Séminaire Dubreil.
Algèbre et théorie
des nombres

Léonce Lesieur

Sur les anneaux tels que $x^n = x$

Séminaire Dubreil. Algèbre et théorie des nombres, tome 19, n° 2 (1965-1966), exp. n° 13, p. 1-8

<http://www.numdam.org/item?id=SD_1965-1966__19_2_A2_0>

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
19e année, 1965/66, n° 13

7 mars 1966

SUR LES ANNEAUX TELS QUE $x^n = x$

par Léonce LESIEUR

A désigne un anneau unitaire vérifiant :

$$x^n = x \quad , \tag{1}$$

n étant un entier > 1 qui peut dans le cas général dépendre de l'élément $x \in A$. On étudiera aussi le cas où n est le même pour tous les éléments. Exemples : A est un anneau de Boole $(n = 2)$; $A = \underset{\sim}{Z}/6\underset{\sim}{Z}$ $(n = 3)$; A est somme directe des corps F_p à p éléments, p parcourant l'ensemble des nombres premiers. Dans ces exemples, les anneaux considérés sont commutatifs. Il s'agit en fait d'une propriété générale, conséquence imprévue de la relation (1).

1. Commutativité de l'anneau A .

Pour établir la commutativité, nous allons suivre la démonstration donnée par N. JACOBSON ([6], p. 217), en établissant successivement les propriétés suivantes :

PROPRIÉTÉ 1. - L'anneau A n'a pas d'éléments nilpotents non nuls.

Supposons $a^N = 0$; il existe $n(a)$ tel que $a^n = a$.

Si $N < n$, on peut écrire $a = a^n = a^N a^{n-N} = 0$.

Si $N \geqslant n - 1$, on considère $N = k(n - 1) + r$, avec $r = 0$ ou $r < n - 1$, d'où :

$$a^N = a^r = 0 \quad (r > 0) \qquad \text{ou} \qquad a^N = a^{n-1} = 0 \quad (r = 0) \quad .$$

PROPRIÉTÉ 2. - Le radical de Jacobson de A est nul.

Remarquons d'abord que A est un anneau régulier (au sens de von NEUMANN) car on a :

$$x = xx^{n-2}x \quad (n > 2) \qquad \text{ou} \qquad x = x.1.x \quad (n = 2) \quad .$$

Si $x \in R_J(A)$ avec $x \neq 0$, $x^{n-1} = e$ est un élément idempotent du radical R_J. On a donc $(1 - e)e = 0$ et, comme $1 - e$ est inversible, $e = 0$. Il en résulte $x = 0$ d'après la propriété 1.

On a donc :

$$0 = \bigcap_{i \in I} P_i \quad ,$$

où les idéaux P_i sont les idéaux primitifs de A. L'anneau A se trouve donc injecté dans le produit direct des anneaux primitifs A/P_i, la projection sur une composante étant la surjection $A \longrightarrow A/P_i$. Pour exprimer que A est un sous-anneau du produit direct avec cette propriété supplémentaire : la projection sur une composante est une surjection, nous dirons que A est un produit sous-direct des anneaux primitifs A/P_i. Chaque anneau primitif A/P_i vérifie également la relation (1). Or on a la propriété suivante :

PROPRIÉTÉ 3. - Tout anneau primitif vérifiant la relation (1) est un corps (commutatif ou non).

En effet, l'anneau A est, ou bien un anneau K_m de matrices $m \times m$ sur un corps K, ou bien contient un anneau dont une image homomorphe est un anneau K_m, avec $m > 1$ ([6], p. 33). Mais ce dernier cas est exclu par la présence dans K_m d'éléments nilpotents non nuls. Il en résulte $A = K_m$ avec $m = 1$, donc $A = K$.

THÉORÈME 1. - Tout anneau A vérifiant (1) est produit sous-direct de corps commutatifs qui vérifient (1), et par suite est commutatif.

En effet, A est produit sous-direct de corps (propriété 3) qui vérifient la relation (1) du fait que la projection sur chaque composante est une surjection. Il suffit alors de démontrer que tout corps vérifiant la relation (1) est commutatif. Nous renvoyons pour la démonstration à N. JACOBSON ([6], p. 181 à 185) ou I. N. HERSTEIN ([5], p. 324).

La démonstration de la propriété 3 suggère les deux problèmes suivants :

PROBLÈME 1. - Si un anneau est primitif sans éléments nilpotents non nuls, est-ce un anneau intègre ?

PROBLÈME 2. - Si un anneau est premier sans éléments nilpotents non nuls, est-ce un anneau intègre ?

La réponse au problème 2 est affirmative, d'après un résultat récent de C. FAITH et Y. UTUMI [2], dans le cas d'un anneau noethérien à gauche premier.

2. Caractéristique de l'anneau A.

c étant la caractéristique de A, l'anneau $\underset{\sim}{Z}.1$ est isomorphe à $\underset{\sim}{Z}/(c)$ et vérifie la relation (1). Comme $\underset{\sim}{Z}$ ne la vérifie pas, la caractéristique ne peut être nulle. Soit donc

$$c = \prod_{i=1}^{i=k} p_i^{\alpha_i}$$

la décomposition de c en facteurs premiers p_i . On a

$$\underset{\sim}{Z}/\underset{\sim}{Z}.c \simeq \bigoplus_{i=1}^{i=k} \underset{\sim}{Z}/(p_i^{\alpha_i}) \quad .$$

Mais, si $\alpha_i > 1$, l'élément p_i serait nilpotent non nul modulo $p_i^{\alpha_i}$, ce qui est impossible dans l'anneau A . On a donc $\alpha_i = 1$ et $\underset{\sim}{Z}.1$ est somme directe d'un nombre fini de corps premiers K_i . Chacun d'eux vérifie la relation $x^{p_i} = x$, d'où, si $n_0 - 1 = $ p. p. c. m. $(p_i - 1)$, on aura, pour tout $x \in \underset{\sim}{Z}.1$, la relation $x^{n_0} = x$.

THÉORÈME 2. - La caractéristique c d'un anneau A vérifiant (1) est le produit d'un nombre fini de nombres premiers distincts p_i , et on a, pour tout élément x de $\underset{\sim}{Z} - 1$, l'égalité $x^{n_0} = x$, avec $n_0 - 1 = $ p. p. c. m. $(p_i - 1)$.

3. Étude de la caractéristique quand $n(x)$ est constant.

Ce qui précède s'applique en particulier au cas où $n(x) = n$ est constant, mais nous pouvons alors relier la caractéristique à l'entier n . L'anneau $\underset{\sim}{Z}.1$ est un sous-anneau de A et, d'après sa structure étudiée au paragraphe 2, on peut affirmer que $n - 1$ est un multiple commun aux nombres $p_i - 1$ si la caractéristique est $c = \prod_{i=1}^{k} p_i$. Posons :

$$c(n) = \prod_{p_i - 1 \mid n-1} p_i \quad . \tag{2}$$

On a donc :

THÉORÈME 3. - Si A vérifie $x^n = x$ (n fixe), la caractéristique est un diviseur de $c(n)$.

Remarquons que $c(n)$ est toujours un nombre pair ($p_i = 2$ convient).

Exemples :

1° La caractéristique du champ de Galois $G(p^f)$ est p , et on a bien : $p - 1 \mid p^f - 1$.

2° $n = 3$. La caractéristique est 3 pour le corps F_3 , et $6 = c(3)$ pour l'anneau $\underset{\sim}{Z}/(6)$.

3° $n = 5$; $c(n) = 30$. La caractéristique est effectivement 30 pour l'anneau $\underset{\sim}{Z}/(30)$, dont tous les éléments vérifient $x^5 = x$.

4° $n = 2q$; $c(n) = 2$. En effet, si $2q - 1 = M(p - 1)$, le nombre premier p doit être pair, donc égal à 2 .

Ce dernier exemple donne le résultat suivant :

THÉORÈME 4. - Si n est pair, la caractéristique est 2 .

En effet, elle divise $c(n) = 2$, donc elle est égale à 2 .

Le nombre $c(n)$ intervient également dans un problème très élémentaire de théorie des nombres. Si c est la caractéristique d'un anneau A vérifiant $x^n - x = 0$, on aura, en prenant $x = k.1$, $(k \in \underset{\sim}{Z})$:

$$(k^n - k).1 = 0 \quad ,$$

et c sera un diviseur de l'ensemble des entiers $k^n - k$.

Plus précisément :

THÉORÈME 5. - Lorsque k décrit $\underset{\sim}{Z}$, le p. g. c. d. des nombres $k^n - k$ est le nombre $c(n)$ donné par la formule (2).

Soit $c'(n)$ le p. g. c. d. des nombres $k^n - k$ $(k \in \underset{\sim}{Z})$. Démontrons l'égalité : $c(n) = c'(n)$.

1° Tout facteur premier de $c(n)$ est facteur de $c'(n)$. Soit p tel que $n - 1 = q(p - 1)$. Il faut montrer que $k^n - k$ est divisible par p , quel que soit k . C'est évident lorsque k est divisible par p . Sinon, $k^{p-1} - 1$ est divisible par p (FERMAT), c'est-à-dire $\overline{k}^{p-1} = \overline{1}$ dans le corps F_p . On en déduit :

$$\overline{k}^{n-1} = (\overline{k}^{p-1})^q = \overline{1} \quad ,$$

d'où $\overline{k}^n = \overline{k}$.

2° Tout facteur premier de $c'(n)$ est facteur de $c(n)$. Soit p premier tel que $k^n - k = 0 \pmod p$ pour tout $k \in \underset{\sim}{Z}$. On en déduit $\overline{k}^n = \overline{k}$ pour tout élément $\overline{k}$ du corps F_p . Or le groupe multiplicatif des éléments non nuls de F_p est cyclique d'ordre $p - 1$; soit $\overline{k_0}$ un générateur de ce groupe. On a donc $\overline{k_0}^{p-1} = 1$, et les puissances de $\overline{k_0}$ égales à $\overline{k_0}$ ont des exposants de la forme $1 + q(p - 1)$. On a donc :

$$n = 1 + q(p - 1) \quad \text{ou} \quad n - 1 = q(p - 1) \quad .$$

3° Les facteurs premiers de $c'(n)$ sont tous distincts. Supposons en effet que p^α $(\alpha > 1)$ soit un diviseur de $c'(n)$. En prenant $k = p$, on voit que p^α diviserait $p^n - p$. Si $\alpha \leqslant n$, p^α diviserait p , ce qui est impossible. Si

$\alpha > n$, p^n serait également un diviseur commun, ce qui ramène au cas précédent.

Il résulte des propriétés 1°, 2°, 3° que $c(n) = c'(n)$. Dans le cas $n = 2q$, on retrouve ainsi la propriété $c(n) = 2$ en prenant $k = -1$.

On peut, dans la démonstration du théorème 5, se contenter de prendre pour k des nombres naturels, d'où :

THÉORÈME 5'. - Lorsque k décrit $\mathbb{N}$, le p. g. c. d. des nombres $k^n - k$ est le nombre $c(n)$ donné par la formule (2).

4. Structure d'un anneau tel que $x^n = x$ (n fixe).

Appliquons le théorème 1 (qui n'est pas un théorème de structure), au cas où n est constant. L'anneau A est donc un produit sous-direct de corps commutatifs vérifiant la relation (1). Il en résulte que chacun des corps composants est un corps fini vérifiant $x^n = x$, c'est-à-dire un champ de Galois $G(p^r)$, avec

$$n - 1 = q(p^r - 1) \quad .$$

On en déduit :

THÉORÈME 6. - Tout anneau A tel que $x^n = x$ (n fixe), est produit sous-direct de champs de Galois $G(p_i^{r_i})$, avec $p_i^{r_i} - 1 \mid n - 1$.

Inversement, tout produit sous-direct de tels champs de Galois est un anneau qui vérifie $x^n = x$.

Comme application, nous allons obtenir des informations sur l'exposant minimum n tel que $x^n - x = 0$ pour tous les éléments de l'anneau. On remarque en effet que, si $m - 1 = \text{p. p. c. m.}\ (p_i^{r_i} - 1)$ est le plus petit commun multiple des nombres $p_i^{r_i} - 1$ intervenant dans les composantes, on a $x^m = x$. L'entier m est l'exposant minimum, et il vérifie : $n - 1 = k(m - 1)$. D'où :

THÉORÈME 7. - L'exposant minimum m d'un anneau donné A tel que $x^m - x = 0$, est tel que $m - 1$ soit le plus petit commun multiple d'entiers de la forme $p_i^{r_i} - 1$ (p_i premier).

Tous les nombres entiers ne peuvent ainsi être obtenus comme exposant minimum. Par exemple, si m est pair, $m - 1$ est impair, et il en résulte nécessairement $p_i = 2$, d'où :

THÉORÈME 7'. - Un exposant minimum pair m est tel que $m - 1$ soit le plus petit commun multiple de nombres entiers de la forme $2^r - 1$.

Par exemple, si $m = 2$ (anneau de Boole), $m = 4$ (produit sous-direct de corps à 2 ou 4 éléments) peuvent être obtenus comme exposant minimum, il n'en est pas de même de $m = 6$: un anneau tel que $x^6 = x$ est un anneau de Boole. En effet, la caractéristique étant égale à 2 (théorème 4), on obtient en développant $(x + 1)^6$ l'égalité $x^4 + x^2 = 0$, c'est-à-dire $x^4 = x^2$, d'où, en multipliant par x^2 , $x^2 = x$.

Remarque. - Au lieu de prendre l'exposant minimum, on peut au contraire se proposer d'augmenter n en le remplaçant par $n + k(n - 1)$ ou $m + k(m - 1)$. On démontre alors qu'il est toujours possible de choisir pour exposant un nombre premier. Par exemple : $x^4 = x \implies x^7 = x$, et 7 est premier.

5. Etude du demi-groupe multiplicatif de l'anneau.

Les demi-groupes dans lesquels $x^n = x$ ont été étudiés en particulier par J. A. GREEN et D. REES [4], et par T. C. BROWN [1]. Dans le cas d'un anneau, il est possible d'obtenir des résultats plus précis sur le demi-groupe, qui tiennent essentiellement à la commutativité.

THÉORÈME 8. - Le demi-groupe multiplicatif d'un anneau vérifiant la condition $x^{n(x)} = x$ est une réunion de groupes multiplicatifs deux à deux disjoints.

Remarquons que tout élément x engendre un groupe cyclique multiplicatif G_x dont l'élément neutre est $x^{n(x)-1} = e$, et qui est un idempotent de A . Si l'intersection des deux groupes cycliques G_x et G_y n'est pas vide, ces deux groupes ont le même élément neutre e (résultat général de la théorie des demi-groupes). Le sous-groupe maximum ayant e comme élément neutre est alors l'ensemble G_e des éléments x pour lesquels il existe $r(x)$ tel que $x^{r(x)} = e$. L'anneau A est alors la réunion des groupes G_e , qui sont deux à deux disjoints, et l'opération dans G_e est l'opération induite par la multiplication dans A . Le théorème est établi.

Par exemple, l'anneau $\underset{\sim}{Z}/(6)$ est la réunion des groupes

$$G_0 = \{\overline{0}\} \ , \quad G_1 = \{\overline{1} \ , \ \overline{5}\} \ , \quad G_4 = \{\overline{4} \ , \ \overline{2}\} \ , \text{ et } \quad G_3 = \{\overline{3}\} \ ,$$

correspondant aux idempotents $\overline{0}$, $\overline{1}$, $\overline{4}$, $\overline{3}$.

On déduit immédiatement du théorème 8 :

THÉORÈME 9. - Un anneau d'intégrité tel que $x^{n(x)} = x$ est un corps.

En effet, les seuls idempotents sont 0 et 1 . Le groupe G_0 est nul ; l'ensemble des éléments non nuls de l'anneau est le groupe G_1 .

6. Retour sur la commutativité.

La démonstration du théorème 8 s'appuie sur la commutativité. Il est possible d'établir simplement le théorème 8 sans supposer la commutativité, à l'aide de la propriété suivante (cf. [6], p. 211).

PROPRIÉTÉ 4. - A étant un anneau vérifiant la condition $x^{n(x)} = x$, tout idempotent est central.

Soit e un idempotent, et soit $x \in A$. Posons $y = ex(1 - e)$. On a $y^2 = 0$, d'où $y = 0$ (propriété 1). Il en résulte $ex = exe$. De même

$$z = (1 - e)xe = 0 \implies xe = exe \quad .$$

On en déduit :

$$ex = xe \ , \quad \forall \ x \in A \quad .$$

Nous laissons au lecteur le soin d'en déduire le théorème 8. Mais la partition en groupes ainsi obtenue ne prouve pas la commutativité. Celle-ci serait assurée si on démontrait que les groupes sont abéliens.

Dans le cas n fixe, on peut essayer de déduire la commutativité $(xy = yx)$ de la relation $x^n = x$, par des identités formelles d'un anneau. Le cas $n = 2$ est bien connu. Donnons une démonstration valable pour $n = 3$. Posons :

$$\varphi(x \ , \ y) = (x + y)^3 - x^3 - y^3 \quad .$$

On a :

$$\varphi(x \ , \ y) = x^2 y + xyx + yx^2 + y^2 x + yxy + xy^2 = 0 \quad . \tag{3}$$

En linéarisant cette relation, c'est-à-dire en remplaçant y par $y + z$, on obtient :

$$S(x \ , \ y \ , \ z) = xyz + yzx + zxy + yxz + zyx + xzy = 0 \quad . \tag{4}$$

De (3) on déduit :

$$0 = x\varphi(x \ , \ y) - \varphi(x \ , \ y)x = x^2 y^2 + (xy)^2 - y^2 x^2 - (yx)^2 + xy - yx \quad .$$

Pour démontrer l'égalité $xy - yx = 0$, il suffit donc d'établir :

$$x^2 y^2 + (xy)^2 - y^2 x^2 - (yx)^2 = 0 \quad .$$

Or cette relation est une conséquence de (4) quand on y remplace z par $xy - yx$.

Le cas n quelconque nécessite la recherche d'identités formelles dans un anneau dont la nature n'a pas encore été trouvée.

Signalons, pour compléter la bibliographie, les travaux de A. L. FOSTER [3] sur les p-anneaux : anneaux de caractéristique p (premier) qui vérifient $x^p = x$.

BIBLIOGRAPHIE

[1] BROWN (Thomas C.). - On the finiteness of semi-groups in which $x^2 = x$, Proc. Cambridge phil. Soc., t. 60, 1964, p. 1028-1029.

[2] FAITH (Carl) and UTUMI (Yuzo). - On noetherian prime rings, Trans. Amer. math. Soc., t. 114, 1964, p. 53-60.

[3] FOSTER (A. L.). - Generalized "Boolean" theory of universal algebras, Math. Z., t. 58, 1953, p. 306-336 et t. 59, 1953/54, p. 191-199.

[4] GREEN (J. A.) and REES (D.). - On semi-groups in which $x^2 = x$, Proc. Cambridge phil. Soc., t. 48, 1952, p. 35-40.

[5] HERSTEIN (I. N.). - Topics in algebra. - New York, Blaisdell publ. Comp., 1964.

[6] JACOBSON (N.). - Structure of rings, 2nd edition. - Providence, American mathematical Society, 1964 (Amer. math. Soc., Coll. Publ., 37).