# Propriétés asymptotiques des anneaux commutatifs finis[†]

**par Nadir Matringe et Jean-François Planchat**

*nadir.matringe@math.univ-poitiers.fr*
*jf.planchat@gmail.com*

RÉSUMÉ. *Soit $A$ un anneau commutatif fini qui n'est pas un corps. On majore son cardinal $|A|$ en fonction du cardinal de l'ensemble $D(A)$ de ses diviseurs de zéro auquel on a adjoint zéro, et ce de manière optimale, en explicitant le cas d'égalité. L'égalité dans la majoration est obtenue pour certains anneaux locaux. Pour la classe des anneaux locaux, on obtient une majoration plus fine, en termes de $|D(A)|$ et de l'indice de nilpotence du nilradical de $A$. Pour la classe des anneaux non locaux, on démontre aussi une majoration plus fine, en termes du nombre de facteurs locaux $r$ de $A$ et du cardinal $|\mathcal{N}|$ du nilradical de $A$, à nouveau optimale, et on explicite à nouveau le cas d'égalité. Les majorations fines de $|A|$ ainsi obtenues ont un comportement asymptotique clair en terme des paramètres en fonction desquels elles sont exprimées.*

ABSTRACT. Asymptotic properties of commutative finite rings

*Let $A$ be a finite commutative ring which is not a field. We bound its cardinality $|A|$ in terms of the cardinality of the set $D(A)$ of its zero divisors to which we add zero, in an optimal manner, making the case of equality explicit. The equality in the majorization is obtained for certain local rings. For the class of local rings, we obtain a finer bound, in terms of $|D(A)|$ and of the nilpotency index of the nilradical of $A$. For the class of non local rings, we also obtain a finer bound, in terms of the number $r$ of local factors of $A$ and of the cardinality $|N|$ of the nilradical of $A$, again optimal, with an explicitation of the case of equality. The finer majorizations of $|A|$ that we obtain have a clear asymptotic behaviour in terms of the parameters that they involve.*

MOTS-CLÉS : *anneau, corps, anneau local, corps résiduel, indice de nilpotence, nilradical*

---

[†]2010 Mathematics Subject Classification : 11T99,13A99

## 1. Préliminaires

Si $E$ est un ensemble fini, on note $|E|$ son cardinal. On fixe $A$ un anneau (unitaire par définition) commutatif fini. On note $A^\times$ le groupe des unités de $A$, et on pose

$$D(A) = \{x \in A \mid \exists y \in A - \{0\},\ xy = 0\} = \{\text{diviseurs de zéro}\} \cup \{0\}.$$

Le *nilradical* de $A$ est par définition l'idéal $\mathcal{N}$ des éléments de $A$ nilpotents. Puisque $A$ est fini, l'ensemble de ses idéaux premiers coïncide avec celui de ses idéaux maximaux (un anneau intègre fini est un corps) ; notons $\{\mathcal{M}_1, \ldots, \mathcal{M}_r\}$ cet ensemble. Si $r = 1$ on dit que $A$ est *local*. La relation entre $A^\times$, $D(A)$, $\mathcal{N}$ et les idéaux $\mathcal{M}_i$ est donnée par les égalités suivantes :

**Proposition 1.** *1.* $A - A^\times = \cup_{i=1}^r \mathcal{M}_i = D(A)$.

*2.* $\mathcal{N} = \cap_{i=1}^r \mathcal{M}_i$,

*Démonstration.* 1. Pour la première égalité on constate qu'un élément est inversible si et seulement si l'idéal qu'il engendre n'est pas propre, *i. e.* n'est inclus dans aucun idéal maximal. Pour l'égalité $A - A^\times = D(A)$, on remarque que $a \in A$ n'est pas inversible si et seulement si l'application $A$-linéaire $x \mapsto ax$ de $A$ dans $A$ n'est pas surjective, *i. e.* si et seulement si elle n'est pas injective ($A$ est fini), *i. e.* si et seulement si son noyau contient un élément non nul.

2. Un élément de $\mathcal{N}$ est dans tout idéal premier car l'unique élément nilpotent d'un anneau intègre est 0. Inversement si $x \in \cap_{i=1}^r \mathcal{M}_i$, alors pour tout $a \in A$ on a $1 - ax \notin \mathcal{M}_i$ et ce quel que soit $i = 1, \ldots, r$, *i. e.* $1 - ax \in A^\times$ d'après le point précédent. Cependant la suite des puissances de $x$ vivant dans un ensemble fini, il existe $1 \leqslant k < \ell$ tels que $x^\ell = x^k$, donc $(1 - x^{\ell-k})x^k = 0$. Comme $1 - x^{\ell-k}$ est inversible, on en déduit que $x$ est nilpotent.

□

Une conséquence du lemme chinois est que l'anneau *réduit* $A/\mathcal{N}$ de $A$ est un produit de corps :

$$A/\mathcal{N} \simeq \prod_{i=1}^r A/\mathcal{M}_i.$$

On note $k_i$ le corps $A/\mathcal{M}_i$ et $q_i$ son cardinal. Si $A$ est local, on note simplement $k := k_1$ son *corps résiduel* et $q := q_1$.

On utilisera le résultat suivant :

**Lemme 1.** *L'ensemble $D(A)$ est réunion de classes modulo $\mathcal{N}$ et*

$$D(A/\mathcal{N}) = D(A)/\mathcal{N}.$$

*De même le groupe $A^\times$ contient le groupe $1 + \mathcal{N}$ et*

$$(A/\mathcal{N})^\times \simeq A^\times/(1 + \mathcal{N}).$$

*Démonstration.* Le groupe additif $\mathcal{N}$ agit naturellement sur $A$ qui est réunion disjointe de $A^\times$ et $D(A)$. Il suffit donc de montrer que $A^\times$ est $\mathcal{N}$-stable pour montrer que $D(A)$ l'est. Or $A^\times + \mathcal{N} = A^\times(1+\mathcal{N}) = A^\times$ car $1+\mathcal{N} \subset A^\times$. Notons $\pi\colon A \to A/\mathcal{N}$ l'application quotient. Cette application envoie $D(A)$ dans $D(A/\mathcal{N})$ et $A^\times$ dans $(A/\mathcal{N})^\times$. On sait que $\pi$ est surjective et que $D(A/\mathcal{N})$ et $(A/\mathcal{N})^\times$ partitionnent $A/\mathcal{N}$. Ainsi, $\pi$ induit une surjection de $D(A)$ sur $D(A/\mathcal{N})$, ce qui donne $D(A/\mathcal{N}) = D(A)/\mathcal{N}$ ; de même, elle induit un morphisme surjectif de $A^\times$ sur $(A/\mathcal{N})^\times$ dont le noyau est $1+\mathcal{N}$. □

***Indice de nilpotence et filtration.***

On rappelle que si $\mathcal{I}, \mathcal{J}$ sont deux idéaux de $A$, on note $\mathcal{I}\mathcal{J}$ l'idéal engendré par les produits $xy$ avec $x \in \mathcal{I}$ et $y \in \mathcal{J}$. On définit alors naturellement $\mathcal{I}^k$ pour tout entier naturel non nul $k$. C'est l'idéal engendré par les produits de $k$ éléments de $\mathcal{I}$.

Il existe un entier $d \geqslant 1$ tel que $\mathcal{N}^d = \{0\}$ et minimal pour cette propriété. Cet entier est nommé *indice de nilpotence* de $\mathcal{N}$. La *filtration* de $\mathcal{N}$ est la suite d'inclusions suivante :

$$\{0\} = \mathcal{N}^d \subset \mathcal{N}^{d-1} \subset \cdots \subset \mathcal{N}. \tag{1}$$

Si $d \geqslant 2$ (autrement dit si $\mathcal{N}$ n'est pas trivial), on munit naturellement chaque quotient $\mathcal{N}^i/\mathcal{N}^{i+1}$ d'une structure de $A/\mathcal{N}$-module. En outre, aucun d'entre eux n'est trivial, *i. e.* $\mathcal{N}^i \neq \mathcal{N}^{i+1}$ pour tout $1 \leqslant i \leqslant d-1$.

## 2. Minoration de $|A|$ en fonction de $|D(A)|$

La proposition suivante résume la situation.

**Proposition 2.** *On a $|A| \geqslant |D(A)| + 1$ et $|A| = |D(A)| + 1$ si et seulement si $A$ est un produit d'anneaux $\mathbb{Z}/2\mathbb{Z}$ (une algèbre de Boole finie).*

*Démonstration.* L'inégalité $|A| \geqslant |D(A)| + 1$ provient du fait que $A$ est unitaire par définition. De plus si $|A| = |D(A)| + 1$ alors $A^\times = \{1\}$. Comme $1 + \mathcal{N} \subset A^\times$ on en déduit $\mathcal{N} = \{0\}$ et donc $A \simeq \prod_{i=1}^{r} k_i$. On doit donc avoir $k_i^\times = \{1\}$ pour tout $i$, c'est-à-dire $k_i \simeq \mathbb{Z}/2\mathbb{Z}$, d'où $A \simeq (\mathbb{Z}/2\mathbb{Z})^r$. Réciproquement un tel anneau vérifie l'égalité. □

## 3. Majoration de $|A|$ en fonction de $|D(A)|$

On suppose désormais que $|D(A)| \geqslant 2$, *i. e.* que *$A$ n'est pas un corps* (dans le cas des corps il n'y a rien de non trivial à dire).

### 3.1. *Le cas des anneaux locaux*

On suppose ici que $A$ est local. Ainsi $D(A) = \mathcal{N}$ est l'unique idéal maximal de $A$, et $\mathcal{N} \neq \{0\}$ par hypothèse, *i. e.* $d \geqslant 2$.

**Théorème 1.** *Si $A$ est local, on a $|A| \leqslant |D(A)|^{1+\frac{1}{d-1}}$, avec égalité si et seulement si l'idéal $\mathcal{N}$ est principal.*

*Démonstration.* D'après l'équation (1) il existe $n_i \geqslant 1$ tel que $|\mathcal{N}^i/\mathcal{N}^{i+1}| = q^{n_i}$ pour $i = 0, \dots, d-1$ (on rappelle que chaque quotient est un $k$-espace vectoriel non trivial), et $n_0 = 1$. Ainsi $|A| = q|\mathcal{N}|$ et $|\mathcal{N}| = q^{n_1+\cdots+n_{d-1}}$, d'où

$$|A| = |\mathcal{N}|^{1+\frac{1}{n_1+\cdots+n_{d-1}}}.$$

Mais comme $n_i \geqslant 1$, on a $d-1 \leqslant n_1 + \cdots + n_{d-1}$, avec égalité si et seulement si $n_i = 1$ pour tout $i = 1, \dots, d-1$. Ainsi $|A| \leqslant |D(A)|^{1+\frac{1}{d-1}}$ avec égalité si et seulement si chaque $\mathcal{N}^i/\mathcal{N}^{i+1}$ est un $k$-espace vectoriel de dimension 1. Il reste à voir que cela équivaut à $\mathcal{N}$ principal. Si $\mathcal{N} = nA$ avec $n \in \mathcal{N}$, alors pour $i = 0, \dots, d-1$, on a $\mathcal{N}^i = n^i A$ si bien que $\mathcal{N}^i/\mathcal{N}^{i+1}$ est la $k$-droite engendrée par $\overline{n^i}$. Réciproquement, si tous les $\mathcal{N}^i/\mathcal{N}^{i+1}$ sont de dimension 1, c'est en particulier le cas de $\mathcal{N}/\mathcal{N}^2$. Soit $\overline{n}$ un vecteur directeur de cette $k$-droite.

L'idéal $nA$ est un sous-$A$-module du $A$-module $\mathcal{N}$, et donc $\overline{nA}$ est un sous-$k$-espace vectoriel de $\mathcal{N}/\mathcal{N}^2$. On a même $\overline{nA} = \mathcal{N}/\mathcal{N}^2$ puisque $\overline{n} \in \overline{nA}$. Ainsi,

$$\mathcal{N} = nA + \mathcal{N}^2. \tag{2}$$

On considère alors le $A$-module $Q := \mathcal{N}/nA$, dont nous allons montrer qu'il est réduit à $\{0\}$, ce qui conclura. Nous aurons besoin pour cela du

**Lemme 2** (de Nakayama)**.** *Soit $R$ un anneau commutatif dont on note $1$ l'élément neutre, $\mathcal{I}$ un idéal de $R$ et $Q$ un $R$-module de type fini tel que $Q \subset \mathcal{I}Q$. Alors il existe $\delta \in 1 + \mathcal{I}$ tel que $\delta Q = \{0\}$.*

*Démonstration.* Considérons $(q_1, \dots, q_n)$ une famille engendrant $Q$. Par hypothèse, il existe des éléments $m_{i,j} \in \mathcal{I}$ tels que $q_i = \sum_j m_{i,j} q_j$ quel que soit $1 \leqslant i \leqslant n$. Considérons alors les matrices carrées de taille $n$ suivantes : $M = (m_{i,j})_{1 \leqslant i,j \leqslant n}$ et $B = I_n - M$ où $I_n$ désigne la matrice identité. On note $\delta$ le déterminant de $B$ et $\tilde{B}$ la transposée de sa comatrice. Soit de plus $V$ la matrice-colonne $\begin{pmatrix} q_1 \\ \vdots \\ q_n \end{pmatrix}$. Par définition des coefficients $m_{i,j}$, on a $MV = V$. Ainsi :

$$\begin{pmatrix} \delta q_1 \\ \vdots \\ \delta q_n \end{pmatrix} = \delta I_n V = \tilde{B}BV = \tilde{B}(V - MV) = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

ce qui montre que $\delta Q$ est réduit à $\{0\}$ puisque la famille $(q_1, \ldots, q_n)$ engendre $Q$. Reste à voir pourquoi $\delta \in 1 + \mathcal{I}$. Cela se voit en développant le déterminant $\delta = \det(I_n - M)$ et en se rappelant que $M$ est à coefficients dans $\mathcal{I}$. □

De (2), on tire $Q = \mathcal{N}Q$. L'anneau $A$ est commutatif et comme $Q$ est fini, il est de type fini : le lemme de Nakayama assure l'existence d'un $\delta \in 1 + \mathcal{N}$ tel que $\delta Q = Q$ est réduit à $\{0\}$, la dernière égalité découlant de ce que les éléments de $1 + \mathcal{N}$ sont inversibles.

□

**Exemple**. Soit $p$ premier et $d \geqslant 2$. L'anneau $A = \mathbb{Z}/p^d\mathbb{Z}$ est local, son nilradical $pA$ est principal et d'indice de nilpotence égal à $d$.

### 3.2. *Le cas des anneaux non locaux*

On suppose maintenant $r \geqslant 2$. On commence par l'étude du cas où $A$ est réduit, c'est-à-dire $A \simeq \prod_{i=1}^{r} k_i$. On s'y ramènera ensuite grâce au lemme 1. Nous exprimerons les résultats à l'aide de la fonction polynomiale $\varphi_r : [0, +\infty[ \to [1, +\infty[$ définie par

$$\varphi_r(x) = (x+1)^r - x^r = \sum_{j=0}^{r-1} \binom{r}{j} x^j$$

et de sa fonction réciproque $\psi_r : [1, +\infty[ \to [0, +\infty[$ (dont l'existence est claire).

Quand $x$ tend vers $+\infty$, on a $\varphi_r(x) \sim r x^{r-1}$ et $\psi_r(x) \sim (x/r)^{1/(r-1)}$.

La preuve du lemme 3 exposée ici est suggérée par Bernard Randé. Ce lemme se déduit aussi rapidement de l'inégalité de Muirhead comme nous l'expliquons en remarque 1.

**Lemme 3.** *Soient $x_1, \ldots, x_r$ des éléments de $[0, +\infty[$, alors*

$$\prod_{i=1}^{r} (1 + x_i) \geqslant \left(1 + \left(\prod_{i=1}^{r} x_i\right)^{1/r}\right)^r$$

*avec égalité si et seulement si tous les $x_i$ sont égaux.*

*Démonstration.* Si l'un des $x_i$ est nul, l'inégalité et le cas d'égalité sont immédiats.

Sinon, posons $y_i = \ln x_i$ pour tout $i$. Il reste à établir :

$$\frac{1}{r} \ln\left(1 + e^{y_i}\right) \geqslant \ln\left(1 + e^{\frac{1}{r}\sum_{i=1}^{r} y_i}\right),$$

le cas d'égalité étant donné par l'égalité de tous les $y_i$.

Ceci est une conséquence immédiate de la stricte convexité de la fonction $y \mapsto \ln(1+e^y)$. □

**Remarque** 1. Le lemme ci-dessus est aussi une conséquence de l'inégalité de convexité dite de Muirhead ([2, Theorem 45, p.44] ou encore [3] pour une démonstration). Notons $S_r$ le groupe des permutations de $\{1,\dots,r\}$. L'inégalité en question affirme que si $x_1,\dots,x_r$ des nombres réels strictement positifs, et $a_1 \geqslant \dots \geqslant a_r$ et $b_1 \geqslant \dots \geqslant b_r$ des nombres réels tels que de plus

$$a_1 + \cdots + a_k \geqslant b_1 + \cdots + b_k$$

pour $k = 1,\dots,r$ avec égalité pour $k = r$. Alors l'inégalité suivante est vérifiée :

$$\sum_{\sigma\in S_r} x_{\sigma(1)}^{a_1} \cdots x_{\sigma(r)}^{a_r} \geqslant \sum_{\sigma\in S_r} x_{\sigma(1)}^{b_1} \cdots x_{\sigma(r)}^{b_r}.$$

Si $(a_1,\dots,a_r) \neq (b_1,\dots,b_r)$, on a égalité ci-dessus si et seulement si $x_1 = \cdots = x_r$. Remarquons ensuite que

$$\prod_{i=1}^{r}(1+x_i) = \sum_{k=0}^{r} \sigma_{r-k}(x_1,\dots,x_r)$$

où $\sigma_0(x_1,\dots,x_r) = 1$ et $\sigma_l(x_1,\dots,x_r) = \sum_{1\leqslant i_1<\cdots<i_l\leqslant r} x_{i_1}\dots x_{i_l}$ pour $l = 1,\dots,r$. L'inégalité de Muirhead pour les $x_i$ pondérés respectivement par

$$(a_1,\dots,a_r) = (\underbrace{1,\dots,1}_{k \text{ fois}},0,\dots,0)$$

et

$$(b_1,\dots,b_r) = (k/r,\dots,k/r)$$

donne alors après une petite simplification

$$\sigma_{r-k}(x_1,\dots,x_r) \geqslant \binom{r}{k}(x_1\dots x_r)^{k/r}$$

pour $k = 0,\dots,r$, et si tous les $x_i$ sont $> 0$ le lemme 3 découle alors de l'égalité du binôme de Newton. Évidemment si un des $x_i$ est nul le lemme est trivial.

Le lemme 3 a pour conséquence immédiate la minoration suivante pour les produits de corps.

**Proposition 3.** *Supposons que $A$ est réduit, alors $|D(A)| \geqslant \varphi_r(|A^\times|) \geqslant r|A^\times|^{(r-1)/r}$.*

*Démonstration.* Il suffit de soustraire $x_1\dots x_r$ des deux côtés de l'inégalité du lemme 3 et de choisir $x_i := q_i - 1$. □

On en déduit, grâce au lemme 1, le résultat suivant pour les anneaux non locaux quelconques.

**Corollaire 1.** *Si $A$ est non local, alors*

$$|D(A)| \geqslant |\mathcal{N}|\varphi_r\left(\left(\frac{|A^\times|}{|\mathcal{N}|}\right)^{1/r}\right) > r|\mathcal{N}|^{1/r}|A^\times|^{(r-1)/r}.$$

*On a égalité dans la première inégalité si et seulement si tous les $q_i$ sont égaux.*

**Théorème 2.** *On suppose que $A$ n'est pas local. Alors*

$$|A| \leqslant \frac{\psi_r\left(|D(A)|/|\mathcal{N}|\right)^r}{|\mathcal{N}|} + |D(A)| < \frac{\left(\frac{1}{r}\,|D(A)|\right)^{\frac{r}{r-1}}}{|\mathcal{N}|^{\frac{1}{r-1}}} + |D(A)|\,.$$

*On a égalité dans la première inégalité si et seulement si tous les $q_i$ sont égaux.*

**Remarque** 2. Notons $d$ l'indice de nilpotence de $\mathcal{N}$. Comme les $\mathcal{M}_i^d$ sont deux à deux comaximaux, on a d'après le lemme chinois

$$A \simeq \prod_{i=1}^{r} A/\mathcal{M}_i^d.$$

Ainsi $A$ est produit d'anneaux locaux, et cette décomposition est unique dans le sens où une autre décomposition $A \simeq \prod_{i=1}^{s} B_i$ avec les $B_i$ locaux implique $s = r$, et $B_i \simeq A/\mathcal{M}_i^d$ quitte à réordonner les $B_i$ (en effet, un anneau fini est local si et seulement si il est indécomposable). Ainsi, l'entier $r$ du théorème précédent est le nombre de facteurs locaux de $A$.

### 3.3. *Une majoration uniforme*

La majoration obtenue ci-dessus dépend de nombreux paramètres. Nous prouvons ici une majoration uniforme valable pour tous les anneaux commutatifs finis, optimale, et explicitons le cas d'égalité.

**Corollaire 2.** *Soit $A$ un anneau commutatif fini qui n'est pas un corps. Alors $|A| \leqslant |D(A)|^2$ avec égalité si et seulement si $A$ est local, $\mathcal{N}$ est principal et d'indice de nilpotence égal à 2.*

*Démonstration.* Dans le cas non local, on a

$$\begin{aligned}
\frac{\left(\frac{1}{r}\,|D(A)|\right)^{\frac{r}{r-1}}}{|\mathcal{N}|^{\frac{1}{r-1}}} + |D(A)| &\leqslant \left(\frac{1}{r}\,|D(A)|\right)^{\frac{r}{r-1}} + |D(A)| && \text{car } |\mathcal{N}| \geqslant 1\\
&\leqslant \left(\frac{1}{2}\,|D(A)|\right)^{\frac{2}{2-1}} + |D(A)| && \text{car } r \geqslant 2\\
&\leqslant \frac{1}{4}\,|D(A)|^2 + |D(A)|\\
&< |D(A)|^2 && \text{car } |D(A)| \geqslant 2.
\end{aligned}$$

Ainsi l'inégalité stricte du théorème 2 combinée à l'inégalité obtenue ci-dessus entraine $|A| < |D(A)|^2$ pour un anneau non local. Si $A$ est local, on a $|A| \leqslant |D(A)|^{1+\frac{1}{d-1}} \leqslant |D(A)|^2$ d'après le théorème 1. De plus il y a égalité si et seulement si $d = 2$ et égalité dans le théorème 1, *i. e.* si et seulement si $\mathcal{N}$ est principal d'indice de nilpotence égal à 2.

□

**Remarque** 3. Bien sûr la majoration uniforme précédente peut s'obtenir de manière plus directe, et nous laissons cet exercice au lecteur.

## 4. Remarques, remerciements

Le corollaire 2 répond à la question Q961. Ce résultat, comme ceux obtenus dans la partie 3.1, sont dus à CORBAS [1] et, indépendamment RAGHAVENDRAN [4]. Nous n'avons pas trouvé de référence pour les résultats de la partie 3.2.

Cette note doit beaucoup à Alain TISSIER, dont les remarques, suggestions et conjectures concernant une précédente version, ont fortement contribué à améliorer les résultats obtenus et à simplifier leur exposition.

## Références

[1] B. CORBAS, *Rings with few zero divisors*, Math. Ann. 181 (1969), p. 1-7.

[2] G. H. HARDY, J. E. LITTLEWOOD, G. PÓLYA, *Inequalities*, Cambridge University Press, 2e éd. (1952).

[3] R. F. MUIRHEAD, *Some methods applicable to identities and inequalities of symmetric algebraic functions of n letters*, Proceedings of the Edinburgh Mathematical Society 21 (1903), p. 144-157.

[4] R. RAGHAVENDRAN, *Finite associative rings*, Comp. Math. 21 (1969), p. 195-229.