page 1

Séminaire de Géométrie de Rennes 14 Janvier 2015

Le principe local-global en algèbre constructive

H. Lombardi, Besançon

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

Voir les transparents : http://hlombardi.free.fr/publis/Rennes2015Slides.pdf

page 2

Le principe local-global en mathématiques classiques

Les idéaux premiers sont omniprésents en algèbre commutative moderne.
Les idéaux premiers semblent en particulier essentiels dans tout ce que l'on appelle le **principe local-global** en mathématiques classiques. Ce principe informel dit que les bonnes propriétés des anneaux ou des modules sont celles qui obéissent à la règle suivante :
• *Forme usuelle d'un principe local-global abstrait. La propriété est satisfaite si, et seulement si, elle est satisfaite après localisation en n'importe quel idéal premier.* [1]

page 3

Il y a cependant des propriétés qui mériteraient d'être qualifiées de bonnes, comme le fait pour un module d'être de type fini ou d'être cohérent, et qui n'obéissent pas à la règle ci-dessus, mais seulement à la règle suivante :
• *Forme variante d'un principe local-global abstrait. La propriété est satisfaite si, et seulement si, elle est satisfaite après localisation au voisinage de n'importe quel idéal premier.*
Dans la règle en question, « après localisation au voisinage de l'idéal premier $\mathfrak{P}$ » signifie qu'il existe un $s \notin \mathfrak{P}$ tel que la propriété est satisfaite pour le changement d'anneau de base $\mathbf{A} \to \mathbf{A}[1/s]$.

page 4

Le lien avec les schémas de Grothendieck

En mathématiques classiques, une propriété peut être légitimement transférée des schémas affines et faisceaux de modules sur ces schémas aux schémas généraux et faisceaux de modules **exactement** quand elle satisfait la forme variante du principe local-global abstrait.
Pour la plupart des propriétés, la forme variante (plus difficile à utiliser) découle de la forme usuelle.

page 5

Le principe local-global en mathématiques constructives

En mathématiques constructives, on a mis au point une contrepartie (une interprétation algorithmique) des principes local-globals des mathématiques classiques sous forme de :
– théorèmes appelés **principes local-globals concrets** d'une part,
– et d'une méthode de décryptage des démonstrations classiques, appelée **machinerie locale-globale constructive de base**, ou encore *machinerie locale-globale à idéaux premiers* d'autre part.
Ceci permet de *transformer* les démonstrations classiques qui utilisent un principe local-global abstrait et aboutissent à une conclusion concrète *en des algorithmes* qui fournissent la conclusion sous forme explicite.
Cette méthode est une extension raisonnée de l'évaluation dynamique à la D5.

1. Variante non pertinente : *après localisation en n'importe quel idéal maximal.*

Définition 1.

1. *Des éléments $s_1, \ldots, s_n$ sont dits* comaximaux *si $\langle 1\rangle = \langle s_1, \ldots, s_n\rangle$. Deux éléments comaximaux sont aussi appelés* étrangers.
2. *Des monoïdes $S_1, \ldots, S_n$ sont dits* comaximaux *si chaque fois que $s_1 \in S_1, \ldots, s_n \in S_n$, les s_i sont comaximaux.*
3. *On dit que* les monoïdes $S_1, \ldots, S_n$ de l'anneau $\mathbf{A}$ recouvrent le monoïde S *si S est contenu dans le saturé de chaque S_i et si un idéal de $\mathbf{A}$ qui coupe chacun des S_i coupe toujours S, autrement dit si l'on a :*

$$\forall s_1 \in S_1 \ \ldots \ \forall s_n \in S_n \ \ \exists\, a_1, \ldots, a_n \in \mathbf{A} \quad \sum_{i=1}^{n} a_i s_i \in S.$$

Principes local-globals concrets

Quatre exemples.
Soient $S_1, \ldots, S_n$ des monoïdes comaximaux de $\mathbf{A}$, $\varphi : M \to N$ et $\theta : N \to P$ des applications linéaires, et $x \in N$. On note $\mathbf{A}_i$ pour $\mathbf{A}_{S_i}$, M_i pour M_{S_i} etc. Alors on a les équivalences suivantes.

1. Recollement concret des solutions de systèmes linéaires :
   $x \in \operatorname{Im}\varphi$ **ssi** $x/1 \in \operatorname{Im}\varphi_i$ pour $i \in [\![1..n]\!]$.
2. Recollement concret des suites exactes :
   La suite $M \xrightarrow{\varphi} N \xrightarrow{\theta} P$ est exacte **ssi**
   les suites $M_i \xrightarrow{\varphi_i} N_i \xrightarrow{\theta_i} P_i$ sont exactes pour $i \in [\![1..n]\!]$.
3. Recollement concret des modules de présentation finie :
   M est de présentation finie **ssi** M_i est de présentation finie pour $i \in [\![1..n]\!]$.
4. Recollement concret de facteurs directs dans les modules de présentation finie. Ici M est un sous-module de type fini d'un module de présentation finie N :
   M est facteur direct dans N **ssi**
   M_i est facteur direct dans N_i pour $i \in [\![1..n]\!]$.

Décryptage, un exemple

Au tableau noir

Un exemple « historique » pour moi, concernant le premier théorème de Bourbaki sur les modules projectifs de type fini.
Pour le décrypter j'avais besoin du théorème suivant.

Théorème (Matrices de projection : idempotents et localisations libres) *Soit $\mathbf{A}$ un anneau, $F \in \mathrm{Mat}_n(\mathbf{A})$ avec $F^2 = F$ et M le module projectif de type fini image de F dans $\mathbf{A}^n$.*
Posons $\mathrm{R}_M(1+X) := \det(\mathrm{I}_n + XF)$ et $\mathrm{R}_M(X) = r_0 + r_1X + \cdots + r_nX^n$.
Alors le système $(r_0, r_1, \ldots, r_n)$ est un système fondamental d'idempotents orthogonaux.
En outre, les mineurs d'ordre $(k+1)$ de la matrice r_kF sont tous nuls.
En conséquence, si s est un mineur diagonal d'ordre k de r_kF, alors le module M_s est libre de rang k sur l'anneau $\mathbf{A}_s$.

Décryptage : introduction

Nous en venons maintenant à la partie « décryptage » de démonstrations classiques lorsqu'elles utilisent la localisation en un idéal premier arbitraire.
Notre but est d'arriver à un résultat permettant d'utiliser un principe local-global concret en lieu et place d'un principe local-global abstrait correspondant. La démonstration classique utilise le lemme de Krull. La contrepartie constructive est le lemme 3.
Les choses sont plus faciles à intuiter en introduisant la notion de **premier idéal**.

Premiers idéaux

Définition 2. *Soient U et I des parties de l'anneau $\mathbf{A}$. Nous notons $\mathcal{M}(U)$ le monoïde engendré par U, et $\mathcal{S}(I,U)$ est le monoïde :*

$$\mathcal{S}(I,U) = \langle I\rangle_{\mathbf{A}} + \mathcal{M}(U).$$

*Le couple $\mathfrak{q} = (I,U)$ est appelé un **premier idéal**, et l'on note $\mathbf{A}_{\mathfrak{q}}$ pour $\mathbf{A}_{\mathcal{S}(I,U)}$. De la même manière on note :*

$$\mathcal{S}(a_1,\dots,a_k;u_1,\dots,u_\ell) = \langle a_1,\dots,a_k\rangle_{\mathbf{A}} + \mathcal{M}(u_1,\dots,u_\ell).$$

Nous disons qu'un tel monoïde admet une description finie *et le couple $(\{a_1,\dots,a_k\},\{u_1,\dots,u_\ell\})$ est appelé un **premier idéal fini**.*

Le premier idéal (I,U) doit être vu comme *une approximation d'un idéal premier* $\mathfrak{p}$ contenant I et ne contenant aucun élément de U. Un premier idéal fini est vu comme une approximation finie.
Si $0 \in \mathcal{S}(I,U)$ l'approximation ne fonctionne pas, on dit que le premier idéal *collapse*.

Premiers idéaux, 2

Le **radical de Jacobson** d'un anneau $\mathbf{A}$ est l'idéal :

$$\mathrm{Rad}(\mathbf{A}) := \Big\{\, a \in \mathbf{A} \mid 1 + a\mathbf{A} \subseteq \mathbf{A}^\times \,\Big\}. \tag{1}$$

Le fait important à souligner est que, vue dans l'anneau localisé $\mathbf{A}_{\mathfrak{q}}$, la partie U est contenue dans les unités, et la partie I est contenue dans le radical de Jacobson.
C'est ce qui va permettre à notre décryptage constructif de fonctionner, car une fois que l'on aura forcé un élément à être dans le radical de Jacobson, il n'en sortira plus jamais.

Un défi de l'algèbre constructive est de ramener tout discours sur les idéaux premiers à un discours sur leurs approximations finies.

Premiers idéaux, 3

Lemme 3. (Lemme de Krull constructif, une version parmi d'autres)
Soit $\mathbf{A}$ *un anneau,* (I, U) *un premier idéal,* $S = \mathcal{S}(I, U)$*, et* $a \in \mathbf{A}$*.*
– *Les monoïdes* $\mathcal{S}(I; U, a)$ *et* $\mathcal{S}(I, a; U)$ *recouvrent le monoïde* $\mathcal{S}(I, U)$*.*
– *En particulier, les monoïdes* $\mathcal{M}(a) = \mathcal{S}(0; a)$ *et* $\mathcal{S}(a; 1) = 1 + a\mathbf{A}$ *sont comaximaux.*
– *De même, si* S*,* S_1*, …,* $S_n \subseteq \mathbf{A}$ *sont des monoïdes comaximaux, alors les monoïdes* $\mathcal{S}(I; U, a)$*,* $\mathcal{S}(I, a; U)$*,* S_1*, …,* S_n *sont comaximaux.*

Le premier point remplace la disjonction utilisée en mathématiques classiques, lorsque l'on dit qu'un élément arbitraire a de $\mathbf{A}$ est :
– ou bien un élément de l'idéal premier $\mathfrak{p}$,
– ou bien un élément du filtre complémentaire.

Machinerie locale-globale à idéaux premiers

Un **anneau local** est un anneau $\mathbf{A}$ où est vérifié l'axiome suivant :

$$\boxed{\forall x,\, y \in \mathbf{A} \qquad x + y \in \mathbf{A}^\times \implies (x \in \mathbf{A}^\times \text{ ou } y \in \mathbf{A}^\times)} \tag{2}$$

Rappelons que le radical de Jacobson de $\mathbf{A}$ est l'idéal :

$$\mathrm{Rad}(\mathbf{A}) := \Big\{\, a \in \mathbf{A} \mid 1 + a\mathbf{A} \subseteq \mathbf{A}^\times \,\Big\}. \tag{3}$$

Un **anneau local résiduellement discret** est un anneau local dont le corps résiduel $\mathbf{k} = \mathbf{A}/\mathrm{Rad}(\mathbf{A})$ est un corps discret. Un tel anneau peut être caractérisé par l'axiome suivant

$$\boxed{\forall x \in \mathbf{A} \qquad x \in \mathbf{A}^\times \text{ ou } x \in \mathrm{Rad}(\mathbf{A})} \tag{4}$$

Machinerie locale-globale à idéaux premiers

Un argument de type local-global typique fonctionne comme suit en mathématiques classiques.

— Lorsque l'anneau est local une certaine propriété P est vérifiée en vertu d'une démonstration assez concrète.
— Lorsque l'anneau n'est pas local, la même propriété est encore vraie (d'un point de vue classique) car il suffit de la vérifier localement. Ceci en vertu d'un principe local-global abstrait.

Nous examinons avec un peu d'attention la première démonstration. Nous voyons alors apparaître certains calculs qui sont faisables en vertu de l'axiome (4), axiome qui est appliqué à des éléments x provenant de la preuve elle-même. Autrement dit, la preuve classique donnée dans le cas local nous fournit une preuve constructive sous l'hypothèse d'un anneau local résiduellement discret.

Machinerie locale-globale à idéaux premiers

Voici maintenant notre décryptage dynamique constructif.
Dans le cas d'un anneau arbitraire, nous répétons la même démonstration, en remplaçant chaque disjonction « $x \in \mathbf{A}^\times$ ou $x \in \mathrm{Rad}(\mathbf{A})$ », par l'introduction des deux anneaux $\mathbf{A}_{\mathcal{S}(I;x,U)}$ et $\mathbf{A}_{\mathcal{S}(I,x;U)}$, où $\mathbf{A}_{\mathcal{S}(I,U)}$ est la localisation « courante » de l'anneau $\mathbf{A}$ de départ, à l'endroit de la preuve où l'on se trouve.
Lorsque la preuve initiale est ainsi déployée, on a construit à la fin un certain nombre (fini parce que la preuve est finie) de localisés $\mathbf{A}_{S_i}$, pour lesquels la propriété est vraie.
D'un point de vue constructif, nous obtenons ainsi le résultat « quasi global », c'est-à-dire après localisation en des monoïdes comaximaux, en vertu du lemme 3.
On fait alors appel à un principe local-global concret pour conclure.

Machinerie locale-globale à idéaux premiers

Le mieux est de traiter un nouvel exemple au tableau.
On parle ici de la solution par Quillen de la conjecture de Serre.

Il y a trois aspects dans la constructivisation de la preuve de Quillen.
1) *Le Quillen patching*
Version constructive.
Quillen Patching. [ACMC, XVI-3.7]
Soit M un module de présentation finie sur $\mathbf{A}[X]$ et $S_1, \ldots, S_n$ des monoïdes comaximaux de $\mathbf{A}$. Alors, M est un module étendu depuis $\mathbf{A}$ si, et seulement si, chaque M_{S_i} est étendu depuis $\mathbf{A}_{S_i}$.
Version classique.
Quillen Patching. [Lam, V.1.6]
Soit M un module de présentation finie sur $\mathbf{A}[X]$

1. *L'ensemble $\{\, s \in \mathbf{A} \mid M_s$ (module sur $\mathbf{A}_s[X]$) est étendu depuis $\mathbf{A}_s \,\}$ est un idéal de $\mathbf{A}$.*
2. *Si pour tout idéal maximal $\mathfrak{m}$ de $\mathbf{A}$, $M_\mathfrak{m}$ est libre (sur $\mathbf{A}_\mathfrak{m}$), alors M est étendu depuis $\mathbf{A}$.*

On voit que Lam a mis un point *1* sans aucune référence à des idéaux maximaux : il a bien compris que le véritable contenu du point *2* (abstrait) est le point *1* (de nature élémentaire), et il insiste dessus.
Ce point *1* n'est qu'une variante de la version constructive, et la preuve dans Lam est essentiellement constructive.
2) *Le théorème de Horrocks, passage du local au global*
Théorème de Horrocks local.
Soit $\mathbf{A}$ un anneau local résiduellement discret et P un module projectif de type fini sur $\mathbf{A}[X]$. Soit S le monoïde des polynômes unitaires de $\mathbf{A}[X]$. On note $\mathbf{A}\langle X\rangle = \mathbf{A}_S[X]$.
Si P_S (module sur $\mathbf{A}\langle X\rangle$) est libre, alors P est libre sur $\mathbf{A}[X]$ (donc étendu depuis $\mathbf{A}$).
On trouve une preuve presque constructive dans Lam, et complètement algorithmique dans [ACMC].
Théorème de Horrocks global.
Soit $\mathbf{A}$ un anneau commutatif arbitraire et P un module projectif de type fini sur $\mathbf{A}[X]$. Soit S le monoïde des polynômes unitaires de $\mathbf{A}[X]$. On note $\mathbf{A}\langle X\rangle = \mathbf{A}_S[X]$.
Si P_S (module sur $\mathbf{A}\langle X\rangle$) est étendu depuis $\mathbf{A}$, alors P étendu depuis $\mathbf{A}$.

Pour passer du local au global, Quillen (et Lam) utilisent le point *2* du Quillen Patching classique.
Nous, nous soumettons la preuve (complètement algorithmique) du cas local résiduellement discret au processus de décryptage. Nous obtenons à la fin de la relecture des monoïdes comaximaux $S_1, \ldots, S_m$ tels que chaque M_{S_i} est étendu depuis $\mathbf{A}$. Nous concluons par le Quillen Patching constructif (qui n'est autre que le point *1* de la version Lam).
3) *L'induction de Quillen*
Induction de Quillen abstraite
Soit $\mathcal{F}$ une classe d'anneaux qui satisfait les propriétés suivantes.

(Q1) *Si $\mathbf{A} \in \mathcal{F}$, alors $\mathbf{A}\langle X\rangle \in \mathcal{F}$.*

(Q2) *Si $\mathbf{A} \in \mathcal{F}$, alors $\mathbf{A}_{\mathfrak{m}} \in \mathcal{F}$ pour tout idéal maximal $\mathfrak{m}$ de $\mathbf{A}$.*

(Q3) *Si $\mathbf{A} \in \mathcal{F}$ est local, tout $\mathbf{A}[X]$-module projectif de type fini est étendu depuis $\mathbf{A}$ (i.e., libre).*

Alors, pour tout $\mathbf{A} \in \mathcal{F}$ et tout $r \geqslant 1$, tout module projectif de type fini sur $\mathbf{A}[X_1, \ldots, X_r]$ est étendu depuis $\mathbf{A}$.
En fait (Q2) et (Q3) servent surtout à traiter le cas $r = 1$.
Comme on le voit sur les deux versions constructives suivantes, sans idéaux maximaux.
Induction de Quillen concrète
Soit $\mathcal{F}$ une classe d'anneaux qui satisfait les propriétés suivantes.

(q1) *Si $\mathbf{A} \in \mathcal{F}$, alors $\mathbf{A}\langle X\rangle \in \mathcal{F}$.*

(q3) *Si $\mathbf{A} \in \mathcal{F}$, tout $\mathbf{A}[X]$-module projectif de type fini est étendu depuis $\mathbf{A}$.*

Alors, pour tout $\mathbf{A} \in \mathcal{F}$ et tout $r \geqslant 1$, tout module projectif de type fini sur $\mathbf{A}[X_1, \ldots, X_r]$ est étendu depuis $\mathbf{A}$.
Cette induction utilise de manière cruciale le théorème de Horrocks global.
Comme cas particulier on a la version suivante qui suffit pour résoudre positivement le problème de Serre (cas des corps, mais aussi des anneaux zéro-dimensionnels réduits, ou des anneaux de Bezout intègres de dimension $\leqslant 1$)
Induction de Quillen concrète, cas libre
Soit $\mathcal{F}$ une classe d'anneaux qui satisfait les propriétés suivantes.

(q0) *Si $\mathbf{A} \in \mathcal{F}$, tout $\mathbf{A}$-module projectif de type fini est libre.*

(q1) *Si $\mathbf{A} \in \mathcal{F}$, alors $\mathbf{A}\langle X\rangle \in \mathcal{F}$.*

Alors, pour tout $\mathbf{A} \in \mathcal{F}$ et tout $r \geqslant 1$, tout module projectif de type fini sur $\mathbf{A}[X_1, \ldots, X_r]$ est étendu depuis $\mathbf{A}$.
Pour décrypter complètement la version abstraite de Quillen, il reste à comprendre comment, à partir de preuves, en mathématiques classiques, qu'une classe d'anneaux vérifie (Q2) et (Q3), on peut fournir une preuve constructive que la classe vérifie (q3).
(Q2) doit être remplacé par : Si $\mathbf{A} \in \mathcal{F}$, alors $\mathbf{A}_{\mathfrak{m}} \in \mathcal{F}$ pour tout premier idéal fini $\mathfrak{m}$ de $\mathbf{A}$.
et (Q3) doit être démontré sous la forme précise suivante : Si $\mathbf{A} \in \mathcal{F}$ est local résiduellement discret, tout $\mathbf{A}[X]$-module projectif de type fini est étendu depuis $\mathbf{A}$ (i.e., libre).
On n'a pas un théorème, mais un fait expérimental : en pratique, notre méthode de décryptage fonctionne dans chaque cas particulier envisagé.

Dans l'ouvrage [ACMC], on a rarement besoin d'utiliser cette machinerie car les principes local-globals concrets suffisent souvent à résoudre directement les problèmes.
Néanmoins, cette machinerie devient indispensable dans le chapitre XVI pour décrypter des démonstrations sophistiquées :
– la démonstration par Quillen du théorème de Quillen-Suslin, la généralisation du résultat aux anneaux principaux,

– la généralisation non noethérienne aux domaines de Bezout de dimension 1 (due à Brewer&Costa),
– et enfin, nettement plus fort encore, la généralisation aux anneaux de Bezout arbitraires et aux anneaux arithmétiques due à Lequain&Simis.

page 18

Machinerie locale-globale à idéaux maximaux

On trouve dans la littérature un certain nombre de preuves dans lesquelles l'auteur démontre un résultat en considérant « le passage au quotient par un idéal maximal arbitraire ».
Cela revient en général à appliquer le principe suivant : *un anneau qui n'a pas d'idéaux maximaux est réduit à* 0.
Le raisonnement se présente comme une preuve par l'absurde. Si l'anneau n'était pas réduit à 0, il contiendrait un idéal maximal. En passant au quotient on travaille sur un corps, où l'on trouve une contraduction.
En se basant sur la méthode dynamique à la D5, on a mis au point une méthode générale pour décrypter ce type de démonstration classique et obtenir la conclusion sous forme d'un algorithme.

page 19

Machinerie locale-globale à idéaux premiers minimaux

La situation est ici analogue à la précédente.
La démonstration classique est basée sur l'adage : *un anneau qui ne possède pas d'idéal premier minimal est réduit à* 0.
Un exemple spectaculaire de décryptage a été obtenu pour le théorème de Traverso-Swan sur les anneaux seminormaux.

page 20

Conclusion

Tout ceci fait écho aux préconisations de **Poincaré**.
1. Ne jamais envisager que des objets susceptibles d'être définis en un nombre fini de mots.
2. Ne jamais perdre de vue que toute proposition sur l'infini doit être la traduction, l'énoncé abrégé de propositions sur le fini.
3. Éviter les classifications et les définitions non prédicatives.
dans : La logique de l'infini, 1909.

page 21

Merci de votre attention