BULLETIN DE LA S. M. F.

JEAN-JACQUES HIBLOT

Sur les anneaux euclidiens

Bulletin de la S. M. F., tome 104 (1976), p. 33-50

<http://www.numdam.org/item?id=BSMF_1976__104__33_0>

Bull. Soc. math. France,
104, 1976, p. 33-50.

SUR LES ANNEAUX EUCLIDIENS

PAR

JEAN-JACQUES HIBLOT

[Université de Paris-Sud, Orsay]

RÉSUMÉ. — Cet article contient des résultats variés sur les anneaux commutatifs euclidiens, intègres ou non. Le lecteur y trouvera entre autres :

— Le fait que, si A est intègre, si A/At est euclidien et si les idéaux principaux de A sont fermés pour la topologie t-adique, alors $A[t^{-1}]$ est euclidien;

— La détermination de ceux des localisés $A[t^{-1}]$ qui sont euclidiens, où A est local régulier de dimension 2 et t irréductible dans A;

— Un théorème sur l'existence d'éléments non nuls de la construction transfinie d'un anneau dans l'un de ses idéaux premiers et dans l'annulateur de celui-ci;

— Une définition abstraite de l'euclidienneté.

I. Un gentil théorème

THÉORÈME 1. — *Soient A un anneau factoriel, et t un élément de A tels que :*

(i) $At \neq A$,

(ii) *A/At est euclidien,*

(iii) *les idéaux principaux sont fermés, pour une topologie moins fine que la topologie t-adique.*

Alors $A[1/t]$ est euclidien.

Démonstration. — Puisque A est factoriel, tout élément $a \neq 0$ de A_t s'écrit d'une manière unique :

$$a = a' t^i \quad \text{avec } i \in \mathbf{Z} \qquad \text{et} \qquad a' \in A - At. \tag{1}$$

Soient φ un algorithme sur A/At, et $s\colon A \to A/At$ la surjection canonique Posons

$$\Phi(a) = \varphi \circ s(a') \quad \text{pour } 0 \neq a \in A_t \qquad \text{et} \qquad \Phi(0) = \varphi \circ s(0).$$

Alors Φ est un algorithme sur A_t $(= A[1/t])$.

En effet, soient a, $b \in A_t$, $b \neq 0$. Montrons que l'on peut écrire

$$a = bq + r \quad \text{avec } q, r \in A_t \qquad \text{et} \qquad \Phi(r) < \Phi(b).$$

Nous remarquons tout de suite qu'il suffit de le démontrer en supposant $a = a'$ ($a \neq 0$) et $b = b'$ (conformément à (1)).

Si $a = 0$ ou si $a \neq 0$ et $a' \in A\,b'$, il n'y a pas de problème.

Si $a \neq 0$ et si $a' \notin A\,b' + A\,t$, puisque $A/A\,t$ est euclidien, pour φ, on a bien

$$a' = b'\,q + r' \qquad \text{avec} \quad q \in A \subset A_t, \quad r' \in A - A\,t$$

et

$$\Phi(r') = \varphi \circ s(r') < \varphi \circ s(b') = \Phi(b').$$

Il nous reste alors à étudier le cas où $a \neq 0$, $a' \notin A\,b'$ et $a' \in A\,b' + A\,t$.

Considérons les équations de la forme

$$a' - t^i r \in A\,b' \quad (r \in A,\ i \in \mathbf{N}).$$

Puisque l'idéal $A\,b'$ est fermé pour la topologie t-adique et que $a' \notin A\,b'$, dans toutes ces équations, l'exposant i est borné.

Soit i_0 le maximum de ces exposants. Prenons une équation $a' - t^{i_0} r_0 \in Ab'$. Dans cette équation, on a certainement $r_0 \in A - (A\,b' + A\,t)$, et si $\varphi \circ s\,(r_0) < \varphi \circ s\,(b')$, nous serons quittes en posant $r = t^{i_0} r_0$.

Finalement, si $\varphi \circ s\,(r_0) \geqslant \varphi \circ s\,(b')$, puisque, comme nous venons de le remarquer, la maximalité de i_0 veut que $r_0 \notin A\,b' + A\,t$, on peut encore écrire

$$r = b'\,q_1 + r_1' \qquad \text{avec} \quad \begin{cases} q_1 \in A \subset A_t, \\ r_1' \in A - A\,t \\ \varphi \circ s(r_1) < \varphi \circ s(b'), \end{cases}$$

ce qui permet de mettre fin à la démonstration en posant $r = t^{i_0} r_1$.

C. Q. F. D.

COROLLAIRE. — *Soient A un anneau local régulier de dimension 2, et $\mathcal{M}$ son idéal maximal. Alors, si t est un élément quelconque de $\mathcal{M} - \mathcal{M}^2$, le localisé $A\,[1/t]$ est un anneau euclidien.*

Démonstration. — C'est bien clair d'après le lemme de Nakayama et le fait que, dans ces conditions, A/At est un anneau de valuation discrète [2] (chapitre 7, § 17, théorème 36, p. 121), donc un anneau euclidien.

Exemple 1. — Soient B un anneau de valuation discrète, b une uniformisante de B, $A = B[[X]]$, où X est une indéterminée. Alors, tout élément non nul de $A[1/b]$ est associé à un élément bien déterminé de l'anneau local régulier A de dimension 2, élément qui est une série formelle à coefficients dans B, dont un coefficient au moins est inversible.

Un algorithme sur $A[1/b]$ est donc donné par l'ordre réduit de cette série formelle.

Exemple 2. — Soient A_0 un anneau euclidien intègre, et $A = A_0[[X]]$, où X est une indéterminée. Puisque A_0 est principal, A est un anneau factoriel de dimension 2 ([1], théorème 72, p. 49), et il n'est pas difficile de voir que ses idéaux principaux sont fermés pour la topologie X-adique.

La construction d'un algorithme sur $A[X^{-1}]$, l'anneau des séries de Laurent à coefficients dans A_0 est donnée, de façon similaire, dans la démonstration de notre « *gentil théorème* » et dans [4] (proposition 8).

Remarque 1. — D'une part, si A est un anneau local noethérien, possédant un élément t dans son idéal maximal, tel que A/At soit euclidien intègre, donc un anneau de valuation discrète, on aura dim $A \leqslant 2$.

D'autre part, si A est un anneau local factoriel de dim = 2, d'idéal maximal $\mathcal{M}$, et si $\mathcal{M}$ contient un élément t tel que A/At soit euclidien, $\mathcal{M}$ sera engendré par deux éléments, A sera régulier, et l'on aura $t \in \mathcal{M} - \mathcal{M}^2$. En sorte que, du moins pour un géomètre-algébriste, notre théorème ne vaut guère plus que son corollaire.

Remarque 2. — L'algorithme de l'exemple 1 et, plus généralement, l'algorithme obtenu dans le corollaire, avec la construction du théorème, et en prenant pour φ la valuation discrète normalisée de A/At, est l'algorithme minimal (ou plus petit algorithme).

En effet, appelons θ le plus petit algorithme sur $A[1/t]$, (on a $(0) = \Phi(0) = -1$, $\theta(A[1/t]^*) = \Phi(A[1/t]^*) = 0$), et supposons $\Phi \neq \theta$. Soit alors n le plus petit entier naturel pour lequel il existe un $b \in A[1/t]$ tel que $\Phi(b) > \theta(b)$. On a $n \geqslant 1$, et comme θ et Φ sont de « *bons algorithmes* » ([1]), on a

$$\theta(b') = \theta(b) \qquad \text{et} \qquad \Phi(b') = \Phi(b)$$

([1]) « *Un bon algorithme* », sur un anneau A, est un algorithme qui vérifie $\Phi(x, y) \geqslant \Phi(x)$, $\forall\, x, y \in A$. En particulier (x et x' sont associés) $\Rightarrow$ ($\Phi(x) = \Phi(x')$).

(toujours avec les définitions et notations du théorème). Donc, nous nous retrouvons avec un $b' \in A$, b' premier à t, et $\Phi(b') > \theta(b')$.

Soit alors $a' \in A$, a' premier à t tel que $\Phi(a') = \theta(a') = \theta(b')$ (comme il en existe indubitablement). Puisque θ est un algorithme, on doit pouvoir écrire

$$a' = b'q + r \qquad \text{avec } q \text{ et } r \text{ dans } A\left[1/t\right]$$

et

$$\theta(r) = \Phi(r) < \theta(b') = \Phi(a').$$

En revenant dans A, c'est-à-dire en remplaçant, comme nous l'avons fait maintes fois, r par son associé r' premier à t, le lecteur verra aisément que l'on devrait avoir $r' \in At + Aa' + Ab'$, ce qui soulève une contradiction.

II. Un théorème restreignant

THÉORÈME 2. — *Soient A un anneau local noethérien, factoriel, et $\mathcal{M}$ son idéal maximal. Supposons qu'il existe dans $\mathcal{M}$ un élément irréductible $t \neq 0$ tel que $A\left[1/t\right]$ soit un anneau euclidien. Alors A est un anneau local régulier de dimension au plus 2, et l'on a*

$$t \in \mathcal{M} - \mathcal{M}^2.$$

Démonstration. — Le lecteur, pourvu qu'il soit un peu familiarisé avec les anneaux noethérien locaux et les anneaux réguliers locaux, comprendra qu'il nous suffit de trouver un élément $b \in \mathcal{M}$ tel que

$$At + Ab = \mathcal{M}.$$

Tout revient donc à démontrer le lemme suivant :

LEMME. — *Soient A un anneau noethérien local, $\mathcal{M}$ son idéal maximal, et $t \in \mathcal{M}$ un élément régulier tel que At soit un idéal premier.*

Supposons que A_t, le localisé de A par rapport aux puissances de t, soit un anneau euclidien, ou, plus généralement, supposons que A_t est, soit un corps, soit un anneau dont la construction transfinie n'est pas triviale, c'est-à-dire ne s'arrête pas aux unites [4]. *Alors*

$$\{\exists b \in \mathcal{M};\ At + Ab = \mathcal{M}\}, \qquad \textit{et par suite} \quad \dim A \leqslant 2.$$

Démonstration. — Faisons les deux remarques préliminaires suivantes :

(*a*) Puisque t est régulier, nous pouvons identifier A à un sous-anneau de A_t au moyen de l'homomorphisme canonique injectif $A \to A_t$.

(*b*) Puisque A est noethérien et que t est régulier, tout élément $z \in A - \{0\}$ s'écrit d'une manière unique :

$$z = t^i y \qquad \text{avec} \quad \begin{cases} i \in \mathbf{N}, \\ y \in A - At. \end{cases}$$

Autrement dit, la fonction $z \mapsto \operatorname{ord} z$ est bien définie sur A et ceci indépendamment du fait que A est local. Mieux, tout élément $z \in A_t$ s'écrit d'une manière unique :

$$z = t^i\, y \qquad \text{avec} \quad \begin{cases} i \in \mathbf{Z}, \\ y \in A - At \end{cases}$$

et, en particulier, puisque, de plus, At est un idéal premier, tout élément $v \in (A_t)^*$ s'écrit d'une manière unique :

$$v = t^j u \qquad \text{avec} \quad \begin{cases} j \in \mathbf{Z}, \\ u \in A - At. \end{cases}$$

Dire que A_t est un corps, c'est dire que A est un G-anneau ou anneau de Goldman (dans la terminologie de [1]), et l'idéal premier At doit être le seul idéal premier de hauteur 1 de cet anneau noethérien intègre A qui, en définitive, ne peut être qu'un anneau de valuation discrète. Dans ce cas, donc, en prenant $b = 0$, on obtient le résultat.

Si la construction transfinie de A_t n'est pas triviale (on a $(A_t)_{-1} = \{0\}$, $(A_t)_0 = (A_t)^*$, $(A_t)_1 \neq \emptyset$), prenons $b \in (A_t)_1$. Alors, par la définition de $(A_t)_1$, tout élément non nul de $A_t/b\,A_t$ est image, par l'homomorphisme canonique $A_t \to A_t/b\,A_t$ d'une unité de A_t.

Comme l'on peut clairement supposer que $b \in A - At$, donc, en fait, $b \in \mathcal{M} - At$, on voit, en particulier, et compte tenu des remarques préliminaires, que l'on a

$$(2) \qquad \forall\, a \in \mathcal{M} - At, \quad \begin{cases} \exists\, x \in A - At, \\ \exists\, u \in A^* \cup \{0\}, \\ \exists\, i, j \in Z, \end{cases} \qquad \text{tels que} \quad a = bxt^i + ut^j.$$

Dans cette égalité, on remarque que

– $bx \in \mathcal{M} - A\,t$ (puisque $A\,t$ est un idéal premier),

– $(i \geqslant 0) \Leftrightarrow (j \geqslant 0$, si $u \neq 0)$,

– $(u = 0) \Rightarrow (i \geqslant 0)$.

Il reste à considérer le cas où $u \neq 0$, $i < 0, j < 0$.

En multipliant les deux membres de (2) par $t^{-\inf(i,j)}$, et en comparant i et j, on voit qu'il y a contradiction, soit avec le fait que A est local, soit avec le fait que $bx \notin A\,t$.

La formule désirée, $A\,t + A\,b = \mathcal{M}$, résulte immédiatement de toutes ces considérations.

La conjonction du « *gentil théorème* » et de ce « *théorème restreignant* » nous permet de tirer la conclusion, provisoire mais assez avancée, suivante :

CONCLUSION. – *Soient A un anneau local régulier de dimension 2, $\mathcal{M}$ son idéal maximal, et $t \in \mathcal{M}$ un élément extrémal, alors :*

$$(A[1/t] \text{ est euclidien}) \Leftrightarrow (t \in \mathcal{M} - \mathcal{M}^2).$$

De plus, si $t \in \mathcal{M}^2$, la construction transfinie est triviale.

Exemple à titre de remarque. – Prenons $A = \mathbf{R}[[X, Y]]$ et $B = \mathbf{C}[[X, Y]]$, où $\mathbf{R}$ et $\mathbf{C}$ sont respectivement le corps des réels et le corps des complexes, et X et Y des variables, analytiquement indépendantes. Alors A et B sont des anneaux locaux réguliers complets de dimension 2, d'égale caractéristique, et B est un A-module libre de rang 2.

Prenons $t = X^2 + Y^2 \in (AX + AY)^2$.

t est extrémal dans A et réductible dans B.

$t = (X + i\,Y)(X - i\,Y)$ avec $i^2 = -1$.

Donc, d'après ce que nous savons déjà. $A[1/t]$ n'est euclidien pour aucun algorithme, alors que $B[1/t]$ est euclidien.

III. Une conséquence du théorème restreignant

THÉORÈME 3. – *Soit A un anneau local régulier, de dimension 2, dont le corps résiduel n'est pas algébriquement clos. Alors, il existe dans A une famille infinie d'éléments irréductibles, premiers entre eux deux à deux, telle que, si S désigne la partie multiplicative engendrée par ces éléments extrémaux*

et par les unités de A, l'anneau principal $S^{-1}A$ a une construction transfinie triviale, et donc n'est pas euclidien.

Démonstration. — Soient M l'idéal maximal de A, $k = A/M$ le corps résiduel, $A' = k[X, Y]$ l'anneau gradué associé, et $h : A \to A'$ l'application canonique. Puisque k n'est pas algébriquement clos, soit $T = T(X, Y) \in A'$, un polynôme homogène et irréductible de degré $n \geqslant 2$. Notons encore

$$S' = \{ l\,T^i;\ l \in k^* \text{ et } i \in \mathbf{N} \} \subset h(A) \subset A'$$

et prenons enfin $S = h^{-1}(S') \subset A$.

Il est assez clair que S est une partie multiplicative saturée et que, déjà dans $h^{-1}(T)$ où il n'y a que des éléments extrémaux, une infinité d'éléments sont premiers entre eux deux à deux (*voir* éventuellement la note à la fin du paragraphe, après la démonstration du corollaire).

Supposons que la construction transfinie de l'anneau principal $S^{-1}A$ ne soit pas triviale (i. e. $(S^{-1}A)^-{}_1 = \{0\}$, $(S^{-1}A)_0 = (S^{-1}A)^*$, $(S^{-1}A)_1 \neq \varnothing$). Soit donc $b \in (S^{-1}A)_1$. On sait bien que b est, dans $S^{-1}A$, associé à un élément de A qui, dans notre propos, a les mêmes propriétés que b et que, pour la circonstance, nous continuerons d'appeler b. Dire ainsi que $b \in (S^{-1}A)_1 \cap A$, c'est dire que

$$\{ \forall a \in A,\ \exists s \in S,\ q \in A,\ r \in S \cup \{0\};\ as = bq + r \}.$$

En appliquant h, ceci signifie que

$$\{ \forall x \in h(A),\ \exists s' \in S',\ Q \in A',\ R \in S' \cup \{0\};\ xs' = h(b)\,Q + R \}.$$

Pour tout $y \in A'$, on a

$$y = \sum_{j=0}^{m} x_j \qquad (m \in \mathbf{N}),$$

avec x_j homogène de degré j, et pour chaque j $(0 \leqslant j \leqslant m)$,

$$x_j s'_j = h(b)\,Q_j + R_j$$

pour des $s'_j \in S'$, $Q_j \in A'$ et $R_j \in S' \cup \{0\}$.

En multipliant y par le produit des s'_j ainsi obtenus, en appelant A'' l'anneau local de A' en (0, 0), et en remarquant que toute somme finie non nulle d'éléments de S' est, dans A', associée à un élément de S'', on prend conscience qu'au bout du compte $h(b)$ qui, par construction n'est pas dans $S' \cup \{0\}$, devrait se trouver dans le premier cran non trivial

de la construction transfinie de l'anneau principal $S'^{-1}A'' = A''[1/t]$, lequel est vide d'après le « *théorème restreignant* ». Contradiction.

COROLLAIRE. — *Avec les mêmes notations, si t est un élément de M tel que $h(t) \in S'$, l'anneau principal $A[1/t]$ n'est pas euclidien. Plus généralement, si $S_1 \subset S$ est une partie multiplicative contenant au moins un élément de M, il en est de même de l'anneau principal $S_1^{-1}A$.*

Démonstration. — C'est bien clair. On ne peut à peu près rien dire de la construction transfinie de ces anneaux principaux, sinon que son intersection avec A est incluse dans $S \cup \{0\}$.

Note. — Soit $t \in h^{-1}(T)$ et, pour tout $p \in \mathbf{N}$, notons A'_p l'ensemble des polynômes homogènes de degré p : $A' = \bigoplus_{p \in N} A'_p$. Dans chaque A'_p considérons l'ensemble non vide des familles $F \subset A'_p$ de polynômes homogènes étrangers à T, telles que, si $x \in F$, $x' \in F$ et $x \neq x'$, alors $x - x'$ est encore étranger à T.

Ordonné par la relation d'inclusion, cet ensemble satisfait les hypothèses du lemme de Zorn. Pour tout $p \in \mathbf{N}$, soit donc F_p une telle famille maximale, et prenons $F' = \bigcup_{p>n} F_p$. Pour chaque $x \in F'$, choisissons un $q_x \in A$ tel que $h(q_x) = x$. Alors, tous les éléments $t = q_x$ $(x \in F')$ sont premiers entre eux deux à deux. La maximalité des F_p n'est là que pour agrandir la famille des $t + q_x$ qui, elle, n'est pas maximale dans $h^{-1}(T)$.

IV. Un curieux théorème

THÉORÈME 4. — *Soit R un anneau non intègre. Supposons que R possède un idéal premier P tel que*

1° *P contienne un élément non nul de la construction transfinie de R;*

2° *$O : P$, l'idéal annulateur de P, contienne, lui aussi, un élément non nul de cette construction transfinie.*

Alors l'anneau R est euclidien.

Pour démontrer ceci, trois petits lemmes seront utiles.

LEMME 1. — *Soient R un anneau, et I un idéal de R, $I \neq R$. Supposons que I contienne un élément non nul de la construction transfinie de R. Alors, l'idéal I est principal, et l'anneau quotient R/I est euclidien.*

(*Nota* : pour un résultat plus général voir l'Appendice après les exercices afférents à ce « *curieux théorème* ».)

Démonstration. — Soient R' la construction transfinie de R, W un ensemble bien ordonné, de même cardinal de R, $\theta : R' \to W$ et $f : R \to R/I$ les applications canoniques. Parmi les éléments non nuls de $I \cap R'$, choisissons un x tel que $\theta(x)$ soit minimal. Alors, clairement, $I = Rx$.

Pour tout $z \in R/I$, posons

$$\varphi(z) = \inf_{y \in f^{-1}((R/I)_z^*) \cap R'} \theta(y) \in W.$$

L'application $\varphi : R/I \to W$, ainsi bien définie, est un algorithme, comme on peut facilement le vérifier.

LEMME 2. — *Soient R un anneau, J un idéal de R, S une partie multiplicative de R, et soient R', $(R/J)'$, $(S^{-1}R)'$ les constructions transfinies, respectivement de R, R/J, $S^{-1}R$. Soit encore W un ensemble bien ordonné contenant strictement, comme segments initiaux, des ensembles bien ordonnés de mêmes cardinaux que R, R/J, $S^{-1}R$, et soient les applications canoniques,*

$$\theta : R' \to W, \qquad \theta' : (R/J)' \to W, \qquad \theta'' : (S^{-1}R)' \to W,$$
$$f : R \to R/J, \qquad g : R \to S^{-1}R.$$

Pour tout $\alpha \in W$, notons R'_α, $(R/J)'_\alpha$, et $(S^{-1}R)'_\alpha$ les images réciproques, respectivement par θ, θ', θ'', du segment initial de W, d'extrémité α, ouvert en α. Alors, pour tout $\alpha \in W$, on a

$$f(R'_\alpha) \subseteq (R/J)'_\alpha \qquad \text{et} \qquad g(R'_\alpha) \subseteq (S^{-1}R)'_\alpha .$$

Démonstration. — C'est évident pour $\alpha = 0$ et $\alpha = 1$; par récurrence, c'est clair pour tout les autres $\alpha \in W$.

LEMME 3. — *Soient R un anneau local, d'idéal maximal M, et P un idéal premier de R, distinct de M. Alors, P ne contient aucun élément non nul de la construction transfinie de R.*

Démonstration. — En vertu du lemme 1, il suffit de voir que, dans un anneau local R dont l'idéal maximal M est principal, un idéal premier non nul, P de R, distinct de M, n'est jamais principal. Par l'absurde, on aurait, en effet,

$$M = Rx, \qquad P = Ry, \qquad y = xy' \quad (y' \in P),$$
$$y' = yz, \qquad y(1-xz) = 0, \qquad \ldots$$

Remarque. — L'idéal maximal d'un anneau local, qui n'est pas un corps, est, en fait, principal si, et seulement si, la construction transfinie de cet

anneau n'est pas triviale. Puisque, dans ce cas, l'intersection de toutes les puissances de cet idéal maximal principal est un idéal premier ou nul, on voit que, dans tous les cas, la construction transfinie d'un anneau local est à valeurs finies.

Démonstration du théorème 4. — On observe tout d'abord que, si P n'est pas maximal, alors $P+(0 : P) = R$ car, sinon, en prenant le localisé de B en un idéal maximal contenant $P+(0 : P)$, on se heurterait au lemme 3. Puisque la condition $P+(0 : P) = R$ implique que

$$P \cap (0 : P) = P(0 : P) = 0$$

et, par conséquent, que $R \approx (R/P) \times (R/(0 : P))$, on voit que la conclusion du « *curieux théorème* » est claire dans tous les cas, autres que celui où P est maximal et où $O : P \subseteq P$. Dans ce dernier cas, on constate sans délai, fait à ne pas négliger, que $0 : P$ est le nilradical de R.

D'après notre lemme 1 et le fait que la principalité des idéaux premiers entraîne celle de tous les idéaux (résultat dû à I. S. COHEN), ceci entraîne déjà que l'anneau R est principal.

Comme l'annulateur d'un idéal premier, contenu dans P, contient l'annulateur de P, on peut éliminer un cas déjà étudié en supposant, de plus, que notre idéal maximal P est aussi un idéal premier minimal de R. Dans ces conditions, pour tout idéal premier P' de R, on a $0 : P' \subseteq P$. Alors, de même qu'il a été relevé au début de la démonstration, si P' est un idéal premier, non maximal, de R, on aura un isomorphisme de R avec le produit $(R/P') \times (R/(0 : P'))$, et l'anneau $R/(0 : P')$, comme on peut le voir d'après le lemme 2, vérifiera, de même que R, les hypothèses de ce théorème.

R n'ayant qu'un nombre fini d'idéaux premiers minimaux et les anneaux artiniens principaux étant connus pour être euclidiens, la conclusion de ce théorème s'obtient par une suite finie de réductions telles que celle que nous venons de décrire.

COROLLAIRE. — *Soit R un anneau non intègre. Alors R est euclidien si, et seulement si, il vérifie les hypothèses du « curieux théorème ».*

Exercices. — 1° Démontrer le corollaire.

2° Soient R un anneau, et R' sa construction transfinie. On sait (d'après, par exemple, [4], proposition 12) que $R-R'$ est stable pour la multiplication. Soit S la partie multiplicative formée de $R-R'$ et de l'ensemble R^* des unités de R. Montrer que l'anneau $S^{-1}R$ est euclidien.

APPENDICE

THÉORÈME. — *Soient R un anneau, et F la famille des idéaux de R qui ne contiennent aucun élément non nul de la construction transfinie de R. Muni de la relation d'inclusion ordinaire, F est un ensemble ordonné satisfaisant les hypothèses du lemme de Zorn, et les éléments maximaux de F sont des idéaux premiers ou principaux. De plus, si I est un tel élément maximal de F, alors l'anneau quotient R/I est euclidien.*

Démonstration. — Le fait que les éléments maximaux de F soient des idéaux premiers ou principaux se démontre de la même manière que la forme du lemme de Cohen, déjà utilisée dans la démonstration du « *curieux théorème* ». Le fait que l'anneau R/I soit euclidien pour un élément maximal $I \in F$ se démontre en procédant comme dans la démonstration du lemme 1.

V. Deux théorèmes accessoires

THÉORÈME 5. — *Soient R un anneau principal (non nécessairement intègre), et X une indéterminée de R. Alors $R(X)$ est un anneau euclidien.*

(Pour la définition de $R(X)$, si nécessaire *voir* par exemple, [3], chapitre I, § 6.)

Démonstration. — Par suite de la principalité de R et de la définition de $R(X)$, il apparaît assez clairement que, les idéaux principaux de R et ceux de $R(X)$, sont en correspondance canonique et biunivoque.

Soit donc W l'ensemble des idéaux principaux de $R(X)$ (ou de R), que nous munissons de la structure d'ordre suivante :

On considère l'idéal nul comme le plus petit élément de W et, sur $W-(0)$, on prend la relation induite par l'opposée de l'inclusion ordinaire.

L'ensemble W ainsi ordonné satisfait évidemment la condition minimale.

Soit $\varphi : R(X) \to W$ l'application canonique. En tenant compte, d'une part, de la correspondance biunivoque rapportée en début de démonstration et, d'autre part, du fait que si a et b sont deux éléments non nuls de R, alors $a+bX$ est dans $R(X)$ un p. g. c. d. de a et de b, le lecteur doit être en mesure de montrer que φ est un algorithme sur $R(X)$. On conclut au moyen de la proposition 11 de [4].

Remarque 1. — Puisque, pour un anneau factoriel R, la principalité de R et celle de $R(X)$ sont équivalentes, on a, comme corollaire, que,

si R est un anneau factoriel, alors la principalité de R, celle de $R(X)$, et l'euclidienneté de $R(X)$, sont simultanément vérifiées.

Remarque 2. – Si R est un anneau principal intègre, le plus petit algorithme sur $R(X)$ est à valeurs finies et, sa valeur en un élément non nul est donnée par le degré du diviseur principal correspondant à cet élément.

Remarque 3. – Ce théorème 5 montre que tout anneau principal est sous-anneau d'un anneau euclidien tel que les spectres (premiers ou maximaux) des deux anneaux soient canoniquement isomorphes. Ainsi, il serait vain d'espérer reconnaître l'euclidienneté d'un anneau à partir d'une propriété (non géométrique) définie uniquement sur son spectre.

THÉORÈME 6.

(*a*) *Soient R un anneau principal, et M un R-module non nul. Supposons que l'anneau $R+M$ soit principal.*

Si R est intègre, alors R est un corps, et l'anneau $R+M$ est euclidien.

Si R n'est pas intègre, alors le R-module M est isomorphe à R/cR pour un certain élément $c \in R$; si l'anneau R/cR est artinien réduit non local; l'anneau R est isomorphe à un produit $(R/cR) \times R'$, où R' est un anneau principal (éventuellement, R' est l'anneau trivial à un seul élément), et l'anneau $R+M$ est euclidien si, et seulement si, R' est euclidien.

(*b*) *Réciproquement, soit $R = R_1 \times R_2$, où R_1 est un anneau artinien réduit non local, et où R_2 est un anneau quelconque. R_1 étant naturellement muni d'une structure de R-module, on a alors que l'anneau $R+R_1$ est principal si, et seulement si, R_2 est principal, et que $R+R_1$ est euclidien si, et seulement si, R_2 est euclidien.*

Démonstration.

(*a*) Soit z un générateur de M. Puisque $z^2 = 0$, z est multiple de tous les éléments premiers de $R+M$; lesquels, en raison de l'application canonique $R+M \to R$, sont de la forme $p+x$, où $p \in R$ est un élément premier, et où $x \in M$ dépend éventuellemert de p. En décrivant qu'un élément premier $p+x \in R+M$ divise z, on trouve qu'une condition nécessaire (et suffisante) pour que l'anneau $R+M$ soit principal est que

(3) $\forall\, p \in R$, p premier, $\exists\, q \in R$, $x \in M$, $y \in M$ tels que

$$pq = 0 \qquad \text{et} \qquad py+qx = z.$$

Soient cR l'annulateur du R-module M, et $p \in R$ un élément premier divisant c. La condition (3), écrite pour cet élément p, fournit un élément q

qui ne saurait être multiple de p, mais qui doit être divisible par tous les éléments premiers qui ne divisent pas p.

En raisonnant ainsi sur tous les éléments premiers de R qui divisent c, on voit que ces éléments sont générateurs d'idéaux premiers qui sont à la fois minimaux et maximaux, d'où le fait que R soit un corps s'il est intègre.

Si R n'est pas intègre, en insistant sur la partie $pq = 0$ de la condition (3), on voit encore, d'après l'unicité des composantes minimales de la décomposition primaire de l'idéal nul de R, que si $p_1 R, \ldots, p_k R$ sont les distincts idéaux premiers contenant c, alors c ne peut qu'être associé à l'élément $p_1 \ldots p_k$; d'où le fait que R/cR est un anneau artinien réduit non local et que $R \approx (R/cR) \times R'$.

Remarques faites que les éléments premiers de R, qui ne divisent pas c, entrent automatiquement dans la condition (3) et que les anneaux $((R/cR) \times R') + (R/cR)$ et $((R/cR) + (R/cR)) \times R'$ sont canoniquement isomorphes, le reste des conclusions du (*a*) et les affirmations du (*b*) devraient être aisément vérifiables par le lecteur.

COROLLAIRE. — *Soient R un anneau euclidien, et M un R-module. Alors l'anneau $R+M$ est euclidien si, et seulement si, il est principal.*

VI. La division euclidienne et le théorème des progressions arithmétiques

INTRODUCTION. — Soit R un anneau factoriel. Parmi les propriétés qui devraient légitimement aider l'anneau R à être euclidien, il est naturel de penser tout d'abord à la condition nécessaire que tous les éléments irréductibles de R appartiennent à la construction transfinie de R; laquelle condition implique au moins, en vertu d'arguments déjà utilisés dans la démonstration du « *curieux théorème* », que l'anneau R est principal. On peut aussi songer à des propriétés comme le théorème des progressions arithmétiques où l'on a, pour certaines paires (a, b) d'éléments de R, par exemple, chaque fois que a et b sont premiers entre eux, des relations $a = bq + r$, avec des conditions sur r...

Malheureusement, il n'a pas paru évident à l'auteur que l'appartenance des éléments irréductibles à la construction transfinie, même combinée avec le théorème des progressions arithmétiques, suffisait à rendre euclidien l'anneau R.

Dans ce qui suit, nous allons cependant voir qu'avec une condition supplémentaire de « *division euclidienne des éléments irréductibles entre eux* », les choses s'arrangent assez bien.

DÉFINITION 1. – Soit $(E, F; e, f, G)$ un système dans lequel

– E et F sont des ensembles non vides,

– $e : F \to 2^{E \times E}$ et $f : 2^F \to 2^E$ sont des applications, et

– $G \subset E \times F$ est telle que la coupe $G_b \subset E$ suivant n'importe quel élément $b \in F$ est non vide. Pour toute partie S de F ($S \in 2^F$), posons

$$S' = \{ b \in F;\ \forall a \in G_b,\ \exists c \in f(S) \text{ tel que } (a, c) \in e(b) \}.$$

Soient W un ensemble bien ordonné contenant strictement un segment initial de même cardinal que F, et $S_0 \in 2^F$.

Définissons $F_0(S_0) = S_0$, $F_1(S_0) = S_0 \cup S_0'$ et, par récurrence, pour tout $\alpha \in W$, $F_\alpha(S_0) = F_{\alpha-1}(S_0) \cup (F_{\alpha-1}(S_0))'$ si $\alpha - 1$ existe et, si $\alpha - 1$ n'existe pas,

$$F_\alpha'(S_0) = \bigcup_{\alpha' < \alpha} F_{\alpha'}(S_0) \qquad \text{et} \qquad F_\alpha(S_0) = F_\alpha'(S_0) \cup (F_\alpha'(S_0))'.$$

De plus, notons $F'(S_0) = \bigcup_{\alpha \in W} F_\alpha(S_0)$.

Nous appellerons $F'(S_0)$ la construction transfinie à partir de S_0 du système $(E, F; e, f; G)$, et nous dirons que ce système est euclidien à partir de S_0 si $F'(S_0) = F$.

Nous appellerons encore F' la construction transfinie du système $(E, F; e, f; G)$, et nous dirons que ce système est euclidien si $F' = F$.

Remarque 1. – L'intérêt essentiel de cette définition est qu'elle permet de bien déterminer en quel sens un objet pourrait être euclidien.

(*a*) On vérifiera que, si f est croissante, l'euclidienneté (à partir de S_0) d'un tel système $(E, F; e, f; G)$ est équivalente à l'existence d'un algorithme (à partir de S_0), $\varphi : F \to W$, où W est un ensemble bien ordonné tel que, si l'on pose

$$\forall \alpha \in W, \quad F_\alpha(\varphi) = \{ b \in F;\ \varphi(b) < \alpha \},$$

on a $F_1(\varphi) \subset S_0$ et, $\forall (a, b) \in G$, $\varphi(b) \geqq 1$,

$$\exists c \in f(F_{\varphi(b)}(\varphi)) \qquad \text{tel que} \quad (a, c) \in e(b).$$

(*b*) Si de plus $F \subset E$ et $E - F \subset f(\varnothing)$, cette euclidienneté est encore équivalente à l'existence d'un algorithme (à partir de S_0), $\varphi : F \to W$

(où W est un ensemble ordonné satisfaisant à la condition minimale), tel que, si l'on note

$$\forall \alpha \in W, \quad F_\alpha(\varphi) = \{ b \in F - S_0 ;\ \varphi(b) < \alpha \},$$

on a, $\forall\, a \in E$, $\forall\, b \in F - S_0$, avec $(a, b) \in G$,

$$\exists\, c \in E \quad \text{tel que} \quad c \in f(S_0 \cup F_{\alpha(b)}(\varphi)) \quad \text{et} \quad (a, c) \in e(b).$$

DÉFINITION 2. — Soient R un anneau factoriel, et $\mathscr{P}$ la famille de ses idéaux premiers. Prenons :

$E = R$,

$F =$ l'ensemble des idéaux principaux, non premiers, de R.

$e(b) =$ le graphe de la congruence modulo b, $\forall\, b$ tel que $(b) \in F$,

$f(S) =$ la partie de R formée de l'élément 0, des unités de R, des éléments irréductibles de R et des éléments $b \in R$ tels que $(b) \in S$ et, enfin

$G =$ le graphe de la relation « a et b sont premiers entre eux » pour $(b) \in F$.

Nous dirons que R a un degré algorithmique pour ses éléments étrangers si la fonction $\sum_{p \in \mathscr{P}} v_p(b)$ (où v_p est la valuation discrète normalisée associée à p et $(b) \in F$) est un algorithme au sens de la remarque 1.

Exemple. — Soit R un anneau factoriel. Prenons E, F, e et G comme dans la définition 2 pour toute partie S de F, $f(S) =$ la partie de R formée de l'élément nul, des unités de R et des éléments irréductibles de R. Alors, l'euclidienneté du système $(E, F; e, f; G)$ est équivalente au théorème des progressions arithmétiques, ou, du moins, à une forme faible de ce théorème où l'on ne demande pas à une classe de congruence de contenir une infinité d'éléments irréductibles.

Un anneau factoriel vérifiant le théorème des progressions arithmétiques a clairement un degré algorithmique pour ses éléments étrangers. D'après un théorème de Bertini, c'est le cas d'un anneau de fonctions algébriques de dim $\geqslant 2$.

DÉFINITION 3. — Soit R un anneau factoriel, et soit $\mathscr{P}$ la famille de ses idéaux premiers divisoriels. Prenons :

$E =$ la partie formée de 0, des unités de R et des éléments irréductibles de R.

$F = \mathscr{P}$,

$e(p) =$ le graphe de la relation induite par la congruence modulo p, $\forall\, p \in F$,

$f(S)$ = la partie de R formée de l'élément 0, des unités de R et des éléments irréductibles p tels que $(p) \in S$,

$G = E \times F$.

Nous dirons que R admet une division euclidienne de ses éléments irréductibles entre eux si le système $(E, F; e, f; G)$ ainsi formé est euclidien au sens de la définition 1.

Exemple 1. — Soit R un anneau euclidien intègre qui a tous ses éléments irréductibles, au plus, dans le deuxième cran non trivial de sa construction transfinie. On voit facilement que R a une division euclidienne de ses éléments irréductibles entre eux. C'est le cas d'un anneau de polynômes à une variable sur **R** ou sur un corps algébriquement clos.

Moyennant une certaine hypothèse de Riemann généralisée, c'est aussi le cas de certains anneaux principaux d'entiers de corps de nombres (*cf.* [5]).

Exemple 2. — Il est facile de vérifier que tous les anneaux de fractions d'un anneau factoriel satisfaisant le théorème des progressions arithmétiques (au sens faible déjà évoqué dans l'exemple relatif à la définition 2) satisfont aussi ce théorème.

Soit donc A un anneau local régulier, de dim = 2, satisfaisant le théorème des progressions arithmétiques (par exemple l'anneau local en (0, 0) de $K[X, Y]$, où K est un corps, et où X, Y sont algébriquement indépendants sur K). Alors, les anneaux euclidiens du « *gentil théorème* » (i. e. les $K[1/t]$ pour $t \in \mathcal{M} - \mathcal{M}^2$, où $\mathcal{M}$ est l'idéal maximal de A) ont une division euclidienne des éléments irréductibles entre eux.

Pour le voir, il suffit de se rappeler que, lorsque l'on faisait la division euclidienne dans $A[1/t]$ de deux éléments a, $b \in A$, étrangers à t, on obtenait un reste de la forme $t^i r$, où l'entier i était maximal, et où l'élément $r \in A$ était dans le même cran de la construction transfinie de $A[1/t]$ que tous les éléments $r' \in A$ tels que $r - r' \in b A$.

THÉORÈME 7. — *Soit R un anneau factoriel qui a, à la fois, un degré algorithmique pour ses éléments étrangers et une division euclidienne de ses éléments irréductibles entre eux. Alors, l'anneau R est euclidien.*

Démonstration. — Munissons l'ensemble $\mathcal{P}$ des idéaux premiers divisoriels de R d'une structure d'ensemble bien ordonné. Tout idéal divisoriel (b) de R s'écrit alors d'une manière unique :

$$(b) = p_1 p_2 \dots p_k \qquad (\text{avec } p_1 \leqslant p_2 \dots \leqslant p_k \text{ et } p_i \in \mathcal{P}).$$

Soit $\varphi_0 : \mathscr{P} \to W_0$ (W_0 bien ordonné), l'algorithme provenant de la définition 3 et du (*a*) de la remarque 1.

Soit $W = \bigcup_{k=1} W_0^k$ la somme disjointe des produits cartésiens W_0^k, ordonné de façon que, si $\alpha \in W_0^k$ et $\beta \in W_0^{k'}$, on a $\alpha < \beta$ si $k < k'$ et si $k = k'$, $\alpha < \beta$ si α est lexicographiquement antérieur à β. W est alors un ensemble bien ordonné.

Prenons $E = R$, $F =$ l'ensemble des diviseurs > 0 de R, e et f les applications évidentes, et $G = E \times F$.

Si $(b) = p_1 p_2 \ldots p_k$ ($p_1 \leqslant p_2 \leqslant \ldots \leqslant p_k$), posons

$$\varphi(b) = (\varphi_0(p_1), \varphi_0(p_2), \ldots, \varphi_0(p_k)) \in W_0^k.$$

Montrons que l'application $\varphi : F \to W$ ainsi définie est un algorithme pour ce système $(E, F; e, f; G)$, ce qui démontrera l'euclidienneté de R.

Soient a, $b \in R$, $d =$ p. g. c. d. (a, b). Écrivons $a = da'$ et $b = db'$. Puisque R a un degré algorithmique pour ses éléments étrangers, et que a' et b' sont premiers entre eux, on peut d'ores et déjà éliminer le cas évident où b' est réductible. Si nous supposons b' irréductible, l'argument précédemment utilisé nous dit que la classe a' mod b' (ou mod b'^2) contient un élément irréductible $c' \in R$ qui, mod b, et d'après l'hypothèse de division euclidienne des éléments irréductibles entre eux, peut être choisi tel que $\varphi_0(c') < \varphi_0(b')$.

Il est alors facile de vérifier que $\varphi((d, c')) < \varphi((d, b'))$...

Remarque 2. – Si W_0 est fini, alors W est isomorphe, comme ensemble bien ordonné, à **N**. C'est le cas des anneaux euclidiens de l'article de WEINBERGER [5].

Remarque 3. – En vertu de l'assertion (*b*) de la remarque 1, on aurait pu énoncer la définition 3 de manière à permettre aux algorithmes d'être à valeurs dans un ensemble ordonné satisfaisant la condition minimale. En prenant sur W_0^k l'ordre tel que $(\alpha_1, \alpha_2, \ldots, \alpha_l) \leqslant (\beta_1, \beta_2, \ldots, \beta_k)$ si $\alpha_1 \leqslant \beta_1$, $\alpha_2 \leqslant \beta_2$, ... et $\alpha_k \leqslant \beta_k$, on aurait obtenu un W satisfaisant encore la condition minimale. Le lecteur pourra réécrire correctement la démonstration dans cette perspective.

COROLLAIRE. – *Soit A un anneau local régulier, de* dim $= 2$, *satisfaisant le théorème des progressions arithmétiques ou ayant, du moins, un degré algorithmique pour ses éléments étrangers.*

Alors, les localisés $A[1/t]$ pour $t \in \mathscr{M}$, où $\mathscr{M}$ est l'idéal maximal de A, qui ont une division euclidienne de leurs éléments irréductibles entre eux, sont euclidiens.

BIBLIOGRAPHIE

[1] KAPLANSKY (I.). — *Commutative rings.* — Boston, Allyn-Bacon, 1970.

[2] MATSUMURA (H). — *Commutative algebra.* — New York, Benjamin, 1970.

[3] NAGATA (M.). — *Local rings.* — New York, J. Wiley, 1962 (*Interscience Tracts in pure and applied Mathematics*, 13).

[4] SAMUEL (P.). — About euclidean rings, *J. of Algebra*, t. 19, 1971, p. 282-301.

[5] WEINBERGER (P.). — On euclidean rings of albebraic integers, "*Analytic number theory*", p. 321-332. — Providence, American mathematical Society, 1973 (*Proceedings of Symposia in pure Mathematics*, 24).

(Texte reçu le 5 décembre 1974.)

Jean-Jacques HIBLOT,
Mathématiques, Bâtiment 425,
Université de Paris-Sud,
Campus universitaire,
91405 Orsay.