Sur les idéaux fermatiens d'un anneau commutatif

par GABRIEL THIERRIN

Si C est l'anneau des nombres entiers et si n est un nombre impair >1, on voit facilement que le dernier théorème de FERMAT est vrai pour l'exposant n si et seulement si l'idéal (0) est tel que la relation $\sum_{i=1}^{3} a_i^n \in (0)$ entraîne $\sum_{i=1}^{3} a_i \in (0)$. Ce fait nous a conduit à considérer dans un anneau commutatif A deux classes d'idéaux qui font l'objet de ce travail, les idéaux (n, r)-fermatiens et n-fermatiens.

Un idéal M de A est (n, r)-fermatien, n et r étant deux entiers fixés avec $n>1$, $r \geqslant 1$, si la relation $\sum_{i=1}^{r} a_i^n \in M$ entraîne $\sum_{i=1}^{r} a_i \in M$. Tout idéal (n, r)-fermatien est semi-premier. Le radical (n, r)-fermatien d'un idéal quelconque M est l'intersection de tous les idéaux (n, r)-fermatiens contenant M; c'est un idéal (n, r)-fermatien et il est intersection d'idéaux premiers (n, r)-fermatiens. Cette propriété entraîne que tout anneau (n, r)-fermatien (non réduit à 0) est isomorphe à une somme sous-directe de domaines d'intégrité (n, r)-fermatiens. (Pour la notion de somme sous-directe d'anneaux, cf. [2], [3]). Un idéal M de A est n-fermatien, s'il est (n, r)-fermatien, quel que soit r. On obtient pour les idéaux n-fermatiens des résultats analogues à ceux des idéaux (n, r)-fermatiens.

1. Idéaux (n, r)-fermatiens

Soient A un anneau commutatif et n et r deux nombres entiers *fixés*, avec $n>1$ et $r \geqslant 1$. Un idéal M de A sera dit *(n, r)-fermatien*, si la relation $\sum_{i=1}^{r} x_i^n \in M$ entraîne $\sum_{i=1}^{r} x_i \in M$.

Un anneau commutatif dont l'idéal (0) est (n, r)-fermatien sera dit un *anneau (n, r)-fermatien*. Par exemple, si n est pair, l'anneau C des nombres entiers est (n, r)-fermatien. On voit d'autre part facilement que l'anneau C est $(n, 3)$-fermatien, n impair, si et seulement si le dernier théorème de FERMAT est vrai pour l'exposant n.

Remarquons que si M est un idéal de A, l'anneau-quotient A/M est (n, r)-fermatien, si et seulement si M est (n, r)-fermatien. Tout idéal (n, r)-fermatien est (n, s)-fermatien, avec $1 \leqslant s \leqslant r$. L'intersection d'idéaux (n, r)-fermatiens est encore un idéal (n, r)-fermatien.

Remarque. Si p et q sont deux nombres entiers positifs fixés, tout idéal M tel que la relation $\sum_{i=1}^{p} x_i^n - \sum_{j=1}^{q} y_j^n \in M$ entraîne $\sum_{i=1}^{p} x_i - \sum_{j=1}^{q} y_j \in M$ est un idéal $(n, p+q)$-fermatien. Si n est impair, c'est immédiat. Supposons n pair et posons $p+q=r$, $p+1=s$. Soit $\sum_{i=1}^{r} a_i^n \in M$. De $x^n - (-x)^n \in M$ suit $x-(-x) = 2x \in M$, quel que soit x. De $\sum_{i=1}^{p} a_i^n + \sum_{i=s}^{r} a_i^n \in M$ et $2\sum_{i=s}^{r} a_i^n \in M$ suit $\sum_{i=1}^{p} a_i^n - \sum_{i=s}^{r} a_i^n \in M$ et $\sum_{i=1}^{p} a_i - \sum_{i=s}^{r} a_i \in M$. Comme $2\sum_{i=s}^{r} a_i \in M$, on a donc $\sum_{i=1}^{r} a_i \in M$.

Rappelons qu'un idéal M est dit *semi-premier*, si la relation $x^2 \in M$ entraîne $x \in M$. Il en résulte que l'on a $x \in M$, dès que l'on a $x^m \in M$, m étant un entier positif quelconque. Par conséquent, un idéal est semi-premier si et seulement s'il est $(n, 1)$-fermatien.

Théorème 1. *Tout idéal (n, r)-fermatien M d'un anneau commutatif est semi-premier.*

En effet, tout idéal (n, r)-fermatien est $(n, 1)$-fermatien, donc semi-premier.

Corollaire 1. *Tout anneau commutatif (n, r)-fermatien ne contient pas d'éléments nilpotents différents de zéro.*

Corollaire 2. *Pour qu'un anneau commutatif A dont la caractéristique est un nombre premier p soit (p, r)-fermatien, il faut et il suffit qu'il ne contienne pas d'éléments nilpotents différents de zéro.*

Si M est un idéal quelconque d'un anneau commutatif A, l'intersection de tous les idéaux (n, r)-fermatiens contenant M est un idéal (n, r)-fermatien qui sera appelé le *radical (n, r)-fermatien de M* et noté par $R_{(n,r)}(M)$. Si $1 \leqslant s \leqslant r$, on a $R_{(n,s)}(M) \subseteq R_{(n,r)}(M)$, puisque tout idéal (n, r)-fermatien est (n, s)-fermatien. Un idéal est (n, r)-fermatien si et seulement s'il coïncide avec son radical (n, r)-fermatien. Désignons par $S_1(M)$ l'idéal engendré par l'ensemble de tous les éléments x de A de la forme $x = \sum_{i=1}^{r} x_i$ avec $\sum_{i=1}^{r} x_i^n \in M$, par $S_2(M)$ l'idéal $S_1[S_1(M)]$, et d'une manière générale par $S_k(M)$ l'idéal $S_1[S_{k-1}(M)]$. On a les relations $M \subseteq S_1(M) \subseteq \ldots \subseteq S_k(M) \subseteq \ldots \subseteq R_{(n,r)}(M)$.

On déduit facilement de là que

$$R_{(n,r)}(M) = \bigcup_{k=1}^{\infty} S_k(M)$$

car $\bigcup_{k=1}^{\infty} S_k(M)$ est un idéal (n, r)-fermatien.

Le radical (n, r)-fermatien de l'idéal (0) de l'anneau A sera appelé le *radical (n, r)-fermatien de A* et noté par $R_{(n,r)}$.

Rappelons qu'un idéal premier P de A est dit un *idéal premier minimal appartenant à* M, si $M \subseteq P$ et s'il n'existe pas d'idéal premier P' tel que $M \subseteq P' \subset P$. Nous dirons de même qu'un idéal premier (n, r)-fermatien Q de A est un *idéal premier* (n, r)*-fermatien minimal appartenant à* M, si $M \subseteq Q$ et s'il n'existe pas d'idéal premier (n, r)-fermatien Q' tel que $M \subseteq Q' \subset Q$.

Théorème 2. *Soit* M *un idéal* (n, r)*-fermatien d'un anneau commutatif* A. *Tout idéal premier minimal appartenant à* M *est un idéal premier* (n, r)*-fermatien minimal appartenant à* M, *et inversement.*

Soit P un idéal premier minimal appartenant à M et supposons $P \subset A$. On sait (cf. [1], [2]) que l'ensemble $B = A - P$ est un sous-demi-groupe multiplicatif maximal ne rencontrant pas M (c'est-à-dire sans éléments communs avec M). Soit $x = \sum_{i=1}^{r} x_i^n \in P$. Si $y = \sum_{i=1}^{r} x_i \notin P$, alors $y \in B$. Désignons par X le sous-demi-groupe multiplicatif cyclique engendré par l'élément x. On a $X \cap M = \emptyset$; en effet de $x^m \in M$ suit, puisque M est semi-premier (théorème 1), $x \in M$ et donc $y \in M \subseteq P$, ce qui est impossible. On a de même $BX \cap M = \emptyset$. En effet, si $b \in B$ et si $bx^m \in M$, on a $(bx)^m \in M$. D'où $bx \in M$ et $b^n x \in M$, c'est-à-dire $\sum_{i=1}^{r} (bx_i)^n \in M$. Cette dernière relation entraîne, puisque M est (n, r)-fermatien, $\sum_{i=1}^{r} bx_i \in M$ et $by \in M \cap B$, ce qui est impossible. De ce qui précède, il résulte que le sous-demi-groupe

$$T = B \cup X \cup BX$$

contient B et ne rencontre pas M; d'où, puisque B est maximal, $T = B$. Comme $x \in T$, on a donc $x \notin P$, ce qui est contradictoire. Par conséquent, $\sum_{i=1}^{r} x_i \in P$, et P est un idéal premier (n, r)-fermatien minimal appartenant à M.

Soit maintenant Q un idéal premier (n, r)-fermatien minimal appartenant à M. On sait que tout idéal premier Q contenant un idéal M contient un idéal premier minimal P appartenant à M. Mais d'après la première partie du théorème, P est (n, r)-fermatien. Donc $P = Q$.

Théorème 3. *Le radical* (n, r)*-fermatien* $R_{(n,r)}(M)$ *d'un idéal quelconque* M *d'un anneau commutatif* A *est l'intersection de tous les idéaux premiers* (n, r)*-fermatiens minimaux appartenant à* M.

Le radical $R_{(n,r)}(M)$ est un idéal (n, r)-fermatien, donc semi-premier. Par conséquent, (cf. [1], [2]), $R_{(n,r)}(M)$ est l'intersection de tous les idéaux premiers minimaux P_i appartenant à $R_{(n,r)}(M)$. D'après le théorème 2, ces idéaux P_i sont tous les idéaux premiers (n, r)-fermatiens minimaux appartenant à $R_{(n,\,r)}\,(M)$. De la définition du radical (n, r)-fermatien suit alors facilement que les idéaux P_i sont aussi tous les idéaux premiers (n, r)-fermatiens minimaux appartenant à M.

Corollaire. *Tout idéal (n, r)-fermatien M de A est l'intersection de tous les idéaux premiers (n, r)-fermatiens minimaux appartenant à M.*

Théorème 4. *Pour qu'un anneau commutatif A (non réduit à zéro) soit isomorphe à une somme sous-directe de domaines d'intégrité (n, r)-fermatiens, il faut et il suffit qu'il soit (n, r)-fermatien.*

On voit facilement que la condition est nécessaire. Elle est aussi suffisante. En effet, l'idéal (0), étant (n, r)-fermatien, est d'après le corollaire du théorème 3, intersection de tous les idéaux premiers (n, r)-fermatiens minimaux P_i appartenant à (0). Par conséquent, A est isomorphe à une somme sous-directe des anneaux-quotients A/P_i. Comme $A \neq 0$, on a $P_i \subset A$ et les anneaux A/P_i sont des domaines d'intégrité (n, r)-fermatiens.

Théorème 5. *Le corps des quotients K d'un domaine d'intégrité (n, r)-fermatien A est un corps (n, r)-fermatien.*

Soit $\sum_{i=1}^{r} k_i^n = 0$, avec $k_i \in K$. Les éléments k_i sont de la forme $k_i = a_i b_i^{-1}$, avec a_i, $b_i \in A$, $b_i \neq 0$. Posons $b = b_1 b_2 \ldots b_r$; on a $b \neq 0$, $bk_i \in A$ et $\sum_{i=1}^{r} (bk_i)^n = 0$. D'où, puisque A est (n, r)-fermatien, $b \sum_{i=1}^{r} k_i = \sum_{i=1}^{r} bk_i = 0$. Par conséquent, $\sum_{i=1}^{r} k_i = 0$ et K est (n, r)-fermatien.

Théorème 6. *Pour que tous les domaines d'intégrité (n, r)-fermatiens soient de caractéristique non nulle, il faut et il suffit que l'anneau C des nombres entiers ne soit pas (n, r)-fermatien.*

La condition est évidemment nécessaire. Elle est suffisante. En effet, soit A un domaine d'intégrité (n, r)-fermatien et soit K le corps des quotients de A. D'après le théorème 5, K est (n, r)-fermatien. Si A est de caractéristique nulle, il en est de même de K. Le corps K contient alors un sous-corps isomorphe au corps des nombres rationnels qui n'est pas (n, r)-fermatien, puisque C ne l'est pas. Par conséquent, K n'est pas (n, r)-fermatien, ce qui est contradictoire.

Théorème 7. *Soit C l'anneau des nombres entiers et soient a et n deux nombres entiers supérieurs à l'unité, avec n impair. Posons $r = a^n + 1$. Le radical (n, r)-fermatien $R_{(n,\,r)}$ de A vérifie la relation*

$$(0) \subset R_{(n,\,r)} \subseteq (2)\ .$$

L'idéal (2) est évidemment (n, r)-fermatien; donc $R_{(n,r)} \subseteq (2)$. On a d'autre part $a^n - a^n = 0$ et $a^n - a \neq 0$. L'élément a^n peut s'écrire $a^n = 1^n + \ldots + 1^n$. On a par conséquent

$$1^n + \ldots + 1^n + (-a)^n = 0 \quad \text{et} \quad 1 + \ldots + 1 + (-a) \neq 0 \ .$$

L'idéal (0) n'est donc pas (n, r)-fermatien. D'où $(0) \subset R_{(n,r)}$.

Théorème 8. *Soit n un nombre entier impair > 1. Si l'anneau C des nombres entiers n'est pas (n, r)-fermatien, tout nombre premier q, à partir d'un certain rang, est de la forme*

$$q = \frac{\sum_{i=1}^{r} a_i^n}{b}, \quad \text{avec} \quad \sum_{i=1}^{r} a_i = 1 \ .$$

Si C n'est pas (n, r)-fermatien, C n'a qu'un nombre fini d'idéaux premiers (n, r)-fermatiens. Par conséquent, tout nombre premier q, à partir d'un certain rang, est tel que l'idéal premier (q) correspondant n'est pas (n, r)-fermatien. Soit Q le corps des classes résiduelles modulo q, $Q = C/(q)$; le corps Q n'est pas (n, r)-fermatien. Il existe par conséquent r éléments $\alpha_1, \ldots, \alpha_r \in Q$ tels que l'on ait $\alpha = \sum_{i=1}^{r} \alpha_i \neq 0$ et $\sum_{i=1}^{r} \alpha_i^n = 0$. En multipliant respectivement par α^{-1} et α^{-n}, on a, en posant $\alpha_i \alpha^{-1} = \beta_i$

$$\sum_{i=1}^{r} \beta_i = 1 \quad \text{et} \quad \sum_{i=1}^{r} \beta_i^n = 0 \ .$$

Ces relations donnent dans C:

$$\sum_{i=1}^{r} b_i = sq + 1 \quad \text{et} \quad \sum_{i=1}^{r} b_i^n = tq \ .$$

Posons $a_i = b_i$ pour $i = 1, \ldots, r-1$, $a_r = b_r - sq$.
On a alors

$$\sum_{i=1}^{r} a_i = 1 \quad \text{et} \quad \sum_{i=1}^{r} a_i^n = bq \neq 0 \ .$$

Donc $q = \dfrac{\sum_{i=1}^{r} a_i^n}{b}$.

Corollaire 1. *Soient a et n deux nombres entiers supérieurs à l'unité, avec n impair, et posons $r = a^n + 1$. Tout nombre premier q, à partir d'un certain rang, est de la forme*

$$q = \frac{\sum_{i=1}^{r} a_i^n}{b} \quad \text{avec} \quad \sum_{i=1}^{r} a_i = 1 \ .$$

En effet, d'après le théorème 7, l'anneau C n'est pas (n, r)-fermatien.

Corollaire 2. *Si l'équation* $x^n + y^n = z^n$ *a des solutions en nombres entiers positifs* x, y, z, *avec* n *impair* > 1, *tout nombre premier* q, *à partir d'un certain rang, est de la forme*

$$q = \frac{a^n + b^n + c^n}{d} \quad \text{avec} \quad a + b + c = 1 \ .$$

En effet, avec cette hypothèse, l'anneau C n'est pas $(n, 3)$-fermatien.

Corollaire 3. *Le dernier théorème de Fermat est vrai pour tout exposant impair* $n > 1$ *tel qu'il existe une infinité de nombres premiers* q *ne pouvant se mettre sous la forme*

$$q = \frac{a^n + b^n + c^n}{d} \quad \text{avec} \quad a + b + c = 1 \ .$$

2. Idéaux n-fermatiens

Soient A un anneau commutatif et n un nombre entier *fixé*, avec $n > 1$. Un idéal M de A sera dit *n-fermatien*, s'il est (n, r)-fermatien pour tout entier positif r. Un anneau commutatif dont l'idéal (0) est n-fermatien sera dit un *anneau n-fermatien*. Si N est un idéal de A, l'anneau-quotient A/N est n-fermatien si et seulement si N est n-fermatien. L'anneau C des nombres entiers est n-fermatien pour n pair; par contre, d'après le théorème 7, C n'est pas n-fermatien pour n impair.

Du corollaire 2 du théorème 1 suit immédiatement que pour qu'un anneau commutatif, dont la caractéristique est un nombre premier p, soit p-fermatien, il faut et il suffit qu'il ne contienne pas d'éléments nilpotents différents de zéro.

L'intersection d'idéaux n-fermatiens est encore un idéal n-fermatien. Si M est un idéal quelconque de A, l'intersection de tous les idéaux n-fermatiens contenant M est un idéal n-fermatien qui sera appelé le *radical n-fermatien* de M et désigné par $R_n(M)$.

Théorème 9. *On a la relation*

$$R_n(M) = \bigcup_{r=1}^{\infty} R_{(n,r)}(M) \ .$$

Posons $\bigcup_{r=1}^{\infty} R_{(n,r)}(M) = S$. Comme $R_{(n,r)}(M) \subseteq R_n(M)$ pour tout entier positif r, on a donc $S \subseteq R_n(M)$. L'ensemble S est un idéal, car $R_{(n,r)}(M)$ est un idéal et on a $R_{(n,r)}(M) \subseteq R_{(n,s)}(M)$ pour $r < s$. D'autre part, on voit facilement que S est un idéal n-fermatien. Donc $R_n(M) \subseteq S$ et $S = R_n(M)$.

Un idéal premier n-fermatien P sera dit un *idéal premier n-fermatien minimal appartenant à l'idéal* M, si $M \subseteq P$ et s'il n'existe pas d'idéal premier n-fermatien P' tel que $M \subseteq P' \subset P$.

Du théorème 2 suit facilement le théorème suivant:

Théorème 10. *Soit M un idéal n-fermatien d'un anneau commutatif A. Tout idéal premier minimal appartenant à M est un idéal premier n-fermatien minimal appartenant à M, et inversement.*

Théorème 11. *Le radical n-fermatien $R_n(M)$ d'un idéal quelconque M d'un anneau commutatif A est l'intersection de tous les idéaux premiers n-fermatiens minimaux appartenant à M.*

Le radical $R_n(M)$ est un idéal n-fermatien, donc semi-premier. Par conséquent, $R_n(M)$ est l'intersection de tous les idéaux premiers minimaux P_i appartenant à $R_n(M)$. D'après le théorème 10, ces idéaux P_i sont tous les idéaux premiers n-fermatiens minimaux appartenant à $R_n(M)$. De la définition du radical n-fermatien suit alors facilement que les idéaux P_i sont aussi tous les idéaux premiers n-fermatiens minimaux appartenant à M.

Corollaire. *Tout idéal n-fermatien M de A est l'intersection de tous les idéaux premiers n-fermatiens minimaux appartenant à M.*

Théorème 12. *Pour qu'un anneau commutatif A (non réduit à zéro) soit isomorphe à une somme sous-directe de domaines d'intégrité n-fermatiens, il faut et il suffit qu'il soit n-fermatien.*

En utilisant le corollaire du théorème 11, la démonstration de ce théorème est analogue à celle du théorème 4.

Théorème 13. *Le corps des quotients d'un domaine d'intégrité n-fermatien est un corps n-fermatien.*

Ce théorème découle immédiatement du théorème 5.

Théorème 14. *Tout anneau n-fermatien A, n impair, est de caractéristique non nulle N et N divise tout nombre de la forme $q^n - q$, q étant un entier quelconque > 1.*

En effet, pour tout $a \in A$, on a l'égalité $q^n a^n + (-qa)^n = 0$ qui peut se mettre sous la forme

$$a^n + \dots + a^n + (-qa)^n = 0 .$$

Par conséquent, $a + \dots + a + (-qa) = 0$, c'est-à-dire $q^n a - qa = (q^n - q)a = 0$. L'anneau A est donc de caractéristique non nulle N et N divise $q^n - q$.

BIBLIOGRAPHIE

[1] W. Krull, *Idealtheorie in Ringen ohne Endlichkeitsbedingung,* Math. Annalen 101 [1929], p. 729–744.
[2] N. H. McCoy, *Rings and ideals,* Carus Mathematical Monographs, no 8, 1948.
[3] N. H. McCoy, *Subdirect sums of rings,* Bull. Amer. Math. Soc., 53 [1947], p. 856–877.

(Reçu le 13 septembre 1957)