PUBLICATIONS MATHÉMATIQUES ET INFORMATIQUES DE RENNES

J. J. HIBLOT

Un type d'euclidienneté dans les anneaux factoriels, réduction d'euclidienneté

Publications des séminaires de mathématiques et informatique de Rennes, 1976, fascicule 4
« Colloque d'algèbre commutative », , exp. n° 4, p. 1-22

<http://www.numdam.org/item?id=PSMIR_1976___4_A2_0>

UN TYPE D'EUCLIDIENNETE DANS LES ANNEAUX FACTORIELS, REDUCTION D'EUCLIDIENNETE

(J.-J. HIBLOT)

I. INTRODUCTION - On a récemment montré dans [2], grâce à la notion de "division euclidienne le long d'une partie multiplicative saturée", qu'il existe des anneaux euclidiens factoriels sans algorithme à valeurs finies.

Rappelons la

DEFINITION 1: Soient A un anneau (comm. et unit.) et S une partie multiplicative saturée de A ne contenant pas zéro. On dit que A possède une division euclidienne le ϕ long de S s'il existe un ensemble ordonné W satisfaisant à la condition minimale et une application $\overset{\phi}{i}: S \to W$, appelée algorithme sur A le long de S, remplissant la condition

$$\forall a \in A, \forall \beta \in S, \text{ avec } a \notin \beta A, \exists\ q \in A, \quad \rho \in S$$

tels que l'on ait

$$a = \beta q + \rho, \text{ avec } \overset{\phi}{i}(\rho) \leq \overset{\phi}{i}(\beta).$$

On dit aussi que A est euclidien pour $\overset{\phi}{i}$ le long de S.

Pour montrer qu'un anneau de fractions convenablement choisi de $\mathbb{Z}[[X]]$ est euclidien, on utilise dans [2] le fait que si un anneau factoriel A est euclidien le long d'une partie multiplicative saturée engendrée par presque tous les éléments (tous sauf un nombre fini) d'un système

représentatif de ses éléments irréductibles, alors il est euclidien (le long de A-(0)).

Dans ce qui suit, on se propose tout d'abord (II) de mettre en relief une classe d'anneaux euclidiens factoriels déjà plus ou moins bien connue mais très insufisamment prospectée: les anneaux euclidiens pour le p.g.c.d.. Nous verrons ensuite (III) qu'à tout anneau factoriel A on peut associer un anneau $\mathcal{R}(A)$, qui est un anneau de fractions de A, tel que la principalité (resp. l'euclidienneté) de A se réduise à la principalité (resp. l'euclidienneté) de $\mathcal{R}(A)$. $\mathcal{R}(A)$ sera appelé le réduit d'euclidienneté de A.

II. DIVISION EUCLIDIENNE POUR LE P.G.C.D. LE LONG D'UNE PARTIE MULTIPLICATIVE SATUREE - Nous allons énoncer un certain nombre de propriétés, valables pour un anneau factoriel A et une partie multiplicative saturée S de A ne contenant pas zéro, et appartenant à des horizons plus ou moins sensiblement différents. Il sera ensuite relativement aisé de vérifier qu'elles sont équivalents .On profitera de ce résultat pour souligner une fois de plus qu'il peut être vraiment significatif de préciser pour quel type d'algorithme un anneau est euclidien.

Mais, avant tout, il nous faut établir quelques petites définitions et notations préliminaires.

DEFINITION 2: Soient A un anneau (comm. et unit.), S une partie multiplicative saturée de A ne contenant pas zéro, et W un ensemble bien ordonné. Nous dirons qu'une fonction $\overset{\circ}{i}: S \to W$ est proprement additive si

1°) $\overset{\circ}{i}(\alpha) = 0$ équivaut à $\alpha \notin A^*$

2°) $\forall \alpha, \beta \in S$, on a $\overset{\circ}{i}(\alpha.\beta) = \overset{\circ}{i}(\alpha) \oplus \overset{\circ}{i}(\beta)$

où $\oplus$ désigne la somme de Hessenberg (cf. [1]).

DEFINITION 3: Soient A un anneau (comm. unit.), S une partie multiplicative saturée de A ne contenant pas zéro, et W un ensemble bien ordonné. Nous dirons qu'une fonction $\overset{\circ}{i}: S \to W$ est proprement multiplicative si

1°) $0 \notin \overset{\circ}{i}(S)$

2°) $\overset{\circ}{i}(\alpha) = 1$ équivaut à $\alpha \in A^*$

3°) $\forall \alpha, \beta \in S$, on a $\overset{\circ}{i}(\alpha.\beta) = \overset{\circ}{i}(\alpha) \otimes \overset{\circ}{i}(\beta)$ où $\otimes$ désigne le produit de Hausdorff (cf. [1]).

DEFINITION 4: Soient A un anneau (comm. unit.), S une partie multiplicative saturée de A ne contenant pas zéro, W un ensemble ordonné satisfaisant à la condition minimale, et $\overset{\circ}{i}: S \to W$ une application. On dit que $\overset{\circ}{i}$ est un bon algorithme sur A le long de S si c'est un algorithme sur A le long de S vérifiant $\forall \alpha, \beta \in S$, $\overset{\circ}{i}(\alpha\beta) \geqslant \overset{\circ}{i}(\beta)$.

Il est clair, en utilisant d'abord ([3] VI Remarque 1), puis en rabonissant à la manière de ([6] Proposition 4), que l'euclidienneté le long de S équivaut à l'existence d'un bon algorithme (le long de S) linéairement valué.

NOTATION 1: Soient A un anneau factoriel et $x \in A$. Nous noterons $\mathcal{S}(x) = \{ y \in A-(0) \text{ avec } x \text{ et } y \text{ étrangers} \}$.

NOTATION 2: Soient A un anneau intègre et S une partie multiplicative saturée de A ne contenant pas zéro. Nous noterons $H(A,S) = \{ y+(1/x) \text{ avec } y \in A \text{ et } x \in S \}$.

Voici la liste annoncée des propriétés valables pour un anneau factoriel A et une partie multiplicative saturée S de A ne contenant pas zéro:

(i) A possède une division euclidienne le long de chacune des parties multiplicatives saturées S' contenues dans S.

(ii) A possède une division euclidienne le long de chacune des parties multiplicatives saturées S' contenues dans S et engendrées par un nombre fini d'éléments irréductibles.

(iii) Toute fonction proprement additive $\phi: S \to W$, à valeurs dans un ensemble bien ordonné W, est un algorithme sur A le long de S.

(iv) Toute fonction proprement multiplicative $\phi: S \to W$, à valeurs dans un ensemble bien ordonné W, est un algorithme

sur A le long de S.

(v) Tout idéal qui rencontre S est principal et $\forall \beta \in S$, l'application canonique $A^* \to (A/\beta A)^*$ est surjective.

(vi) Tout idéal qui rencontre S est principal et $\forall \beta \in S$, la partie multiplicative $A^* + \beta A$ est saturée.

(vii) $\forall \beta \in S$, on a $\delta(\beta) \subset A^* + \beta A$.

(viii) $\forall a \in A$, $\forall \beta \in S$, $\exists q \in A$, et $\delta \in S$ tels que $a = \beta q + \delta$ où δ est un p.g.d.d. de a et de β.

(ix) $\forall a \in A$, $\forall \beta \in S$, avec a et β étrangers, $\exists q \in A$, et $u \in A^*$ tels que $a = \beta q + u$.

(x) L'application canonique $\beta \mapsto \beta \cdot A$ définie sur S et à valeurs dans l'ensemble des idéaux principaux de A ordonné par l'opposé de l'inclusion est un algorithme sur A le long de S.

(xi) Il existe un ensemble ordonné W satisfaisant à la condition minimale et où toute paire admet une borne inférieure tel que A soit euclidien le long de S pour un bon algorithme $\overset{\circ}{1}: S \to W$ vérifiant la condition

(*) $\forall \alpha, \beta \in S$, $\forall q \in A$, si $\alpha + \beta q \in S$, alors $\overset{\circ}{1}(\alpha + \beta q) \leq \inf(\overset{\circ}{1}(\alpha), \overset{\circ}{1}(\beta))$.

(xii) $S^{-1}A \subset H(A,S)$.

(xiii) H(A,S) est un sous-anneau du corps des fractions de A.

(xiv) H(A,S) est un sous A-module de ce corps des fractions.

(xv) H(A,S) est un sous-groupe additif de ce corps des fractions de A.

(xvi) $\forall \beta \in S$, on a $\beta\, H(A,S) = H(A,S)$.

Les implications suivantes sont assez claires:

(i) $\rightarrow$ (ii); (ii) $\rightarrow$ (ix); (ix) $\rightarrow$ (vii); (vii) $\rightarrow$ (xii); (xii) $\rightarrow$ (xiii); (xiii) $\rightarrow$ (xiv); (xiv) $\rightarrow$ (xv); (xiv) $\rightarrow$ (xii); (xii) $\rightarrow$ (xvi); (xii) $\rightarrow$ (ix); (ix) $\rightarrow$ (viii); (viii) $\rightarrow$ (x); (x) $\rightarrow$ (xi); (x) $\rightarrow$ (viii); (viii) $\rightarrow$ (iii); (viii) $\rightarrow$ (iv); (iii) $\rightarrow$ (i); (iv) $\rightarrow$ (i); (v) $\rightarrow$ (vi); (vi) $\rightarrow$ (ix); (viii) $\rightarrow$ (ix); ((viii) et (ix)) $\rightarrow$ (v).

Dans la dernière implication, la principalité d'un idéal $\mathcal{J}$ rencontrant S s'obtient de façon classique en prenant dans $\mathcal{J} \cap S$ un élément de degré divisoriel minimum.

On vérifie que (xi) $\rightarrow$ (x) en remarquant que le bon algorithme $\overset{\circ}{i}$ se factorise à travers S/A^* en un isomorphisme $S/A^* \longrightarrow \overset{\circ}{I}(S)$, S/A^* étant muni de l'ordre induit par l'opposé de l'inclusion des idéaux principaux de A.

La démonstration des implications (xv) $\overset{?}{\rightarrow}$ (xiii) et (xvi) $\rightarrow$ (xii) nécessite des arguments qui seront développés dans III; aussi espérons-nous que le lecteur voudra bien se satisfaire provisoirement de l'équivalence des propriétés (i) - (xiv).

DEFINITION 5: Soient A un anneau factoriel et S une partie multiplicative saturée de A ne contenant pas zéro. Nous dirons que A est euclidien pour le p.g.c.d. le long de S si la propriété (viii) ci-dessus est vérifiée.

DEFINITION 6: Nous dirons qu'un anneau factoriel A est euclidien pour le p.g.c.d. s'il est euclidien pour le p.g.c.d. le long de A-(0).

Remarque 1: La propriété (v) n'est qu'une légère adaptation de ce qui est parfois appelé "second stable range condition" (cf. [5] pages 14 et 46).

Remarque 2: L'intérêt des propriétés (iii) et (iv) est lié, entre autres, au fait que tous les anneaux commutatifs actuellement connus pour être euclidiens le sont, sinon pour un algorithme proprement additif, du moins pour un algorithme proprement multiplicatif.Il semble pourtant, à ce propos, qu'il n'existe pas sur $\underline{Z}$ d'algorithme proprement additif. Cette conjecture vaut-elle aussi pour les cinq anneaux euclidiens d'entiers des corps quadratiques imaginaires?

On peut aussi se demander si tout anneau euclidien intègre possède un algorithme proprement multiplicatif. Dans la négative, existerait-il un anneau euclidien intègre sans algorithme proprement multiplicatif, mais possédant un algorithme "multiplicatif" à valeurs dans la partie positive d'un corps totalement ordonné?

Remarque 3: Si A est un anneau euclidien le long d'une des ses parties multiplicatives saturées S, S est clairement contenue dans la construction transfinie de A.

Si A est factoriel et euclidien pour le p.g.c.d. le long de S, tout $a \in S$ appartient au $d^\circ(a)$-ième cran non trivial de la construction transfinie de A, $d^\circ(a)$ désignant le degré du diviseur principal a A. C'est dire que le plus petit algorithme d'un anneau euclidien pour le p.g.c.d. est le degré divisoriel. Pour autant, si K est un corps algébriquement clos, et si X est transcendant sur K, l'anneau $A = K[X]$ est bien connu pour être euclidien pour le degré divisoriel (cf. [6]) mais, par unicité des restes, n'est clairement pas euclidien pour le p.g.c.d.. Nous verrons même que $\forall\, F(X) \in A-(0)$, $A[F(X)^{-1}]$ n'est pas euclidien pour le p.g.c.d..

EXEMPLE 1: Soient x et y deux éléments non nuls d'un anneau factoriel A. Si A est euclidien le long de $\delta(xy)$, il l'est aussi le long de $\delta(x)$ et de $\delta(y)$. Donc, d'après les propriétés (i) et (ii), puisque tout anneau est euclidien le long de ses unités, on voit qu'un anneau semilocal principal est euclidien pour le p.g.c.d..

Dans la propriété (xi), si $S = A-(0)$, la condition (*) équivaut à la condition (**): $\forall\, \alpha, \beta \in A-(0)$, si $\alpha+\beta \neq 0$, alors $\mathring{1}(\alpha+\beta) \leq \inf(\mathring{1}(\alpha), \mathring{1}(\beta))$. Ceci nous autorise à présenter la notion d'anneau euclidien pour le p.g.c.d. comme une généralisation de la notion d'anneau de valuation discrète.

EXEMPLE 2: Soient B un anneau principal et X une indéterminée sur B. Alors, l'anneau de fractions B(X) de B[X] obtenu en rendant inversibles les polynomes primitifs, est euclidien pour le p.g.c.d.; et si B est intègre, le groupe des idéaux fractionnaires de B est canoniquement isomorphe à celui de B(X) (cf. [3] V THEOREME 5). En intersectant B(X) avec un nombre fini d'anneaux de valuations discrètes essentielles de B[X], on obtient encore un anneau euclidien pour le p.g.c.d., comme il est facile de le vérifier.

Remarque 4: Bien qu'il semble que, par une localisation finie (i.e. en rendant inversibles des éléments irréductibles en nombre fini) de $\underline{Z}$, l'on puisse obtenir des anneaux euclidiens pour le p.g.c.d. le long d'une partie multiplicative saturée non triviale (e.g. $\underline{Z}[1/2]$ et $\underline{Z}[1/11]$ pouraient être euclidiens le long de la partie multiplicative saturée engendrée par 3), il est à observer que l'euclidienneté pour le p.g.c.d. (le long de tous les éléments non nuls) suppose une certaine abondance d'unités. Plus précisément:

Un anneau principal intègre A ne peut être euclidien pour le p.g.c.d. dans aucun des deux cas suivant:

(a) Le groupe abélien A^* est de type fini;

(b) A est une algèbre sur un corps K et le groupe quotient A^*/K^* est de type fini.

On peut le voir comme suit:

Dans le cas (a), si k est le plus petit cardinal d'un système générateur de A^*, et si $l > k$ est un entier, on peut toujours trouver l éléments irréductibles $p_1, p_2, \ldots, p_l \nmid A$ premiers entre eux deux à deux tels que les corps de restes A/p_jA $(1 \leqslant j \leqslant l)$ ne soient pas de charactéristique 2. Alors, chaque $(A/p_jA)^*$ contient un sous-groupe d'ordre 2 et, d'après le théorème chinois, $(A/p_1p_2\ldots p_lA)^*$ contient un sous-groupe isomorphe à $(\underline{Z}/2\underline{Z})^l$. Donc, la surjectivité de l'application canonique $A^* \to (A/p_1p_2\ldots p_lA)^*$ contredirait un fait bien connu sur le rang des sous-groupes d'un groupe libre de type fini.

Dans le cas (b), si $\mathrm{char}(K) \neq 2$, on se ramène au cas (a) en raisonnant modulo K^*. Si $\mathrm{char}(K) = 2$, si k est le plus petit cardinal d'un système générateur de A^*/K^*, et si $l > k$ est un entier, on prend l éléments irréductibles $p_1, p_2, \ldots, p_l \nmid A$ premiers entre eux deux à deux, et on remarque que les éléments $1+p_j$ $(1 \leqslant j \leqslant l)$ engendrent dans $(A/p_1^2p_2^2\ldots p_l^2A)^*/K^*$ (après réduction modulo K^*) un sous-groupe isomorphe à $(\underline{Z}/2\underline{Z})^l$. Même résultat!...

En d'autres termes, dans les cas (a) et (b), si k est le plus petit cardinal d'un système générateur de A^* (rep. de A^*/K^*), l'anneau factoriel A ne peut être euclidien pour le p.g.c.d. le long d'une partie multiplicative saturée engendrée par au moins k+1 éléments irréductibles.premiers entre eux deux à deux.

Le groupe des unités d'un sous-anneau d'un corps global euclidien pour le p.g.c.d. est donc de type infini. L'exemple 3 ci-après montre que, néanmoins, le groupe des idéaux fractionnaires d'un tel anneau peut, lui aussi, être de type infini.

NOTATION 3: Soient A un sous-anneau principal d'un corps global, $x \notin A-(0)$ et $y \notin A-(0)$ deux éléments étrangers. Nous noterons respectivement

$A_{(x+yA)}$ l'anneau de fractions de A obtenu en rendant inversibles tous les éléments irréductibles $p \notin A-(0)$ qui vérifient $p-x \notin yA$ et $\mathrm{card}(A/pA) > \mathrm{card}(A/xA)$

$A_{(\overline{x+yA})}$ l'anneau de fractions de A obtenu en rendant inversibles tous les éléments irréductibles de A qui sont congrus à x modulo yA.

EXEMPLE 3: Soient A un sous-anneau principal d'un corps global, $x \notin A-(0)$ et $y \notin A-(0)$ deux éléments étrangers, et $p_1, p_2, \ldots, p_r \notin A-(0)$ des éléments irréductibles de A étrangers à y tels que $(A/yA)^*$ soit engendré par les classes résiduelles modulo (y) de x, $p_1, p_2, \ldots, p_r$ et des éléments de A^*. On vérifie alors directement, en utilisant le théorème chinois, le théorème des progressions arithmétiques et quelques autres propriétés des corps globaux, que les anneaux $A_{(x+yA)}[1/y]$ et $A_{(x+yA)}[1/p_1p_2\ldots p_r]$ sont euclidiens pour le p.g.c.d., de même que leurs anneaux de fractions respectifs $A_{(\overline{x+yA})}[1/y]$ et $A_{(\overline{x+yA})}[1/p_1p_2\ldots p_r]$.

On remarquera que l'anneau $A_{(x+yA)}$ est euclidien pour

le p.g.c.d. le long de tous les éléments premiers à y, mais que $A_{(x+yA)}$ n'est pas euclidien pour le p.g.c.d. si $(A/yA)^*$ n'est pas engendré par les classes modulo (y) de x et des éléments de A^*.

Remarque 5: Si la fermeture intégrale d'un anneau semilocal principal intègre dans une extension finie de son corps des fractions est clairement toujours un anneau semi-local principal, la fermeture intégrale d'un anneau euclidien pour le p.g.c.d. dans une extension finie de son corps des fractions n'est pas, en général, un anneau euclidien pour le p.g.c.d.. La loi de réciprocité de Artin (cf. [4]) et les exemples 3 ci-dessus permettent de construire de nombreux contre-exemples. En particulier, on trouve que la fermeture intégrale dans $\mathbb{Q}[\sqrt{-5}]$ d'un sous-anneau euclidien pour le p.g.c.d. de $\mathbb{Q}$ peut être un anneau de Dedekind non principal, et que la fermeture intégrale dans $\mathbb{Q}[\sqrt{-19}]$ d'un sous-anneau euclidien pour le p.g.c.d. de $\mathbb{Q}$ peut être un anneau principal non euclidien pour le p.g.c.d..

Remarque 6: Soient B un anneau factoriel et X une indéterminée sur B. En adaptant les raisonnements de ([5] 5.), on peut voir que l'anneau $B[[X]][X^{-1}]$ n'est euclidien pour le p.g.c.d. le long d'aucune partie multiplicative saturée non triviale.

III. REDUCTION D'EUCLIDIENNETE - Il est bien connu (cf. [6] Proposition 7) qu'on ne diminue pas l'euclidienneté d'un anneau en passant à l'un quelconque de ses anneaux de fractions. Bien plus, de nombreux travaux, dans des domaines variés, mettent en relief le fait qu'un anneau non euclidien peut être rendu euclidien par une petite localisation appropriée . Nous nous proposons de montrer ici que certaines localisations sont, au contraire, assez neutres de ce point de vue, i.e. que certains anneaux de fractions d'un anneau donné ne sont peut être pas plus euclidiens que l'anneau lui-même.

NOTATION 4: Soient A un anneau intègre et S et T deux parties multiplicatives saturées de A ne contenant pas zéro. Nous noterons $T^{-1}S$ la partie multiplicative saturée de $T^{-1}A$ engendrée par S.

NOTATION 5: Soient A un anneau intègre, K son corps d'effractions, et S une partie multiplicative saturée de A ne contenant pas zéro. Nous noterons

$$\mathcal{R}(A,S) = \{ z \in K \text{ tels que } z+H(A,S) = H(A,S) \},$$

$$\mathcal{R}^*(A,S) = \{ z \in K^* \text{ tels que } zH(A,S) = H(A,S) \},$$

$$\Gamma(A,S) = A \cap \mathcal{R}^*(A,S).$$

THEOREME 1: Soient A un anneau factoriel et S une partie multiplicative saturée de A ne contenant pas zéro. Alors, si la condition

$(^{*}_{x}{}^{*})$ $\forall \beta \in A-(0)$, $\forall y \in A-(0)$, avec β et y premiers entre eux et $1/\beta \in \mathcal{R}(A,S)$, $\exists$ $s \in S$ tel que $y-s \in \beta A$.

est vérifiée, on a:

(i) $\mathcal{R}(A,S) = \Gamma(A,S)^{-1}A$;

(ii) $\mathcal{R}^{*}(A,S) = \mathcal{R}(A,S)^{*}$;

(iii) $\mathcal{R}(\mathcal{R}(A,S), \Gamma(A,S)^{-1}S) = \mathcal{R}(A,S)$;

(iv) La principalité de tous les idéaux de A qui rencontrent S équivaut à la principalité de tous les idéaux de $\mathcal{R}(A,S)$ qui rencontrent $\Gamma(A,S)^{-1}S$;

(v)? A est euclidien le long de S si et seulement si $\mathcal{R}(A,S)$ est euclidien le long de $\Gamma(A,S)^{-1}S$; plus précisément, tout algorithme sur A proprement additif (resp. proprement multiplicatif) le long de S provient d'un algorithme sur $\mathcal{R}(A,S)$ proprement additif (resp. proprement multiplicatif) le long de $\Gamma(A,S)^{-1}S$.

DEMONSTRATION: Parmi les conséquences immédiates des définitions, on remarque tout d'abord que l'on a

(a) $A \subset \mathcal{R}(A,S)$ et $A^{*} \subset \mathcal{R}^{*}(A,S) \subset \mathcal{R}(A,S) \subset H(A,S)$,

(b) $\forall z \in \mathcal{R}(A,S$ et $\forall z' \in \mathcal{R}^{*}(A,S)$, on a $z'z \in \mathcal{R}(A,S)$.

En utilisant de plus la factorialité de A, on vérifie encore directement que l'on a

(c) Soit a/β une fraction irréductible. Alors $a/\beta \in \mathcal{R}(A,S)$ si et seulement si $\forall x \in S$, $ax+\beta$ est congru modulo (βx) à $(\beta,x)((\beta,x),(ax+\beta)/(\beta,x))$ où (y,y') désigne un p.g.c.d. de y et y'.

(d) Soit α/β une fraction irréductible. Alors, $\alpha/\beta \in \mathcal{R}^*(A,S)$ si et seulement si $\forall\, x \in S$ et $\forall\, w \in 1+xA$

1°) αw est congru modulo (βx) à $(\alpha,x)(\beta,w)$,

2°) βw est congru modulo (αx) à $(\beta,x)(\alpha,w)$.

Soit $a/\beta \in \mathcal{R}(A,S)$ une fraction irréductible. D'après (c) puis (a), on a $1/\beta \in \mathcal{R}(A,S)$. D'après (c), on a maintenant $\forall\, s \in S$ avec s et β premiers entre eux, $s/\beta \in \mathcal{R}((A,S)$. Et, d'après $(^*_*{}^*)$ et (a), $\forall\, y \in A-(0)$ avec y et β étrangers, la fraction irréductible y/β appartient à $\mathcal{R}(A,S)$.

Soient $\beta, \beta' \in A-(0)$ étrangers avec $1/\beta\beta' \in \mathcal{R}(A,S)$. Puisque $\beta'^2 \in S$ (d'après (a)), on peut calculer $\beta'^2 x + \beta\beta'$ modulo $(\beta\beta' x)$ pour tout $x \in S$ à l'aide de (c) et simplifier la congruence par β' pour obtenir que $\beta'/\beta \in \mathcal{R}(A,S)$ et donc que $1/\beta \in \mathcal{R}(A,S)$.

Soient $\pi \in A-(0)$ un élément irréductible et $k \in \underline{N}$ un entier $\geqslant 2$ tels que $1/\pi^k \in \mathcal{R}(A,S)$. Par (c), et par simplification par π^{k-1}, on peut voir directement que $1/\pi$ (ou $x+\pi$) vérifie la congruence de (c) $\forall\, x \in S$ sauf dans le cas où les ordres en (π) de x et de $x+\pi$ sont respectivement égal à 1 et supérieur ou égal à 2. Ce dernier cas se résout également: en simplifiant par π^2, il équivaut à demander que $\forall\, y \in A$ avec $\pi.y-1 \in S$, $\exists\, u \in A^*$ tel que $y-u \in (\pi y-1)A$; or, on sait déjà calculer $(\pi y-1)+\pi$ ...

En d'autres termes:

(e) Soit $a/\beta \in \mathcal{R}(A,S)$ une fraction irréductible. Alors, $\forall\, y \in A$, on a $y/\beta \in \mathcal{R}(A,S)$.

Soient $\beta \in S$ et $x \in S$ avec $1/\beta \in \mathcal{R}(A,S)$. Puisque $(\beta,x)/\beta \in \mathcal{R}(A,S)$, (c) nous dit que β est congru à (β,x) modulo (x). Soit de plus $w = xy+1 \in 1+xA$. En calculant $w/(\beta,y)$ modulo $(\beta^2 x/(\beta,y))$ toujours au moyen de (c) (ce qui peut se faire d'après (e)), et en simplifiant la congruence par $\beta/(\beta,y)$, on trouve que w est congru modulo (βx) à (β,w).

Autrement dit, nous venons, d'après (d), de montrer l'inclusion $\mathcal{R}(A,S) \subseteq \mathcal{R}(A,S)^{-1}A$.

Comme l'inclusion inverse résulte immédiatement de (a) et (b), le (i) est prouvé.

L'inclusion $\mathcal{R}^*(A,S) \subseteq \mathcal{R}(A,S)^*$ est triviale et l'inclusion inverse se déduit immédiatement de (i) et du fait expliqué plus haut que, si $1/\beta\beta' \in \mathcal{R}(A,S)$, alors, $1/\beta \in \mathcal{R}(A,S)$. Ce qui prouve (ii).

(iii) provient automatiquement du fait directement vérifiable que $H(\mathcal{R}(A,S), \Gamma(A,S)^{-1}S) = H(A,S)$.

La principalité de tous les idéaux de A (resp. $\mathcal{R}(A,S)$) qui rencontrent S (resp. $\Gamma(A,S)^{-1}S$) équivaut (disons par factorialité) à la principalité de tous les idéaux premiers de A (resp. $\mathcal{R}(A,S)$) qui rencontrent S (resp. $\Gamma(A,S)^{-1}S$). Puisque A est (évidemment) euclidien pour le p.g.c.d. le long de $\Gamma(A,S)$, d'après (II Remarque 3) et

([3] IV), l'assertion (iv) vient simplement du fait que l'on n'a rendu inversibles que des éléments de la construction transfinie de A.

Considérons une équation

(1) $a\alpha - r(\gamma/\delta) = b\beta q(\varphi/\eta)$

où $b \notin S$, $a \notin A-bA$, $r \notin S$ et $q \notin A$ sont étrangers à tous les éléments de $\Gamma(A,S)$,

$\alpha, \beta, \gamma, \delta, \varphi, \eta \notin \Gamma(A,S)$ et les fractions γ/δ et φ/η sont irréductibles.

Puisque $\gamma/\delta \notin \mathcal{R}^*(A,S)$, on peut supposer, après avoir utilisé (d) et (c), que γ et δ divisent β. En particulier, $d^\circ(\gamma)+d^\circ(\delta) \leqslant d^\circ(\beta)$. On peut même voir que, si $\gamma \notin A^*$, δ et β/γ ne sont pas premiers entre eux; et donc, dans ce cas, $d^\circ(\gamma)+d^\circ(\delta) < d^\circ(\beta)$. Ce résultat ne suffit pas à prouver cette assertion (v) que l'auteur croyait tout d'abord avoir démontré. Mais il semble que ce puisse être assez pour maintenir cette assertion au moins comme une conjecture. Si un contrexemple existe, il faudra sans doute le chercher assez loin, et il ne sera sans doute pas inintéressant.

DEFINITION 6: Soient A un anneau factoriel et S une partie multiplicative saturée de A ne contenant pas zéro et vérifiant $(**)$. Nous appelerons $\mathcal{R}(A) = \mathcal{R}(A,A-(0))$ (resp. $\mathcal{R}(A,S)$) le réduit d'euclidienneté de A (resp. de A le long de S), et $\Gamma(A) = \Gamma(A,A-(0))$ (resp. $\Gamma(A,S)$) le centre de réduction de A (resp. de A le long de S).

DEMONSTRATION DE (xv) $\overset{?}{\rightarrow}$ (xiii) ET (xvi) $\rightarrow$ (xii) (cf. II):

Remarquons tout d'abord que, si un anneau factoriel A est euclidien pour le p.g.c.d. le long d'une partie multiplicative saturée S ne contenant pas zéro, la condition $(^{*}_{*}{}^{*})$ est vérifiée. Réciproquement, si $(^{*}_{*}{}^{*})$ est vérifiée pour une partie multiplicative saturée S d'un anneau factoriel A, et si H(A,S) est un sous-groupe additif du corps d'effractions de A, alors, d'après le Théorème 1, $H(A,S) = \mathcal{R}(A,S)$ est un anneau, et A est euclidien pour le p.g.c.d. le long de S. Par contre, si $(^{*}_{*}{}^{*})$ n'est pas vérifiée, H(A,S) peut très bien être un sous-groupe additif du corps d'effractions de A sans être un anneau. A titre de contrexemple, il suffit de prendre un anneau factoriel B qui soit euclidien pour le p.g.c.d. le long d'une partie multiplicative saturée non triviale S ne contenant pas zéro, et une indéterminée X sur B. Alors, S est encore saturée dans l'anneau factoriel $A = B[X]$, et, d'après ([3] IV), A n'est sûrement pas euclidien le long de S, bien que $H(A,S) = A+S^{-1}B$ soit un sous-groupe additif du corps des fractions de A.

Indépendamment de la condition $(^{*}_{*}{}^{*})$, l'implication (xvi) $\rightarrow$ (xii) de II se déduit directement des remarques (a) et (b) de la démonstration du Théorème 1.

Remarque 7: Soit A un anneau factoriel. Alors, l'ensemble non vide $\Sigma(A)$ des parties multiplicatives saturées de A le long desquelles A est euclidien pour le p.g.c.d.

est, pour la relation d'inclusion, un ensemble ordonné qui vérifie les hypothèses du lemme de Zorn et, $\forall\, S \in \Sigma(A)$, on a $\Gamma(A)S \in \Sigma(A)$ (d'après (d) de la démonstration du Théorème 1). Ce qui veut dire que $\Gamma(A)$ est contenu dans l'intersection $\Delta(A)$ de tous les éléments maximaux de $\Sigma(A)$. Cette inclusion n'est généralement pas une égalité, comme le montre l'exemple suivant:

EXEMPLE 4: Soient A un sous-anneau principal d'un corps global, $y \in A-(0)$ et $x \in 1+yA$. Alors, si $y \notin A^*$ et qu'aucun facteur irréductible de y n'appartient au premier cran non trivial de la construction transfinie de A, on a

$\mathcal{R}(A_{(x+yA)}) = A_{(\overline{x+yA})} = A_{(1+yA)}$,

$\mathcal{R}(A_{(x+yA)})$ = la partie multiplicative saturée de $A_{(x+yA)}$ engendrée par les éléments irréductibles $p \in 1+yA$ tels que $\mathrm{card}(A/pA) \leqslant \mathrm{card}(A/xA)$,

$\Gamma(A_{(x+yA)}) = \mathcal{S}(y)$.

Remarque 8: Soient A un anneau factoriel, S une partie multiplicative saturée de A ne contenant pas zéro vérifiant $(**)$, et T une autre partie multiplicative saturée de A. Alors, $T^{-1}S$ vérifie $(**)$ dans $T^{-1}A$ et

$$T^{-1}\mathcal{R}(A,S) \subseteq \mathcal{R}(T^{-1}A, T^{-1}S).$$

L'exemple 4 ci-dessus et l'exemple 3 du II permettent de se rendre compte que cette inclusion n'est généralement pas une égalité.

EXEMPLE 5: Soit A un anneau semilocal factoriel avec un idéal maximal $\mathfrak{M}$ de hauteur > 1 et r idéaux maximaux de hauteur 1 Ap_1, Ap_2, ..., Ap_r $(r > 1)$. Alors, la remarque (c) de la démonstration du Théorème 1 permet de vérifier directement (mais pas nécessairement immédiatement) que $1/p_1p_2\ldots p_r \notin \mathcal{R}(A)$. i.e. $\mathcal{R}(A) = A[1/p_1p_2\ldots p_r] = A_{\mathfrak{M}}$.

Si A est régulier de dimension 2, et si $t \notin \mathfrak{M} - \mathfrak{M}^2$, on peut remarquer que $A[1/t]$ et $\mathcal{R}(A)[1/t] = \mathcal{R}(A[1/t])$ sont euclidiens le long de toutes les parties $\mathcal{S}(y)$, où $y \notin A$.

Remarque 9: Si un anneau intègre A est euclidien pour une fonction ψ_x (cf. [5] p. 43-44), alors A ne peut être euclidien pour le p.g.c.d. que le long de ses unités ou peut-être le long de la partie multiplicative saturée engendrée par x, et $\mathcal{R}(A) = A$.

IV. CONCLUSION - Le but essentiel de cet exposé était de suggérer la possibilité, pour la notion de division euclidienne le long d'une partie multiplicative saturée, de permettre une analyse plus rafinée de l'euclidienneté. L'auteur, qui n'est qu'un mathématicien en herbe à qui l'on a fait trop d'honneur en le laissant parler devant des mathématiciens confirmés, s'excuse de la trivialité de son exposé qui ne comporte qu'un théorème, et d'avoir cédé à la facilité de donner des conjectures, parfois, plutôt que des résultats solides. Et, comme pour aggraver

son cas, il se propose de terminer avec quelques dernières questions et conjectures:

Se peut-il que pour un anneau d'entiers algébriques A et un élément $x \in A-(0)$ l'on ait $\mathfrak{R}(A[1/x]) \neq A[1/x]$?

On peut formuler la même question pour les anneaux de fonctions algébriques à une variable sur un corps fini; mais, comme dans ce cas, l'euclidienneté pour le p.g.c.d. le long d'une partie multiplicative saturée non triviale semble à l'auteur plus dificile à obtenir, celui-ci propose de conjecturer que les localisés finis principaux d'anneaux de fonctions algébriques à une variable sur un corps fini soient tous réduits.

BIBLIOGRAPHIE

[1] P. W. Carruth, Arithmetic of ordinals with application to the theory of ordered abelian groups, Bull. Amer. Math. Soc. 48 (1942), 262-271.

[2] J. J. Hiblot, Des anneaux euclidiens dont le plus petit algorithme n'est pas à valeurs finies, C. R. Acad. Sc. Paris t 281 (22 septembre 1975), 411-414.

[3] J. J. Hiblot, Sur les anneaux euclidiens, Bull. Soc. Math. de France, Tome 104 - 1976, N°1.

[4] S. Lang, Algebraic number theory, Reading, Massachusetts, 1970.

[5] H. W. Lenstra Jr., Lectures on euclidean rings, Seminary Bielefeld summer 1974.

[6] P. Samuel, About euclidean rings, J. of Algebra 19 (1971), 282-301.