s, g$ dans $\mathbf{K}[X_1, \ldots, X_n]$. Considérons l'algèbre quotient $\mathbf{A} = \mathbf{K}[\underline{X}]/\langle f_1, \ldots, f_s\rangle$.

1. *Ou bien il existe un quotient non nul $\mathbf{B}$ de $\mathbf{A}$ qui est une $\mathbf{K}$-algèbre strictement finie avec $g \#_{\mathbf{B}} 0$(*).*
2. *Ou bien g est nilpotent dans $\mathbf{A}$, autrement dit, il existe un entier N tel que $g^N \in \langle f_1, \ldots, f_s\rangle_{\mathbf{K}[\underline{X}]}$. A fortiori, g s'annule en tout zéro du système polynomial $(f_1, \ldots, f_s)$ dans n'importe quelle $\mathbf{K}$-algèbre réduite.*

*A fortiori $g \# 0$ dans tout quotient de $\mathbf{B}$.

Merci de votre attention