CARACTÉRISATION DE CERTAINS TYPES D'ANNEAUX EUCLIDIENS

Autor(en): **Picavet, Gabriel**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **18 (1972)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **25.04.2024**

Persistenter Link: https://doi.org/10.5169/seals-45375

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

CARACTÉRISATION DE CERTAINS TYPES D'ANNEAUX EUCLIDIENS

par Gabriel PICAVET

On dispose dans l'ensemble **N** des entiers de la théorie de la division Euclidienne: pour tout couple (a, b) d'entiers non nuls, il existe deux entiers q et r tels que $a = bq + r$, où r satisfait $0 \leqslant r < b$. On peut de plus affirmer que les entiers q et r sont déterminés de façon unique.

Une première généralisation consiste à étendre à l'ensemble **Z** des entiers rationnels cette opération. On sait que pour tout couple (a, b) d'éléments non nuls de **Z**, il existe deux entiers rationnels q et r tels que: $a = bq + r$, où r satisfait $|r| < |b|$.

Plus généralement soit A un anneau unifère, et désignons par A^* l'ensemble des éléments non nuls de A. L'anneau A sera supposé commutatif et non réduit à zéro dans toute la suite. Suivant [1] Ch. 7, Par. 1, exercice 7 on a:

DÉFINITION: Un anneau A est dit Euclidien s'il est intègre et s'il existe une application φ de A^* dans **N**, appelée stathme Euclidien, satisfaisant aux conditions suivantes:

1) Pour tout couple d'éléments x et y de A^* $\varphi(xy) \geqslant \varphi(x)$.

2) Pour tout couple d'éléments a et b de A^*, il existe des éléments q et r de A tels que $a = bq + r$ où r satisfait soit $r = 0$ soit $\varphi(r) < \varphi(b)$.

La condition 1) est évidemment satisfaite pour la fonction valeur absolue sur **Z***. Mais en fait cette condition n'est pas essentielle, de même on peut remplacer **N** dans la définition par un ensemble bien ordonné. On pourra consulter à cet effet [3]. Nous utiliserons pour la suite la définition donnée ci-dessus.

Une première remarque est que l'unicité du quotient et du reste dans **N** disparaît dans **Z**. Soient en effet $a \neq 0$ et $b > 0$ des éléments de **Z** et supposons que l'on ait: $a = bq + r$ et $a = bq' + r'$ avec $r \neq 0$ et $|r| < b$, ainsi que $|r'| < b$.

On voit facilement que $r \neq 0$ entraîne $r' \neq 0$. Si l'on suppose $r \neq r'$, on déduit des relations précédentes que $b \leqslant |r - r'| < 2b$ et puisque b divise $|r - r'|$, on obtient: $r' - r = b$ ou $r' - r = -b$.

On obtient alors $r' = r - \frac{r}{|r|} b$. Réciproquement si $a = bq + r$ avec les mêmes conditions que ci-dessus pour a, b, q, r, on peut écrire

$$a = b\left(q + \frac{r}{|r|}\right) + r - \frac{r}{|r|} b \text{ et } \left| r - \frac{r}{|r|} b \right| < b.$$

Ceci montre que dans le cas d'une division avec un reste r non nul, il existe une autre division et une seule avec un reste r' différent de r.

D'autre part si l'on considère un anneau de polynomes $K[X]$ à une indéterminée sur un corps commutatif K, l'application d qui à tout polynome non nul associe son degré est un stathme qui fait de $K[X]$ un anneau Euclidien.

Il est connu que dans ce type d'anneaux le quotient et le reste d'une division sont uniques.

On peut donc se poser le problème de la caractérisation des couples (A, φ) formés d'un anneau Euclidien et de son stathme, pour lesquels il y a unicité du quotient et du reste dans toute division. Ce problème est résolu dans la partie I.

Dans la partie II, on caractérise les couples (A, φ) Euclidiens tels que φ possède les propriétés formelles de la valeur absolue sur $\mathbf{Z}$.

I. Caractérisation des Anneaux Euclidiens pour lesquels il y a unicité de la division

Il convient de noter un anneau Euclidien par un couple (A, φ), car un anneau peut être Euclidien pour des stathmes différents. On sait, voir par exemple [4] Ch. I, Par. 15, que dans un anneau Euclidien (A, φ) deux éléments a et b de A sont associés si et seulement si $\varphi(a) = \varphi(b)$ et $a \mid b$. Il en résulte que u est un élément inversible de A (ou unité) si et seulement si $\varphi(u) = \varphi(1)$. L'ensemble des unités de A sera noté par $U(A)$.

Définition 1: On dira que pour un anneau Euclidien il y a unicité de la division si le couple (q, r) dont la définition de l'introduction assure l'existence est unique.

Proposition 1: Il y a unicité de la division pour (A, φ) si et seulement si: pour tout couple (a, b) d'éléments de A^* tels que $a \neq b$ on a $\varphi(a - b) \leqslant \mathrm{Sup}(\varphi(a), \varphi(b))$.

Supposons qu'il y ait unicité, et soient a et b des éléments distincts de A^*. Si $a - b = -a$ alors $\varphi(a - b) = \varphi(a)$ et dans ce cas $\varphi(a - b) \leqslant \mathrm{Sup}(\varphi(a), \varphi(b))$. Si $2a - b$ est différent de 0, on peut écrire:

$$2a - b = (a-b) \cdot 1 + a$$
$$2a - b = (a-b) \cdot 2 + b$$

L'hypothèse $\varphi(a) < \varphi(a - b)$ et $\varphi(b) < \varphi(a - b)$ entraîne alors $a = b$, par unicité de la division, ce qui est absurde. D'où: $\varphi(a - b) \leqslant \mathrm{Sup}(\varphi(a), \varphi(b))$.

La réciproque est bien connue, sa démonstration pouvant se calquer sur celle qui prouve l'unicité de la division dans un anneau de polynomes.

PROPOSITION 2: Soit (A, φ) un anneau Euclidien pour lequel il y a unicité de la division. Alors A contient un sous corps K constitué par les unités de A et 0.

Il suffit de prouver que K est un sous groupe additif de A. Soient ε et ε' des éléments de K distincts et non nuls. La suite d'inégalités: $\varphi(1) \leqslant \varphi(\varepsilon - \varepsilon') \leqslant \mathrm{Sup}(\varphi(\varepsilon), \varphi(\varepsilon')) = \varphi(1)$ entraîne $\varepsilon - \varepsilon'$ est une unité.

PROPOSITION 3: Soit (A, φ) un anneau Euclidien pour lequel il y a unicité de la division. Si x et y éléments distincts de A^* sont tels que $\varphi(y) < \varphi(x)$, alors $\varphi(x - y) = \varphi(x)$.

La proposition 1 montre déjà que $\varphi(x - y) \leqslant \varphi(x)$. Supposons que $\varphi(x - y) < \varphi(x)$, alors $2x - y$ est différent de 0, car dans le cas contraire on aurait $\varphi(x - y)$ égal à $\varphi(x)$. Les relations:

$$2x - y = x \cdot 1 + (x-y) \quad \text{avec} \quad \varphi(x-y) < \varphi(x)$$
$$2x - y = x \cdot 2 + (-y) \quad \text{avec} \quad \varphi(-y) < \varphi(x)$$

entraînent, par unicité de la divison: $1 = 2$. On aurait alors A réduit à 0, ce qui est impossible. Par suite $\varphi(x - y) = \varphi(x)$.

PROPOSITION 4: Soit (A, φ) un anneau Euclidien pour lequel il y a unicité de la division. Si A n'est pas un corps, il existe un élément x de A^* tel que:

1) Pour tout élément a de A^*, il existe un nombre fini d'éléments $\varepsilon_0, \ldots, \varepsilon_n$ de K, déterminés de façon unique et tels que $a = \sum_{i=0}^{n} \varepsilon_i x^i$.

2) Si dans l'écriture de a ci-dessus $\varepsilon_n \neq 0$, alors $\varphi(a) = \varphi(x^n)$.

L'ensemble B des éléments a de A^* tels que $\varphi(a) > \varphi(1)$ n'est pas vide. En effet, dans le cas contraire on aurait pour tout élément x de A^* $\varphi(x) = \varphi(1)$ et A serait un corps. Or $\varphi(B)$ est inclus dans $\mathbf{N}$ et par conséquent il possède un plus petit élément $\varphi(x)$.

Soit alors un élément a de A^*. Dans le cas où a appartient à K, l'assertion 1) est démontrée. Si a n'est pas une unité, on peut écrire $a = x\,q_0 + r_0$ avec $r_0 = 0$ ou $\varphi(r_0) < \varphi(x)$. Dans les deux cas r_0 appartient à K, et par suite $a - r_0$ est différent de 0. De plus $\varphi(a - r_0) = \varphi(a)$. C'est clair si $r_0 = 0$.

Sinon on remarque que $\varphi(r_0) = 1 < \varphi(a)$ et alors $\varphi(a - r_0) = \varphi(a)$, d'après le résultat de la proposition 3). On en déduit que $\varphi(q_0 x) = \varphi(a)$ et par suite $\varphi(q_0) \leqslant \varphi(a)$. Si on avait $\varphi(q_0) = \varphi(a)$, on aurait alors x appartient à $U(A)$ puisque $\varphi(q_0) = \varphi(q_0 x)$ dans ce cas. Par conséquent on a $\varphi(q_0) < \varphi(a)$.

En conclusion on peut écrire $a = x\,q_0 + \varepsilon_0$ avec ε_0 élément de K et $\varphi(q_0) < \varphi(a)$.

Dans ces conditions, si q_0 appartient à K, l'assertion 1) est démontrée. Si q_0 n'appartient pas à K, on est ramené à la situation précédente avec: $q_0 = x\,q_1 + \varepsilon_1$ où ε_1 est élément de K. On démontre de même que précédemment que $\varphi(q_1) < \varphi(q_0)$. On construit ainsi, par récurrence, une suite $q_0, \ldots, q_n$ d'éléments de A^* tels que $\varphi(q_n) < \varphi(q_{n-1}) < \ldots < \varphi(q_0) < \varphi(a)$ et définis par des relations $q_i = x\,q_{i+1} + \varepsilon_{i+1}$ où ε_{i+1} est un élément de K. La suite d'entiers $\varphi(q_i)$ étant strictement décroissante, il existe un entier n tel que: $\varphi(q_n) < \varphi(x)$ donc tel que q_n soit élément de K. Il suffit alors d'éliminer les éléments q_i des relations les définissant pour prouver l'assertion 1). Montrons que la décomposition de a suivant les puissances de x se fait de façon unique. Pour cela, on peut remarquer qu'il suffit de prouver l'indépendance linéaire des puissances de x sur K. Soit donc une relation $\varepsilon_0 + \varepsilon_i x + \ldots + \varepsilon_n x^n = 0$ où les ε_i sont des éléments de K. Si ε_0 est différent de 0, la relation ci-dessus entraîne que x est une unité, ce qui est impossible. Par suite ε_0 est égal à 0; simplifiant alors la relation par x (A est intègre), on est ramené à une relation $\varepsilon_1 + \ldots + \varepsilon_n x^{n-1} = 0$. On démontre de même que tous les ε_i sont nuls.

Démontrons maintenant l'assertion 2). Pour tout entier n, x^{n-1} divise x^n et ces deux éléments ne sont pas associés, il en résulte que $\varphi(x^{n-1}) < \varphi(x^n)$ pour tout entier n. Soit $a = \varepsilon_0 + \varepsilon_1 x + \ldots + \varepsilon_n x^n$ ou $\varepsilon_n \neq 0$.

Posant $q = \varepsilon_1 + \ldots + \varepsilon_n x^{n-1}$, on obtient $a = \varepsilon_0 + xq$. Or xq est différent de 0 puisque $\varepsilon_n \neq 0$, il résulte alors de la proposition 3) que

$\varphi(a) = \varphi(xq)$ dans le cas où ε_0 n'est pas nul. Cette égalité est encore vraie lorsque $\varepsilon_0 = 0$.

Mais, de façon analogue, on peut écrire: $xq = \varepsilon_1 x + x^2 q'$ et comme ci-dessus on en déduit que $\varphi(xq) = \varphi(x^2 q')$. On démontre, ainsi, par récurrence, que $\varphi(a) = \varphi(\varepsilon_n x^n) = \varphi(x^n)$.

PROPOSITION 5: Soit (A, φ) un anneau Euclidien pour lequel il y a unicité de la division et tel que A ne soit pas un corps. Alors A s'identifie à un anneau de polynomes $K[X]$ sur un corps et son stathme φ à une fonction de $K[X]^*$ dans $\mathbf{N}$ du type $\omega \circ d$, où ω est une fonction strictement croissante de $\mathbf{N}$ dans $\mathbf{N}$ et d la fonction degré sur $K[X]$. Réciproquement $(K[X], \omega \circ d)$, où ω et d sont définis comme ci-dessus, est un anneau Euclidien pour lequel il y a unicité de la division.

La partie directe est une interprétation de la proposition 4). La réciproque est évidente.

II. CARACTÉRISATION DES ANNEAUX EUCLIDIENS DONT LE STATHME POSSÈDE LES PROPRIÉTÉS DE LA VALEUR ABSOLUE SUR $\mathbf{Z}$

DÉFINITION 1: On dira que l'anneau Euclidien (A, φ) vérifie la propriété (H) si A n'est pas un corps et si le stathme φ vérifie:

1) Pour tout couple d'éléments x et y de A^* $\varphi(xy) = \varphi(x)\,\varphi(y)$.

2) Pour tout couple d'éléments x et y de A^* l'égalité $\varphi(x) = \varphi(y)$ équivaut à x et y sont des éléments associés.

3) Pour tout couple d'éléments x et y de A^* tels que $x + y \neq 0$ $\varphi(x + y) \leqslant \varphi(x) + \varphi(y)$.

On se propose de prouver que si (A, φ) vérifie (H), il est alors isomorphe à $(\mathbf{Z}, |\ |)$ en un sens qui sera précisé plus loin.

REMARQUE 1: Un anneau Euclidien dont le stathme est constant est un corps. Cette remarque jointe au fait que $\varphi(1)^2 = \varphi(1)$ lorsque (A, φ) vérifie (H), montre que dans ce cas $\varphi(1) = 1$. On peut alors prolonger φ à A en posant $\varphi(0) = 0$. On pourra donc considérer φ comme une « norme » sur A.

PROPOSITION 1: Soit (A, φ) un anneau Euclidien vérifiant (H). L'application canonique de $\mathbf{Z}$ dans A est une injection.

Supposons la caractéristique de A égale à $p \neq 0$. Pour tout élément de A^* différent de -1 et désigné par x on a les relations:

$$(\varphi(1+x))^{p^n} = \varphi(1+x^{p^n}) \leqslant 1 + \varphi(x)^{p^n}$$

pour tout entier n.

Ces relations sont obtenues à l'aide de 1) et 3) Déf. 1 et résultent de ce que p, étant un nombre premier, divise les coefficients binomiaux C_p^k.

De l'inégalité $\varphi(1+x) \leqslant (1+\varphi(x)^{p^n})^{\frac{1}{p^n}}$, on déduit par passage à la limite $\varphi(1+x) \leqslant \varphi(x)$. Il en résulte que pour tout élément y de A^* et distinct de -1 et 1 on a $\varphi(y) \leqslant \varphi(1-y) \leqslant \varphi(y)$ et par suite $\varphi(y) = \varphi(1-y)$.

D'après Déf. 1, 2), il existe ε élément de $U(A)$ tel que $1 - y = \varepsilon y$.

Alors A serait un corps, ce qui est impossible et $p = 0$.

Remarque 2: Comme dans I, l'hypothèse « A n'est pas un corps » entraîne l'existence d'un plus petit élément $\varphi(x_1)$ dans $\varphi(B_1)$ où B_1 est l'ensemble des éléments a de A^* tels que $\varphi(a) > 1$. Alors pour tout entier n, il existe un élément x de A^* tel que $\varphi(x) > n$. Il suffit de remarquer que

$$\varphi(x_1^k) = (\varphi(x_1))^k.$$

Par suite B_n, ensemble des éléments de A^* tels que $\varphi(x) > n$, est tel que $\varphi(B_n)$ possède un plus petit élément $\varphi(x_n)$. On posera $x_0 = 1$.

LEMME: Soit (A, φ) un anneau Euclidien vérifiant (H) et soit x un élément de A^* non inversible. Si pour tout élément ε de $U(A)$ on a $\varphi(x) \leqslant \varphi(1+\varepsilon x)$ alors: $\varphi(x) = 2$ et x est somme de deux unités de A.

On peut déjà remarquer que $1 + \varepsilon x$ n'est pas nul, x n'appartenant pas à $U(A)$. On a d'autre part les inégalités: $\varphi(x) \leqslant \varphi(1+\varepsilon x) \leqslant 1 + \varphi(x)$.

Or x n'étant pas une unité, on ne peut avoir $\varphi(x) = \varphi(1+\varepsilon x)$, cette égalité entraînant d'après Déf. 1, 2, l'existence d'un élément η de $U(A)$ tel que $\eta x = 1 + \varepsilon x$. On obtient donc, pour tout unité ε l'égalité

$$\varphi(1+\varepsilon x) = 1 + \varphi(x).$$

Il en résulte que $\varphi(1+x) = \varphi(1-x)$, et par suite $1 + x = \varepsilon(1-x)$ où ε appartient à $U(A)$. On en déduit: $x(1+\varepsilon) = \varepsilon - 1$, mais ε étant différent de 1 car $2x \neq 0$ d'après la proposition 1, cette égalité entraîne: $1 < \varphi(x) \leqslant \varphi(\varepsilon - 1) \leqslant 2$. Ceci prouve que $\varphi(x) = 2$. D'autre part,

$\varphi(x)\,\varphi(1+\varepsilon) = \varphi(\varepsilon - 1) \leqslant 2$ entraîne: $1 + \varepsilon$ appartient à $U(A)$ et par suite $x = (1+\varepsilon)^{-1}(1-\varepsilon)$ est une somme de deux unités.

PROPOSITION 2: Lorsque (A, φ) est un anneau Euclidien vérifiant (H), la famille (x_n) définie dans la remarque 2 possède les propriétés suivantes: Pour tout entier n, x_n est une somme de $n+1$ unités et $\varphi(x_n) = n + 1$.

La preuve se fait par récurrence. Supposons que pour toute unité ε de A on ait $\varphi(x_1) \leqslant \varphi(1 + \varepsilon x_1)$, le lemme montre que dans ce cas x_1 est somme de deux unités et que $\varphi(x_1) = 2$. Si, par contre, il existe une unité ε telle que $\varphi(1 + \varepsilon x_1) < \varphi(x_1)$, la définition de x_1 montre que $1 + \varepsilon x_1$ est une unité. Alors x_1 est somme de deux unités α et β et de plus $1 < \varphi(x_1) \leqslant 2$ entraîne $\varphi(x_1) = 2$.

Supposons maintenant que pour $n \geqslant 2$ on ait pour tout entier $p \leqslant n$: x_p est somme de $p+1$ unités et $\varphi(x_p) = p + 1$. Par division Euclidienne on obtient: $1 = x_{n+1}\,q + r$ où $\varphi(r) < \varphi(x_{n+1})$. En effet r ne peut être nul puisque x_{n+1} n'est pas une unité. On peut, d'autre part, supposer que r est différent de 1 et que q est une unité. En effet, il existe une unité ε telle que $\varphi(1 + \varepsilon x_{n+1})$ soit strictement inférieur à $\varphi(x_{n+1})$, le lemme entraînant dans le cas contraire $\varphi(x_{n+1}) = 2$ en contradiction avec $\varphi(x_{n+1}) > n + 1$. Considérons l'égalité $1 = x_{n+1}(-\varepsilon) + (1 + \varepsilon x_{n+1})$; ayant $\varphi(1 + \varepsilon x_{n+1}) < \varphi(x_{n+1})$, la définition de x_{n+1} montre que $\varphi(r) \leqslant n + 1$ où $r = 1 + \varepsilon x_{n+1}$. D'autre part $1 - r = -\varepsilon x_{n+1}$ entraîne: $n + 1 < \varphi(x_{n+1}) \leqslant n + 2$ et alors $\varphi(x_{n+1}) = n + 2$. Si on avait $\varphi(r) < n + 1$ on aurait $\varphi(x_{n+1}) \leqslant 1 + \varphi(r) < n + 2$. Ceci prouve que $\varphi(r) = n + 1 = \varphi(x_n)$, d'où r est somme de $n+1$ unités, et, par suite, x_{n+1} est une somme de $n + 2$ unités.

Corrollaire : Tout élément non nul d'un anneau Euclidien vérifiant (H) est une somme d'unités.

PROPOSITION 3: Dans tout anneau Euclidien (A, φ) vérifiant (H), il existe un entier rationnel p tel que $\varphi(p) > 1$.

La preuve, comme celle de la proposition suivante, utilise la technique de [2] Ch. 6, Par. 6. Ceci provient du fait que l'on peut considérer φ comme une « norme ».

Supposons que pour tout entier $n \neq 0$ on ait $\varphi(n) = 1$. Pour tout couple d'éléments x et y de A l'inégalité $\varphi(x + y) \leqslant \varphi(x) + \varphi(y)$ entraîne $\varphi(x + y) \leqslant 2\,\mathrm{Sup}(\varphi(x), \varphi(y))$. Soit s un entier non nul et posons $\Psi = \varphi^s$, les propriétés de φ entraînent: $\Psi(x)\,\Psi(y) = \Psi(xy)$ et

$\Psi(x+y) \leqslant 2^s \operatorname{Sup}(\Psi(x), \Psi(y))$ pour tout couple (x, y) d'éléments de A. On peut alors utiliser une partie de la Prop. 2 de [2], qui montre que pour $n = 2^r - 1$, on a: $\Psi(x+y)^n \leqslant C^r (\Psi(x) + \Psi(y))^n$ où $C = 2^s$. On en déduit, par passage à la limite dans l'inégalité $\Psi(x+y) \leqslant \overline{C^n}^r (\Psi(x) + \Psi(y))$, que $\Psi(x+y) \leqslant \Psi(x) + \Psi(y)$. Alors $\varphi(x+y) \leqslant (\varphi^s(x) + \varphi^s(y))^{\frac{1}{s}}$ donne par passage à la limite: $\varphi(x+y) \leqslant \operatorname{Sup}(\varphi(x), \varphi(y))$. La partie I montre qu'alors A est isomorphe à un anneau de polynomes $K[X]$, ce qui est impossible puisque X serait d'après le corollaire une somme d'unités.

PROPOSITION 4: La restriction à $\mathbf{Z}$ du stathme φ d'un anneau Euclidien vérifiant (H) est la valeur absolue $|\ |$ sur $\mathbf{Z}$. Il en résulte que tout élément x de A peut s'écrire $x = n\varepsilon$ où n est un entier rationnel et ε une unité.

La preuve s'inspire de [2] Prop. 4, Par. 6, N° 3. Soient a et b des entiers non nuls et différents de 1 et soit g l'application de $\mathbf{Z}^* - \{1\}$ dans $\mathbf{R}$ définie par $g(x) = \dfrac{\operatorname{Log}(\varphi(x))}{\operatorname{Log}|x|}$. Désignons, pour $n \geqslant 2$, la partie entière de $n \dfrac{\operatorname{Log} a}{\operatorname{Log} b}$ par $q(n)$. C'est le plus petit entier m tel que $b^m \leqslant a^n < b^{m+1}$ et il satisfait

$$\lim_{n \to +\infty} \frac{q(n)}{n} = \frac{\operatorname{Log}(a)}{\operatorname{Log}(b)} \text{ et } \lim_{n \to +\infty} q(n) = +\infty.$$

On sait de plus que $a^n = \alpha_0 + \alpha_1 b + \ldots + \alpha_{q(n)} b^{q(n)}$ où les α_i sont des entiers satisfaisant: $0 \leqslant \alpha_i < b$. En utilisant les propriétés de φ, on obtient: $\varphi(a)^n \leqslant b(1 + \varphi(b) + \ldots + \varphi(b)^{q(n)})$. Dans ces conditions on ne peut avoir $\varphi(b) = 1$; en effet $\varphi(b) = 1$ donne $\varphi(a)^n \leqslant (q(n) + 1) b$ ou encore $\operatorname{Log}(\varphi(a)) \leqslant \dfrac{\operatorname{Log}[(q(n) + 1) b].}{n}$ Cette dernière inégalité, entraîne alors par passage à la limite, $\varphi(a) = 1$ pour tout élément de $\mathbf{Z}^*$ distinct de 1, ce qui contredit la proposition 3. On peut donc écrire:

$$\varphi(a)^n \leqslant \frac{b\left(1 - \varphi(b)^{-q(n)-1}\right)}{-1 + \varphi(b)} \varphi(b)^{q(n)+1}$$

où encore:

$$n \operatorname{Log}(\varphi(a)) \leqslant \operatorname{Log}\left(b(\varphi(b) - 1)^{-1}\left(1 - \varphi(b)^{-q(n)-1}\right)\right) + (q(n) + 1)(\log(\varphi(b)).$$

On en déduit que

$$g(a) \leqslant \gamma(n) + \frac{q(n)+1}{n} \cdot \frac{\mathrm{Log}(\varphi(b))}{\mathrm{Log}(a)}$$

où $\gamma(n)$ est une fonction qui tend vers 0 quand n tend vers l'infini. Il en résulte, par passage à la limite, que $g(a) \leqslant g(b)$ et donc $g(a) = g(b)$. Soit $s = g(2)$, alors, pour tout entier a non nul et distinct de 1, $g(a) = s$ entraîne: $\varphi(a) = a^s$. Cette formule se prolonge à $\mathbf{Z}$ par $\varphi(a) = |a|^s$. Puisque, d'après la proposition 3, il existe un entier p tel que $\varphi(p) < 1$, on a forcément $s > 0$. D'autre part $\varphi(2) \leqslant 2$ entraîne $2^s \leqslant 2$, ce qui montre que $s \leqslant 1$. L'hypothèse $s < 1$ entraîne $2^s < 2$ et d'autre part $\varphi(2) = 2^s$ est un entier nous montre qu'alors $2^s = 0$ ou $2^s = 1$ ce qui est absurde. Il en résulte que $s = 1$ et la proposition est démontrée.

PROPOSITION 5: Un anneau Euclidien vérifiant (H) ne possède pas d'unité telle que $\varepsilon^2 = -1$.

Soit ε une unité telle que $\varepsilon^2 = -1$. On a alors la suite d'égalités: $\varphi(1+\varepsilon)^2 = \varphi((1+\varepsilon)^2) = \varphi(2\varepsilon) = \varphi(2) = 2$ qui conduit à la contradiction $\varphi(1+\varepsilon)^2$ est un entier égal à 2.

PROPOSITION 6: L'ensemble des unités d'un anneau Euclidien vérifiant (H) est réduit à $\{-1, 1\}$.

Soit ε une unité de A autre que 1 et -1. Alors $1+\varepsilon$ ne peut être une unité.

Supposons que ce ne soit pas le cas et considérons $1-\varepsilon$. De $\varphi(1-\varepsilon) \leqslant 2$ on déduit, compte tenu de la proposition 4, que $1-\varepsilon = u$ ou $1-\varepsilon = 2u$ où u est une unité de A. Soit v l'unité égale à $1+\varepsilon$. Si l'on a $1-\varepsilon = 2u$, on obtient $2(1-u) = v$ et alors $2\varphi(1-u) = 1$ est absurde. Si l'on a $1-\varepsilon = u$, on obtient $4\varepsilon = (1+\varepsilon)^2 - (1-\varepsilon)^2 = v^2 - u^2$ et alors on a $4 = \varphi(4\varepsilon) = \varphi(v^2-u^2) < 2$ qui est absurde. Donc $1+\varepsilon$ n'est pas une unité, et, puisque $\varphi(1+\varepsilon) \leqslant 2$, on en déduit $\varphi(1+\varepsilon) = 2$. La proposition 4 nous montre qu'alors $1+\varepsilon = 2u$ où u est une unité. D'autre part $\varepsilon^2 \neq 1$ entraîne $\varepsilon^4 \neq 1$ d'après la proposition 5.

Soit η l'unité égale à $-\varepsilon^2$, elle vérifie $\eta^2 \neq 1$ et le raisonnement précédent nous montre que $1+\eta = 2w$ et $1-\varepsilon = 2v$ où v et w sont des unités de A.

La relation $1+\eta = (1+\varepsilon)(1-\varepsilon)$ entraîne alors $2uv = w$ ou encore $2 = \varphi(uv) = \varphi(w) = 1$ ce qui est absurde.

DÉFINITIONS 2: Soient (A, φ) et (A', φ') deux anneaux Euclidiens. Un homomorphisme h de l'anneau A dans l'anneau A' est dit Euclidien si $\varphi' oh = \varphi$. Deux anneaux Euclidiens seront dits isomorphes s'il existe un homomorphisme d'anneaux Euclidiens de l'un dans l'autre qui soit un isomorphisme d'anneaux.

THÉORÈME: Un anneau Euclidien vérifiant (H) est canoniquement isomorphe à $(\mathbf{Z}, |\ |)$.

L'injection canonique de $\mathbf{Z}$ dans A est une surjection puisque, les unités de A étant 1 ou -1, la proposition 4 nous montre que tout élément de A peut s'écrire $x = n \,.\, 1$ où n est un entier relatif.

BIBLIOGRAPHIE

[1] BOURBAKI, N., Eléments de Mathématiques, Livre II, Algèbre, Chapitres 6 et 7. Hermann.
[2] —— Eléments de Mathématiques, XXX, Algèbre Commutative, Chapitres 5 et 6. Hermann.
[3] SAMUEL, P., About Euclidian Rings, *Journal of Algebra*. Vol. 19, n° 2, October 1971.
[4] ZARISKI and SAMUEL, Commutative Algebra. D. Van Nostrand Company.

(Reçu le 29 mai 1972)

Gabriel Picavet
Département de Mathématiques Pures
Complexe Scientifique Universitaire des Cézaux
Université de Clermont
F-63-Clermont-Ferrand