PUBLICATIONS MATHÉMATIQUES ET INFORMATIQUES DE RENNES

PIERRE SAMUEL

Anneaux euclidiens

Publications des séminaires de mathématiques et informatique de Rennes, 1972, fascicule 4
« Colloque d'algèbre commutative », , exp. n° 3, p. 1-4

<http://www.numdam.org/item?id=PSMIR_1972___4_A3_0>

ANNEAUX EUCLIDIENS

Pierre Samuel
UNIVERSITE de PARIS XI^{e} (ORSAY)

I - L'exposé qui suit est, dans sa plus grande partie, extrait de mon article "About euclidean rings" (J. of Algebra, I9 (I97I), 282-30I). On définit d'ordinaire un anneau euclidien comme un anneau intègre muni d'une application $\varphi : A \longrightarrow \underline{N}$ (un "algorithme" ou un "stathme") telle que :

I) $\varphi(ab) \geq \varphi(a)$ pour tous a, b dans A non nuls ;

2) Pour $a,b \in A$ et $b \neq 0$, il existe q et r dans A tels que $a = bq + r$ et $\varphi(x) < \varphi(b)$.

Il s'agit ainsi d'une notion sympathique, qui généralise des choses bien connues. Les anneaux euclidiens sont principaux, et l'euclidianité est une bonne hypothèse pour des réductions fines de matrices et dans certaines questions arithmétiques. Mais, au moins pour démontrer que tout idéal est principal, on a seulement besoin d'une application de A dans un ensemble <u>bien ordonné</u> W qui satisfasse à (2) ; une telle application sera appelée un <u>algorithme</u> sur l'anneau A, et A sera dit <u>euclidien</u> s'il admet un algorithme.

J'ignore si cette généralisation élargit vraiment la classe des anneaux euclidiens. Le remplacement de W par un ensemble ordonné satisfaisant à la condition minimale n'apporte par contre rien de plus.

II - Soit A un anneau euclidien pour un algorithme φ . Un changement d'algorithme permet de récupérer le propriété (I). On a les résultats suivants :

- Un anneau principal ayant un nombre fini d'idéaux premiers (en particulier un anneau de valuation discrète) est euclidien.
- Un produit fini d'anneaux euclidiens est euclidien.
- Un anneau de fractions d'un anneau euclidien est euclidien.
- Si A est euclidien, il en est de même de $A[[X]]\ [X^{-I}]$.

III - Un fait intéressant est que, si A est euclidien, il admet un plus petit algorithme (en fait la borne inférieure de tous les algorithmes sur A, après qu'on se soit arrangé pour qu'ils prennent leurs valeurs dans un même grand ensemble bien ordonné). Cela avait été remarqué par Th. Motzkin en I949. Sur un anneau A, le plus petit algorithme est obtenu par la construction transfinie suivante :

Soit W un ordinal tel que card(A) < card(W). On pose $A_o = (0)$. Pour $j > 0$ dans W, on définit A_j par induction transfinie : $A'_j = \bigcup_{i<j} A_i$ est déjà défini, et A_j est l'ensemble formé par 0 et par les éléments b tels que l'application canonique $A'_j \longrightarrow A/Ab$ soit surjective.
Ainsi A_I est formé par 0 et les unités. Pour A_2, on y ajoute les éléments b tels que chaque classe modulo Ab admette un représentant qui soit 0 ou une unité.

Si A est euclidien, son plus petit algorithme φ est donné par :

3) $$\varphi(x) = j \iff x \in A_j - A'_j.$$

Mais la construction transfinie peut être effectuée dans n'importe quel anneau (commutatif) A ; cet anneau A est euclidien, si et seulement si elle épuise A, c'est-à-dire si $A = \bigcup_j A_j$.

Sur $\underline{Z}$, le plus petit algorithme φ est donné par $\varphi(n)$ = nombre de chiffres dans le développement binaire de $|n|$. Sur $k[X]$ (k corps), c'est $\varphi(P) = I + d^\circ(P)$, donc l'algorithme ordinaire. Sur les classiques anneaux euclidiens $\underline{Z}[\sqrt{-I}]$ et $\underline{Z}[\sqrt{-2}]$. Le plus petit algorithme paraît fort irrégulier.

Lorsque les corps résiduels de l'anneau euclidien A sont finis, le plus petit algorithme sur A est à valeurs finies ; notre généralisation n'apporte donc pas de nouveaux anneaux euclidiens parmi les anneaux d'entiers de corps de nombres algébriques. Mais le problème général est tout vert.

Cependant, l'on a surtout recherché les corps de nombres K, dont

l'anneau A des entiers est euclidien "pour la norme" (c'est-à-dire tel que $x \longmapsto |N_{K/Q}(x)|$ soit un algorithme) ; ceux dont l'anneau est euclidien "tout court" sont mystérieux. Il n'y a cependant pas de mystère pour les corps quadratiques imaginaires $Q(\sqrt{d})$ ($d < 0$ sans facteur carré) : l'anneau est euclidien seulement pour d = -I, -2, -3, -7 et -II (sion la construction transfinie s'arrête au stade A_I), et l'on sait qu'il est alors euclidien pour la norme. Pour les corps quadratiques réels, des travaux culminant avec ceux de Davenport-Chatland ont donné la liste des I6 dont l'anneau est euclidien pour la norme :

d = 2, 3, 5, 6, 7, II, I3, I7, I9, 2I, 29, 33, 37, 4I, 57, 73 ;

mais il pourraît être euclidien "tout court" pour d'autres valeurs de d ; l'anneau $Z[\sqrt{I4}]$ est un bon candidat (principal, la construction transfinie attrape rapidement beaucoup d'éléments).

NB - Avec d = -I9, -43, -67, et -I63, on obtient des anneaux principaux qui ne sont euclidiens pour aucun algorithme.

IV - Les anneaux de courbes affines normales (= non singlières) sont intéressants eux aussi. On se place sur un corps k quelconque ; la courbe affine C est obtenue en enlevant d'une courbe normale projective $\overline{C}$ un nombre fini de points (ou "places" ou "valuations"), les "points à l'infini" ; soit d le PGCD des degrés des diviseurs sur $\overline{C}$ et d' le PGCD des degrés des diviseurs à l'infini. L'anneau de coordonnées $A = k[C]$ est un anneau de Dedekind, dont le groupe des classes d'idéaux se calcule sans malice au moyen de la théorie de la jacobienne.

Sur l'euclidianité de A, on a des résultats complets en genre g = 0. On a alors d = I ou 2 (à cause des diviseurs canoniques, qui sont de degré -2).

- Si d = I, on a l'équivalence de :

  i) d' = I

  ii) A est principal

  iii) A est euclidien "pour le degré" ($\varphi(x) = I + [A/Ax : k]$ pour $x \neq 0$).

- Si d = 2, A est principal si et seulement si d' = 2 ; mais il n'est jamais euclidien. De plus, lorsque d = d' = I et que k est un corps infini, le plus petit algorithme sur A est donné par $\varphi(x) = I + [A/Ax : k]$ $(x \neq 0)$.

La démonstration de ces faits utilise un résultat étrange, pas commode à démontrer (au moins pour moi !) et où on se sert du théorème de densité de Cebotarev :

Lemme. Soient K un corps infini, L un K-espace vectoriel de dimension finie, W un sous espace propre de L, et G un sous-groupe commutatif de type fini de Aut(L). Alors on a $G.W \neq L$.

L'hypothèse de commutativité de G paraît nécessaire, à cause de $SI(2,\underline{Z})$ opérant sur $\underline{Q}^2$. Il résulte du lemme que, si K est un corps infini et L une extension propre de K, laors le groupe L^*/K^* n'est jamais de type fini.

En genre g > I, il y a lieu de penser que les anneaux euclidiens sont exceptionnels. Si k est algébriquement clos, "A principal" implique "g = 0". Lorsque k est infini et que C n'a qu'un nombre fini de points rationnels, son anneau A n'est pas euclidien.
J.V. Armitage aurait montré qu'il n'y a pas d'anneaux $A = k[C]$ euclidiens "pour le degré" lorsque k est infini et que $g \geqslant I$. D'après R. Mac Rae, le cas où k est fini soulève des questions arithmétiques fines de densité.

En conclusion, la théorie des anneaux euclidiens est pleine de problèmes ouverts, qui ont une saveur assez différente de celle des questions habituellement traitées.