Séminaire d'histoire et de philosophie des mathématiques.

2/6/2023

La philosophie de l'algèbre dynamique.

Cette expression est due à Henri Lombardi (HL) qui, ensemble avec ses collaborateurs (Thierry Coquand, Marie-Françoise Roy (MFR), Michel Coste (MC), Ihsen Yengui), étudie le "contenu constructif des mathématiques classiques". Il s'agit de comprendre l'usage de concepts non constructifs en mathématiques classiques. En voici un exemple : considérons l'extension K du corps $\mathbb{Q}$ avec les racines de $X^2-\varepsilon_n$, où $\varepsilon_n = 1$ si $2n+6$ s'écrit comme la somme de deux nombres premiers et $\varepsilon_n = -1$ sinon. K est bien construit, mais on ne sait pas si $K=\mathbb{Q}$ ou $K=\mathbb{Q}(i)$. Si on considère maintenant l'extension A de K avec la racine de X^2+1, c'est-à-dire l'anneau $K[X]/(X^2+1)$, c'est un corps dans le premier cas et dans le deuxième cas on a $(X+i)(X-i)=0$, ce qui permet de l'identifier comme $K\oplus K$. Par exemple, on ne sait pas décomposer X^2+1 en facteurs irréductibles sur ce corps.

Le déclic pour HL est venu de la lecture d'un texte connu comme D5 (J Della Dora C Di Crescenzo D Duval) qui décrit une implémentation du calcul dans $\mathbb{Q}[X_1,\dots,X_n]/(P_1(X_1), P_2(X_1,X_2),\dots,P_n(X_1,\dots,X_n))$ sans connaître au préalable une factorisation de $P_1(X_1), P_2(X_1,X_2),\dots, P_n(X_1,\dots,X_{n-1},X_n)$. Notons bien que $+, -, \times$ ne posent pas problème : c'est $=$ et $/$ qui posent problème. L'exemple qu'ils donnent est le programme

« Si $a=0$ alors 0 sinon $\frac{1}{a}$ » pour l'image a de $A(X) = 2X^4+X^3+X^2+X-1$ dans $\mathbb{Q}[X]/P(X)$ avec $P(X) = 2X^4-3X^3-3X-2$:

→ "sans rien savoir", cela donne $\frac{1}{4X^3+X^2+4X+1}$ (en travaillant simplement dans l'anneau $\mathbb{Q}[\ \ ]/(\ \ ,\dots)$)

→ si on sait tout, on a $P(X) = (X^2+1)(2X+1)(X-2)$ et $\mathbb{Q}[X]/P(X)$ est le produit de $\mathbb{Q}[X]/(X^2+1)$, $\mathbb{Q}[X]/(2X+1)$, $\mathbb{Q}[X]/(X-2)$ et le résultat est respectivement : $0 \bmod X^2+1$, $-\frac{4}{5} \bmod 2X+1$, $\frac{1}{45} \bmod X-2$

→ Leur proposition est de regarder ce qu'il faut savoir de $P(X)$ pour répondre à la question, et donc de considérer la connaissance de $\mathbb{Q}[X]/P(X)$ comme un objet dynamique, en changement, qui s'adapte au programme rencontré.

Ici, la clé est de noter que si $P(X)$ n'a pas de facteur carré (sinon on regarde le discriminant de P et P'), on peut factoriser $P(X)$ par son pgcd avec $A(X)$: et on aura $A(X) = 0$ mod ce pgcd et $A(X)$ inversible mod $\frac{P}{\text{ce pgcd}}$.

Ici, ce pgcd $= X^2+1$ et $\frac{P}{\text{ce pgcd}} = 2X^2-3X-2$ et la résolution d'un système linéaire donne $\frac{1}{a} = \frac{74}{225}X - \frac{143}{225}$.

"We don't use any factorization algorithm nor any primitive element computation".

C'est cette idée qui a permis à MC+HL+MFR de démontrer des Nullstellensätze effectifs. Voici leur exemple prototypique : montrer que dans la théorie des corps ordonnés on a $x^3-y^3=0 \vdash x-y=0$: supposons que $x^3-y^3=0$.

Il y a deux cas à considérer :

(1) $x=0$: alors $y^3=0$, dont il s'ensuit que $\begin{smallmatrix} y^4=0 \\ y^2=0 \end{smallmatrix}$ $y=0$ et donc $x-y=0$

(2) $x^2>0$: alors $x^3-y^3 = (x-y)(x^2+xy+y^2) = (x-y)\Big(\underbrace{\tfrac{3}{4}x^2+\big(\tfrac{x}{2}+y\big)^2}_{>0 \text{ d'inverse } z}\Big)$; introduisons l'inverse z de cette somme de carrés : on a, $x-y=0$.

Le cas (1) est certifié algébriquement par :

Quimmte

(Ex1) $$(x-y)^4 + y(x^3-y^3) - (x^3-3x^2y+6xy^2-4y^3)x = 0.$$

$x^4-4x^3y+6x^2y^2-4xy^3+y^4$

$+\,x^3y \qquad -y^4$

Le cas (2) l'est par : (Ex2) $$(x-y)^2x^2+2(x-y)^2x^2+(x-y)^2(2y+x)^2-4(x-y)(x^3-y^3)=0$$

$$4(x-y)(x^3-y^3) = 3(x-y)^2x^2+(x-y)^2(x+2y)^2$$

Les deux cas ensemble donnent :

$$(x^3-3x^2y+6xy^2-4y^3)^2x^2 = \big((x-y)^4+y(x^3-y^3)\big)^2$$

$$(x-y)^2x^2(\quad)^2+2(x-y)^2x^2(\quad)^2+(x-y)^2(2y+x)^2(\quad)^2-4(x-y)(x^3-y^3)(\quad)^2 \overset{?}{=} 0$$

$$(x-y)^2\big((x-y)^4+y(x^3-y^3)\big)^2+2(x-y)^2x^2\big((x-y)^4+y(x^3-y^3)\big)^2+(x-y)^2(2y+x)^2(\quad)^2-4(x-y)(x^3-y^3)(\quad) \overset{?}{=} 0$$

i.e. $(x-y)^6 +$ des carrés $+ (x^3-y^3)A(x,y) = 0$.

Soit I un anneau intègre, K son corps de fractions, $G = K^*$ le groupe multiplicatif

ex : $I = \mathbb{Z}$, $K = \mathbb{Q}$, $G = \mathbb{Q}^*$. Quand a-t-on α divisible par β, i.e. $\alpha\beta^{-1} \in I$?

On a le théorème de décomposition en facteurs premiers. La valeur de α en p doit être au moins égale à la valeur de β.

Cela se généralise en valuations et anneaux de valuation :

B sous-anneau propre de K est de valuation si ses non inversibles forment un idéal tel que tout suranneau contient l'inverse d'un non inversible de B.

$I = \mathbb{Z}$. $B_p = \{ \frac{a}{b} : p \nmid b \}$

Krull : Si I est intégralement clos, il est l'intersection de ses anneaux de valuation

(un $a \in K$ tel que $a^n + a_1 a^{n-1} + \dots + a_n = 0$ avec $a_1, \dots, a_n \in I$ est dans I)

Dém : • les B sont intégralement clos : considérons le suranneau des élts int. dép. : s'il ne contenait l'inverse d'un non inversible a de B, on aurait $a^{-n} + a_1 a^{-n+1} + \dots + a_n = 0$ avec $a_1, \dots, a_n \in B$ et en multipliant par a^n,
$1 = -a(a_1 + \dots + a_n a^{n-1})$ ↯

• Si a n'est pas dans I intégralement clos, alors $a^{-1} \in I[a^{-1}]$, mais a^{-1} n'y est pas inversible : $a^{-1}(a_0 a^{-n} + a_1 a^{-n+1} + \dots + a_n) = 1$ donnerait une rel de dépendance intégrale pour a. Le lemme de Zorn donne un suranneau B maximal contenant $I[a^{-1}]$ mais pas a et on voit que c'est un anneau de valuation

---

Lorenzen 1950 propose la construction suivante. Nous nous demandons dans quelles circonstances $a \in B$ vaut pour tout suranneau de valuation B de I. Pour z arbitraires on a toujours $z \in B$ ou $z^{-1} \in B$. Donc, dès que $a \in I[z]$ ou $a \in I[z^{-1}]$, alors $a \in B$. Similairement, si on a $z_1, \dots, z_n$ tels que $a \in I[z_1^{\pm 1}, \dots, z_n^{\pm 1}]$ pour tous les 2^n choix de signe ± 1, alors $a \in B$ pour tout B.

Cette condition est aussi nécessaire. Sinon, Zorn, suranneau maximal $\bar{I}$ avec la propriété que pour tous $z_1, \dots, z_n$ on a $a \notin \bar{I}[z_1^{\pm 1}, \dots, z_n^{\pm 1}]$. En particulier $a \notin \bar{I}$.

Si $\bar{I}$ n'était pas un anneau de valuation on aurait z avec $z \notin \bar{I}$ et $z^{-1} \notin \bar{I}$.
Par maximalité, $a \in \bar{I}[z][x_1^{\pm 1}, \dots, x_m^{\pm 1}]$, $a \in \bar{I}[z^{-1}][y_1^{\pm 1}, \dots, y_n^{\pm 1}]$. Mais alors $a \in \bar{I}[z^{\pm 1}, x_1^{\pm 1}, \dots, y_n^{\pm 1}]$
Donc $\bar{I}$ est un anneau de valuation

Quelle est la signification de ces 2^n choix de signes : c'est en considérant $z_1 = \alpha_1\beta_1^{-1}, \dots, z_n = \alpha_n\beta_n^{-1}$, de faire comme si I était totalement ordonné.

$1 \in \langle a^{-1}, a^{-1}z, \dots, a^{-1}z^{p} \rangle_{I[a^{-1}]}$ $\qquad a \in I[z]$

$1 \in \langle a^{-1}, a^{-1}z^{-1}, \dots, a^{-1}z^{-p} \rangle_{I[a^{-1}]}$ $\qquad a \in I[z^{-1}]$

donne $z^k \in \langle a^{-1}z^{-n}, \dots, a^{-1}, \dots, a^{-1}z^{n} \rangle_{I[a^{-1}]}$ pour $k = -p \dots p$, et il y a une matrice à coefficients dans $a^{-1}I[a^{-1}]$ telle que $M \begin{bmatrix} z^{-k} \\ \vdots \\ z^{k} \end{bmatrix} = \begin{bmatrix} z^{-k} \\ \vdots \\ z^{k} \end{bmatrix}$, i.e. $(Id - M)\begin{bmatrix} z^{-n} \\ \vdots \\ z^{k} \end{bmatrix} = 0$

Le déterminant trick donne $1 \in a^{-1}I[a^{-1}]$, i.e. une relation de dépendance intégrale pour a.

$a^{-1}(a_0 a^{-n} + a_1 a^{-n+1} + \dots + a_n) = 1 \qquad a^{n+1} - a_n a^{n} - \dots - a_0 = 0.$