La non-nullité dans un anneau est-elle diophantienne?

Laurent Moret-Bailly

IRMAR, Université de Rennes 1

Séminaire de géométrie et théorie des modèles,
7 mars 2008

Summary

Conventions :

- Les anneaux sont commutatifs et unitaires.
- Pour les experts : si R est un anneau, on considérera la définissablilté sur R dans un langage $L(R)$ qui est le « langage des anneaux » $(+, \times, 0, 1)$, enrichi de:
  - une constante pour chaque élément de R
  - la constante logique FAUX.

Ensembles existentiellement définissables :

Si R est un anneau et $n \in \mathbb{N}$, alors :

- les sous-ensembles *algébriques élémentaires* de R^n sont définis par des systèmes finis d'équations polynômes, à coefficients dans R :

$$\{t \in R^n \mid F_1(t) = \cdots = F_r(t) = 0\}$$

- les sous-ensembles *algébriques* de R^n sont les réunions finies d'ensembles algébriques élémentaires ;
- les sous-ensembles *constructibles* sont les combinaisons booléennes finies d'ensembles algébriques (élémentaires) ;
- les sous-ensembles *existentiels positifs*, ou *diophantiens*, sont les projections de sous-ensembles algébriques d'un R^{n+p} ;
- les sous-ensembles *existentiels* sont les projections de sous-ensembles constructibles d'un R^{n+p}.

Remarques :

- on peut remplacer « projections » par « images par une application polynomiale » ;
- si R est intègre, tout ensemble algébrique est élémentaire ;

Remarques :

- les ensembles existentiels (positifs) sont les ensembles définissables par une formule existentielle (positive) dans le langage $L(R)$:

- la constante FAUX sert à assurer que l'ensemble vide est diophantien dans R^n lorsque R est l'anneau nul :

$$\emptyset = \{t \in R^n \mid \text{FAUX}\}; \quad \text{si } R \neq \{0\}, \quad \emptyset = \{t \in R^n \mid 1 = 0\}.$$

Exemples :

$E \subset R$	E **diophantien dans** R **?**	
$\mathbb{R}_+ \subset \mathbb{R}$	oui	carrés
$\mathbb{N} \subset \mathbb{Z}$	oui	sommes de 4 carrés
$\mathbb{Z} \subset \mathbb{R}$	non	infinité de composantes connexes
$\mathbb{R} \subset \mathbb{C}$	non	infini, à complémentaire infini
$\mathbb{Z} \subset \mathbb{Q}$	?	(conjecture de Mazur $\Rightarrow$ non)

« $\mathbb{Z}$ diophantien dans $\mathbb{Q}$ » impliquerait une réponse négative au dixième problème de Hilbert pour $\mathbb{Q}$.

« Existentiel » contre « diophantien »

Il est clair que « diophantien » implique « existentiel ».

La réciproque est vraie (pour R donné) si et seulement si R vérifie la

Condition (C) :

$R \setminus \{0\}$ est diophantien dans R.

Condition (C) :

$R \setminus \{0\}$ est diophantien dans R.

Problèmes :

trouver des classes utiles d'anneaux vérifiant (C) ;

trouver des classes utiles d'anneaux ne vérifiant pas (C).

Exemples d'anneaux vérifiant (C)

- les anneaux finis ;
- les corps : $(t \neq 0) \Leftrightarrow (\exists x)(tx = 1)$;
- $R_1 \times R_2$ vérifie (C) $\Leftrightarrow$ R_1 et R_2 vérifient (C) ;
- $\mathbb{Z}$ vérifie (C) : pour $t \in \mathbb{Z}$, on a

$$t \neq 0 \quad \Leftrightarrow \quad (\exists x)(\exists y) \ \ t^2 = (1+2x)(1+3y)$$

$$\Leftrightarrow \quad (\exists w)(\exists x)(\exists y) \ \ tw = (1+2x)(1+3y).$$

- La dernière formule montre aussi que tout anneau d'entiers algébriques vérifie (C).

Exemples d'anneaux ne vérifiant pas (C)

- $\mathbb{Z}_p$ (p premier)
  (tout ensemble diophantien est p-adiquement compact) ;
- plus généralement : les anneaux compacts infinis
  (exemples : $\mathbb{F}_p[[t]]$, $\mathbb{F}_p^{\mathbb{N}}$) ;
- les produits infinis d'anneaux non nuls
  (tout ensemble diophantien est fermé pour la topologie pro-discrète) ;
- $R\left[(X_i)_{i\in I}\right]$ (R anneau non nul, I infini).

Cas noethérien : résultats

Théorème 1

Soit R un anneau intègre noethérien.

Si R n'est pas local hensélien, il vérifie (C).

Corollaire

R intègre noethérien ; $S \subset R$ partie multiplicative

(1) *Si $S \not\subset R^\times$, alors $S^{-1}R$ vérifie (C).*

(2) *Si R vérifie (C), alors $S^{-1}R$ vérifie (C).*

Démonstration : (1) $S^{-1}R$ n'est jamais local hensélien.

(2) est conséquence de (1).

Cas noethérien : résultats

Que se passe-t-il dans le cas local hensélien ?

Théorème 2

Soit R un anneau local hensélien excellent, d'idéal maximal $\mathfrak{m}$.

Pour tout $n \in \mathbb{N}$, tout sous-ensemble diophantien de R^n est fermé pour la topologie $\mathfrak{m}$-adique.

En particulier, si $\dim R \geq 1$, R ne vérifie pas (C).

Remarque :

il existe un anneau de valuation discrète hensélien qui vérifie (C).

Anneaux noethériens non intègres

Proposition

Soit R un anneau noethérien.

On suppose que tout quotient intègre de R vérifie (C).

Alors R vérifie (C). Plus généralement, tout anneau de fractions $S^{-1}R$ vérifie (C).

(démonstration facile par dévissage)

Corollaire

Tout anneau artinien vérifie (C).

Corollaire

Tout anneau de fractions d'un anneau de Jacobson noethérien vérifie (C).

(Exemples : les algèbres de type fini sur un corps, ou sur $\mathbb{Z}$)

Un exemple non noethérien

Théorème 3

Soit X un espace $\mathbb{C}$-analytique de Stein, irréductible et réduit.

Alors l'anneau $\mathcal{H}(X)$ des fonctions holomorphes sur X vérifie (C).

Faits élémentaires :

- Si $I \subset R$ est un idéal de type fini et si R/I vérifie (C), alors $R \setminus I$ est diophantien dans R.

- (restriction de Weil) Si une R-algèbre finie libre non nulle vérifie (C), alors R vérifie (C).

Lemme (des deux idéaux)

Données : R noethérien intègre ; $\mathfrak{p}, \mathfrak{q} \in \operatorname{Spec} R$.

On suppose que :

- *$\mathfrak{p} \cap \mathfrak{q}$ ne contient aucun idéal premier non nul,*
- *$R/\mathfrak{p}$ et $R/\mathfrak{q}$ vérifient (C).*

Alors R vérifie (C).

Explicitement : pour $t \in R$, on a $t \neq 0$ si et seulement si

$$\exists x, y, z, \begin{cases} xy = zt \\ x \notin \mathfrak{p} \\ y \notin \mathfrak{q} \end{cases}$$

et les conditions $x \notin \mathfrak{p}$ et $y \notin \mathfrak{q}$ sont diophantiennes.

Corollaire

Soit A intègre noethérien vérifiant (C). Alors $A[X]$ vérifie (C).

Démonstration : appliquer le lemme des deux idéaux avec $\mathfrak{p} = (X)$ et $\mathfrak{q} = (X - 1)$.

Remarque : on peut supprimer l'hypothèse noethérienne du corollaire en raffinant le lemme des deux idéaux.

Le lemme des deux idéaux ne s'applique pas (par exemple) si R est local de dimension 1.

Dans ce cas, on peut (parfois) remplacer R par une R-algèbre finie libre qui n'est pas locale.

Exemple : $R = \mathbb{Z}_{(2)}$. L'anneau

$$S = R[X]/(X^2 + X + 2)$$

- est libre de rang 2 sur R ;
- a deux idéaux maximaux (de hauteur 1).

Le lemme des deux idéaux implique que S vérifie (C), donc R aussi par restriction de Weil.

Ceci ne marche pas pour $R = \mathbb{Z}_2$ (S n'est pas intègre).

Lemme (de dédoublement)

R intègre noethérien, $K = \mathrm{Frac}\,(R)$, $\mathfrak{p} \in \mathrm{Spec}(R)$ non nul.

On suppose que R n'est pas local d'idéal maximal $\mathfrak{p}$.

Alors il existe un polynôme

$$F = X^2 + aX + b \in R[X]$$

tel que $a \notin \mathfrak{p}$, $b \in \mathfrak{p}$, et F est irréductible dans $K[X]$.

En particulier, la R-algèbre $S := R[X]/(F)$ a les propriétés suivantes :

- *S est intègre ;*
- *S est libre de rang 2 comme R-module,*
- *S a deux idéaux premiers au-dessus de $\mathfrak{p}$, à quotients isomorphes à $R/\mathfrak{p}$ (puisque $F = X(X + a)$ modulo $\mathfrak{p}$).*

Le cas non local

En combinant le lemme des deux idéaux, le lemme de dédoublement et une récurrence sur la dimension, on obtient :

Proposition

Donnéees : R intègre noethérien, $\mathfrak{p} \in \mathrm{Spec}(R)$ non nul.

On suppose que R n'est pas local d'idéal maximal $\mathfrak{p}$.

Si $R/\mathfrak{p}$ vérifie (C), R aussi.

Corollaire

Tout anneau noethérien intègre non local vérifie (C).

Démonstration : appliquer la proposition à un idéal maximal de R.

Fin de la démonstration du théorème 1 : le cas non hensélien

Si R est local, noethérien et non hensélien, il existe une R-algèbre finie S intègre et non locale, donc vérifiant (C).

On écrit $S = L/\mathfrak{p}$, où L est finie libre sur R. (L n'est pas nécessairement intègre !)

$L/\mathfrak{p}$ vérifie (C), donc $L \setminus \mathfrak{p}$ est diophantien dans L, et aussi dans le R-module libre sous-jacent à L.

On peut supposer (quitte à changer S) que $\mathfrak{p}$ est minimal dans L. Comme L est plat sur R (et R intègre), on a alors $R \cap \mathfrak{p} = \{0\}$. Donc

$$R \cap (L \setminus \mathfrak{p}) = R \setminus \{0\}$$

est diophantien dans R, cqfd.

Le cas hensélien :

propriétés d'approximation

Soient R un anneau noethérien, I un idéal de R, $\widehat{R}$ le complété I-adique de R. On considère les propriétés suivantes :

(PA) (« propriété d'approximation »)

Pour tout R-schéma X affine de type fini, $X(R)$ est dense dans $X(\widehat{R})$.

(HI) (« principe de Hasse infinitésimal »)

Pour tout X affine de type fini sur R, si $X(R/I^q) \neq \emptyset$ pour tout $q \geq 0$, alors $X(R) \neq \emptyset$.

(PAF) (« propriété d'approximation forte »)

Pour tout X affine de type fini sur R et tout $q \in \mathbb{N}$, il existe $h \in \mathbb{N}$ tel que

$$\mathrm{Im}\left(X(R) \to X(R/I^q)\right) = \mathrm{Im}\left(X(R/I^{q+h}) \to X(R/I^q)\right).$$

- On a toujours (pour R et I donnés)
$$(\mathrm{PAF}) \Rightarrow (\mathrm{HI}) \Rightarrow (\mathrm{PA}).$$

- Les trois propriétés sont équivalentes si R est local d'idéal maximal I (Pfister-Popescu, Becker-Denef-Lipshitz-van den Dries).

- Elles sont vérifiées si R est local hensélien d'idéal maximal I et excellent (Greenberg, Artin, Popescu, Spivakovsky).

Lien entre (HI) et (C) :

Proposition

Soient R un anneau noethérien, I un idéal de R. Les conditions suivantes sont équivalentes :

1. *(R, I) vérifie (HI) ;*
2. *pour tout $n \in \mathbb{N}$, tout sous-ensemble diophantien de R^n est fermé pour la topologie I-adique.*

(Démonstration directe à partir des définitions).

Le théorème 2 en résulte :

Théorème

Soit R un anneau local hensélien excellent, d'idéal maximal $\mathfrak{m}$.

Pour tout $n \in \mathbb{N}$, tout sous-ensemble diophantien de R^n est fermé pour la topologie $\mathfrak{m}$-adique.

En particulier, si $\dim R \geq 1$, R ne vérifie pas (C).

Remarque :

les résultats précédents impliquent :

Proposition

Soient R un anneau noethérien, I un idéal de R non contenu dans un idéal premier minimal. Si (R, I) vérifie (HI) (et a fortiori s'il vérifie (PAF)), alors R est semi-local hensélien.

Par exemple $\big(\mathbb{Z}[[X]], (X)\big)$ ne vérifie pas (HI).

Remarque : Spivakovsky avait déjà donné des exemples de couples henséliens excellents ne vérifiant pas (HI), en réponse à une question de Popescu.