# Structure des anneaux commutatifs finis[†]

**par Colas Bardavid[*] et Éric Pité**

[*]*Professeur en PCSI au Lycée Sainte-Geneviève*

RÉSUMÉ. *On démontre, par des méthodes élémentaires, un théorème de structure pour les anneaux commutatifs finis. Ce résultat est un cas particulier d'une propriété plus générale qu'on peut décrire en termes géométriques.*

ABSTRACT. Structure of Finite Commutative Rings.
*We prove, by elementary methods, a structure theorem for finite commutative rings. This result is a special case of a more general result of which we give a geometrical interpretation.*

MOTS-CLÉS : *Anneaux commutatifs finis, anneaux locaux, idéal premier, idéal maximal, idéaux comaximaux*

## Notations et conventions

**Tous les anneaux de ce texte sont commutatifs unitaires.**

Pour faciliter la lecture, on notera avec des polices différentes les anneaux quelconques et les anneaux finis :

– les lettres $\mathbf{A}$, $\mathbf{B}$, *etc.* désigneront des anneaux commutatifs unitaires ;

– les lettres $\mathbb{A}$, $\mathbb{B}$, *etc.* désigneront des anneaux commutatifs unitaires *finis*.

[†]2020 Mathematics Subject Classification : 11T99, 13A99, 13E10, 13H05, 13M05, 97H40

## 1. Introduction

### 1.1. *Le résultat principal*

Ce texte rassemble quelques réflexions sur les *anneaux commutatifs finis*. On y fait également un peu de combinatoire. On y prouve (c'est le résultat principal) un théorème de dévissage :

**Théorème.** Pour tout anneau commutatif fini $\mathbb{A}$, il existe des anneaux locaux finis $\mathbb{A}_1, \ldots, \mathbb{A}_m$ tel que $\mathbb{A}$ est isomorphe au produit $\mathbb{A}_1 \times \cdots \times \mathbb{A}_m$.

### 1.2. *Plan de l'article*

- La partie 2 donne une démonstration du théorème chinois par un lemme combinatoire.
- La partie 3 présente les idéaux premiers et maximaux des anneaux commutatifs finis afin de démontrer le théorème principal dans la partie 4.
- La partie 5 présente une application du théorème principal : c'est une réponse à une question de la rubrique Question/Réponse, qui est en fait à l'origine de cet article.
- Dans la dernière section, on montre que ce résultat de structure n'a rien de surprenant : c'est un cas particulier d'un théorème plus général portant sur les anneaux artiniens. Nous y expliquerons ce qu'est un anneau artinien et quelles interprétations géométriques on peut donner du théorème et de ces objets.

La preuve donnée n'exige aucune connaissance prérequise en algèbre commutative, si ce n'est une certaine habitude des anneaux quotients. Nous avons parsemé le texte d'exercices pour les lecteurs qui aiment les chercher.

### 1.3. *Un cas bien connu*

Le théorème ci-dessus est bien connu dans le cas où $\mathbb{A} = \mathbb{Z}/m\mathbb{Z}$ : c'est le théorème chinois. Si $m = p_1^{n_1} \cdots p_k^{n_k}$ est une décomposition en produit de nombres premiers, on a un isomorphisme d'anneaux

$$\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{n_k}\mathbb{Z}.$$

Chaque anneau $\mathbb{Z}/p_i^{n_i}\mathbb{Z}$ ne possède qu'un seul idéal maximal, il est local.

### 1.4. *Anneaux locaux*

Commençons cet article par une définition. Le lecteur intéressé pourra consulter [2, chap II §3, p. 102].

**Définition.** Un anneau $\mathbf{A}$ est dit *local* quand il possède un[1] et un seul idéal maximal.

**Exercice 1.** Soit $\mathbf{A}$ un anneau.

1. Montrer que $\mathbf{A}$ est local si, et seulement si, $\mathbf{A} \setminus \mathrm{U}(\mathbf{A})$ est un idéal, où on a noté $\mathrm{U}(\mathbf{A})$ le groupe des inversibles de $\mathbf{A}$.
2. Dans ce cas, caractériser l'unique idéal maximal de $\mathbf{A}$.

**Exercice 2.** Parmi les anneaux suivants, lesquels sont locaux ?

1. Un corps $K$.
2. L'anneau des entiers relatifs $\mathbb{Z}$.
3. Le sous-anneau de $\mathbb{Q}$ dont les éléments ont des dénominateurs impairs.
4. Le sous-anneau $\mathbb{Z}_{(p)}$ de $\mathbb{Q}$ où l'on n'autorise que les fractions dont le dénominateur est premier avec $p$ (un nombre premier).
5. L'anneau $K[[X]]$ des séries formelles sur le corps $K$ en une indéterminée $X$.
6. L'anneau $\mathbf{A}[[X]]$.
7. L'anneau des entiers $p$-adiques, $\mathbb{Z}_p$.
8. L'anneau nul.

**Exercice 3.** Soit $p$ un nombre premier. Montrer que

$$\left\{ \begin{pmatrix} a & 0 & b \\ 0 & a & c \\ 0 & 0 & a \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{Z}/p\mathbb{Z} \right\}$$

est un anneau commutatif fini local.

On rappelle que si $I$ et $J$ sont des idéaux de $A$, *le produit de $I$ et $J$*, noté $IJ$, est l'idéal de $A$ engendré par $\{xy \mid x \in I \text{ et } y \in J\}$.

**Exercice 4.** Soient $\mathfrak{m}$ est un idéal maximal de $\mathbf{A}$ et $i \in \mathbb{N}^*$. En considérant le morphisme canonique

$$\mathbf{A} \longrightarrow \mathbf{A}/\mathfrak{m}^i$$

et l'image directe par ce morphisme de l'idéal $\mathfrak{m}$, montrer que l'anneau quotient $\mathbf{A}/\mathfrak{m}^i$ est local.

---

[1] En supposant l'axiome du choix (ce qu'on fera), le lemme de Zorn nous assure que tout anneau non nul possède au moins un idéal maximal.

## 2. Idéaux comaximaux et théorème chinois

Par souci de complétude, on énonce et démontre le théorème chinois. Si $I$ et $J$ sont des idéaux de $\mathbf{A}$ tels que $I + J = \mathbf{A}$, on dira que $I$ et $J$ sont *comaximaux*. On trouve dans la littérature d'autres adjectifs pour cette propriété : *« $I$ et $J$ premiers entre eux »* ou *« $I$ et $J$ étrangers l'un à l'autre »*.

**Exercice 5.** Pour $n \in \mathbb{N}^*$, on note encore $n$ l'élément $\underbrace{1_A + \cdots + 1_A}_{n \text{ fois}}$ de $A$.

Soient $p$ et $q$ des nombres premiers distincts.

1. Montrer que $(p)$ et $(q)$, en tant qu'idéaux de $\mathbf{A}$, sont comaximaux.
2. Soient $r$ et $s$ des entiers non nuls.
   (a) Montrer qu'il en est de même pour $(p^r)$ et $(q^s)$.
   (b) Montrer que $\mathfrak{m}^r$ et $\mathfrak{n}^s$ sont comaximaux, où $\mathfrak{m}$, $\mathfrak{n}$ sont des idéaux maximaux distincts de $\mathbf{A}$.

Dans la suite, $n$ est un entier naturel non nul.

**Proposition 1** (Théorème chinois)**.** *Soient $I_1, \ldots, I_n$ des idéaux de $\mathbf{A}$ deux à deux comaximaux. Alors,*

1. *La flèche produit $\mathbf{A} \longrightarrow \prod_{i=1}^{n} \mathbf{A}/I_i$ des projections canoniques est surjective.*
2. *Ainsi, on a : $\mathbf{A}/(I_1 \cap \ldots \cap I_n) \simeq \prod_{i=1}^{n} \mathbf{A}/I_i$.*
3. *On a : $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$.*

### *Un lemme combinatoire*

On va utiliser dans notre preuve un lemme combinatoire. Dans la suite, on note

$$\Delta_n := \left\{ (i,j) \in [\![1,n]\!]^2 \;\middle|\; i < j \right\};$$

cet ensemble est muni des deux projections $p_i : \Delta_n \longrightarrow [\![1,n]\!]$ pour $i = 1, 2$.

Pour $E \subset \Delta_n$, on s'intéresse à l'ensemble d'indices

$$\mathbf{I}(E) := p_1(E) \cup p_2(\Delta_n \setminus E).$$

composé des premières coordonnées des éléments de $E$ et des secondes coordonnées des éléments de $\Delta_n \setminus E$.

**Lemme 1.** *Soit $E$ une partie de $\Delta_n$. Alors,*

$$\mathbf{I}(E) = [\![1,n]\!] \quad \textit{ou} \quad \exists i_0 \in [\![1,n]\!]\,,\ \mathbf{I}(E) = [\![1,n]\!] \setminus \{i_0\}\,.$$

***Démonstration.*** On suppose que $\mathbf{I}(E) \neq [\![1,n]\!]$. Soit $i_0$ un indice qui n'est pas dans $\mathbf{I}(E)$. Soit $j > i_0$ ; alors $(i_0, j)$ ne peut pas être dans $E$ et est donc dans $\Delta_n \setminus E$. Donc $p_2(i_0, j)$, qui vaut $j$, est dans $I$. Si $j < i_0$, on raisonne de même avec $(j, i_0)$.
Ainsi, $\mathbf{I}(E) = [\![1,n]\!] \setminus \{i_0\}$. ***cqfd***

**Exercice 6.** De façon plus générale, si $P$ est une partie de $[\![1,n]\!]$ et si $E \subset P$, on note

$$\mathbf{I}_P(E) := p_1(E) \cup p_2(P \setminus E).$$

On dit que $P$ *évite au plus $k$ indices* si $\forall E \subset P,\ \operatorname{card}\big([\![1,n]\!] \setminus \mathbf{I}_P(E)\big) \leqslant k$. On appelle *degré d'évitement de $P$* et on note $\mathbf{e}(P)$ l'entier

$$\mathbf{e}(P) := \max_{E \subset P} \operatorname{card}\big([\![1,n]\!] \setminus \mathbf{I}_P(E)\big).$$

Ainsi, le lemme 1 signifie que le degré d'évitement de $\Delta_n$ vaut 1.

1. Montrer que si $P$ contient $\Delta_n$, alors $P$ évite au plus un indice.
2. Montrer que $[\![1,n]\!]$ n'évite aucun indice, c'est-à-dire que $\mathbf{e}([\![1,n]\!]) = 0$.
3. Quelles sont les parties $P$ de $[\![1,n]\!]$ telles que $\mathbf{e}(P) = 1$ ?

***Décomposition de l'unité***

**Lemme 2.** *Soient $I_1, \ldots, I_n$ des idéaux de $\mathbf{A}$ deux à deux comaximaux. Alors, il existe $x_1, \ldots x_n$ tels que*

$$\forall i \in [\![1,n]\!]\,,\ x_i \in \prod_{j \neq i} I_j \qquad \textit{et} \qquad x_1 + \cdots + x_n = 1.$$

***Démonstration.*** Comme, les $I_i$ sont deux à deux comaximaux, fixons, pour tout $(i,j) \in \Delta_n$, des éléments $a_{(i,j)} \in I_i$ et $b_{(i,j)} \in I_j$ tels que

$$a_{(i,j)} + b_{(i,j)} = 1.$$

On a donc

$$\prod_{(i,j)\in\Delta_n} \big(a_{(i,j)} + b_{(i,j)}\big) = 1.$$

On développe ce produit : pour chaque parenthèse, on choisit soit $a$, soit $b$. Formellement, cela donne :

$$\prod_{(i,j)\in\Delta_n} \big(a_{(i,j)} + b_{(i,j)}\big) = \sum_{E \subset \Delta_n} \prod_{(i,j)\in E} a_{(i,j)} \prod_{(i,j)\in[\![1,n]\!]\setminus E} b_{(i,j)}.$$

Fixons $E \subset \Delta_n$, et notons

$$x := \prod_{(i,j)\in E} a_{(i,j)} \prod_{(i,j)\in[\![1,n]\!]\setminus E} b_{(i,j)}.$$

Si $\mathbf{I}(E) = [\![1,n]\!] \setminus \{i_0\}$ pour un $i_0$, alors on a $x \in \prod_{j\neq i_0} I_j$. Si $\mathbf{I}(E) = [\![1,n]\!]$, on a $x \in \prod_{j=1}^{n} I_j$, donc en particulier $x \in \prod_{j=2}^{n} I_j$, par exemple.

Ainsi, chaque élément dans cette somme est dans un $\prod_{j\neq i_0} I_j$ pour un $i_0$ bien choisi.

Donc, en regroupant les éléments $x$ qui appartiennent au même produit d'idéaux, on en déduit qu'il existe $x_1, \dots x_n$ tels que

$$\forall i \in [\![1,n]\!]\,,\ x_i \in \prod_{j\neq i} I_j \quad \text{et} \quad x_1 + \cdots + x_n = 1.$$

***cqfd***

***Démonstration de la proposition 1***

Fixons-nous une telle décomposition de l'unité ; elle nous permet de prouver les trois points du théorème chinois.

1. Soit $(a_i)_{1\leqslant i\leqslant n}$ une famille dans $\mathbf{A}^n$. On pose $x := a_1x_1 + \cdots + a_nx_n$.
   On vérifie alors que, pour tout $i$, $x = a_i \pmod{I_i}$ : le morphisme
   $$\mathbf{A} \longrightarrow \prod_{i=1}^{n} \mathbf{A}/I_i$$
   est donc bien surjectif.
2. Il suffit de remarquer que le noyau de la flèche précédente est $I_1 \cap \cdots \cap I_n$.
3. On veut montrer que $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$.
   L'inclusion $\supset$ est toujours vraie. Soit $x \in I_1 \cap \cdots \cap I_n$.
   Alors, en multipliant $x$ par la décomposition de l'unité, on trouve
   $$x = \sum_{i=1}^{n} xx_i.$$
   Or, pour tout $i$, $xx_i \in I_1 \cdots I_n$, d'où le résultat.

***Étude d'un exemple***

On va voir dans cet exemple que la preuve donnée ci-dessous est effective.

- On considère les nombres premiers $\mathbf{5}$, $\mathbf{7}$ et $\mathbf{11}$.
- On a les relations de Bézout

$$\begin{aligned} 3 \cdot \mathbf{7} - 4 \cdot \mathbf{5} &= 1 \\ 1 \cdot \mathbf{11} - 2 \cdot \mathbf{5} &= 1 \\ 2 \cdot \mathbf{11} - 3 \cdot \mathbf{7} &= 1. \end{aligned}$$

- En les multipliant entre elles, comme dans la preuve, on obtient la décomposition de l'unité suivante :

$$3 \cdot \mathbf{7} \cdot \mathbf{11} - 8 \cdot \mathbf{5} \cdot \mathbf{11} + 6 \cdot \mathbf{5} \cdot \mathbf{7} = 1. \tag{1}$$

- Voyons maintenant comment cette décomposition de l'unité permet de résoudre les sytèmes de congruences. Par exemple, résolvons

$$(S) : \begin{cases} x \equiv 1 \ (5) \\ x \equiv 5 \ (7) \\ x \equiv 8 \ (11) \end{cases} .$$

  En suivant la démonstration du théorème chinois, on trouve qu'une solution de $(S)$ est

$$x := 1 \cdot 3 \cdot \mathbf{7} \cdot \mathbf{11} + 5 \cdot (-8) \cdot \mathbf{5} \cdot \mathbf{11} + 8 \cdot 6 \cdot \mathbf{5} \cdot \mathbf{7} = -289.$$

  Cette méthode permet, une fois qu'on a obtenu la décomposition (1) de l'unité, de résoudre le système $(S)$ pour tous les restes modulo $5$, $7$ et $11$.

## 3. Idéaux premiers et maximaux des anneaux finis

Dans toute la suite de ce texte, $\mathbb{A}$ est un anneau commutatif unitaire *fini*.

**Proposition 2.** *Les idéaux premiers de* $\mathbb{A}$ *sont les idéaux maximaux de* $\mathbb{A}$.

***Démonstration.*** En effet, si $\mathfrak{p}$ est un idéal premier de $\mathbb{A}$, alors $\mathbb{A}/\mathfrak{p}$ est un anneau intègre fini. Or, on sait que les anneaux intègres finis sont forcément des corps. Donc, $\mathfrak{p}$ est maximal. Réciproquement, un idéal maximal est toujours premier. ***cqfd***

Rappelons que pour un anneau $\mathbf{A}$, on note $\mathrm{Nil}(\mathbf{A})$ l'ensemble des éléments nilpotents de $\mathbf{A}$ : c'est le *nilradical de* $\mathbf{A}$.

**Exercice 7.** Montrer que $\mathrm{Nil}(\mathbf{A})$ est un idéal de $\mathbf{A}$.

On note $\mathfrak{m}_1$, $\mathfrak{m}_2$, ..., $\mathfrak{m}_n$ les idéaux maximaux de $\mathbb{A}$. On a :

**Proposition 3.**

$$\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_n = \mathrm{Nil}(\mathbb{A}).$$

***Démonstration.*** Déjà, comme les $\mathfrak{m}_i$ sont comaximaux, on a $\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_n = \bigcap_{i=1}^{n}\mathfrak{m}_i$. Soit $\mathfrak{m}$ l'un des idéaux maximaux. Soit $x \in \mathrm{Nil}(\mathbb{A})$ et soit $p \in \mathbb{N}^*$ tel que $x^p = 0$. On a $x^p \in \mathfrak{m}$. Comme $\mathfrak{m}$ est premier, on a $x \in \mathfrak{m}$.

Traitons l'autre inclusion.

Soit $x \in \mathbb{A}$ qui n'est pas nilpotent. On considère $S = \{1, x, x^2, \ldots\}$. On considère les idéaux $I$ de $\mathbb{A}$ tels que $I \cap S = \varnothing$. Il y en a au moins un, à savoir $(0)$. Soit $I_0$ un tel idéal et qui soit maximal[2].

Montrons que $I_0$ est premier. Soient $a \notin I_0$ et $b \notin I_0$. Alors, par maximalité de $I_0$, on sait que $I_0 + (a)$ intersecte $S$. On peut donc écrire

$$\alpha a + i_0 = x^p,$$

où $\alpha \in \mathbb{A}, i_0 \in I_0$ et $p \in \mathbb{N}$. De même, on écrit $\beta b + i_0' = x^q$. En multipliant ces deux relations, on obtient $\gamma ab + i_0'' = x^{p+q}$. Donc, nécessairement, $ab \notin I_0$.

Ainsi, $I_0$ est premier et donc maximal. Par définition de $I_0$, on a $x \notin I_0$ et donc $x \notin \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_n$.

Par contraposition, on a ainsi $\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_n \subset \mathrm{Nil}(\mathbb{A})$. ***cqfd***

**Proposition 4.** *Il existe $q_1, \ldots, q_n$ des entiers non nuls tels que*

$$\mathfrak{m}_1{}^{q_1}\mathfrak{m}_2{}^{q_2}\cdots\mathfrak{m}_n{}^{q_n} = (0).$$

***Démonstration.*** Comme $\mathbb{A}$ est fini, soit $N$ tel que

$$\forall x \in \mathrm{Nil}(\mathbb{A}),\ x^N = 0.$$

On considère $\mathfrak{m}$ un idéal maximal de $\mathbb{A}$ ; on note $p$ son cardinal.
Soient $q \in \mathbb{N}$ et $x_1, x_2, \ldots, x_q \in \mathfrak{m}$. Comme $A$ est fini, si $q$ est suffisamment grand, « on sera obligé de prendre plusieurs fois le même $x_i$ ». Plus précisément, d'après le principe des tiroirs, si $q \geqslant p(N-1)+1$, alors l'un des $x_i$ apparaîtra au moins $N$ fois dans le produit $x_1x_2\cdots x_q$. Ainsi, il existe $q \in \mathbb{N}$ tel que

$$\mathfrak{m}^q \subset \sum_{x\in\mathfrak{m}}(x^N).$$

On note $q_i$ un tel entier pour $\mathfrak{m}_i$. Montrons que

$$\mathfrak{m}_1{}^{q_1}\mathfrak{m}_2{}^{q_2}\cdots\mathfrak{m}_n{}^{q_n} = (0).$$

[2] On n'a pas besoin du lemme de Zorn ici, puisque $\mathbb{A}$ est fini.

Cet idéal est engendré par les éléments du type

$$a := \underbrace{x_1 \cdots x_{q_1}}_{\in \mathfrak{m}_1{}^{q_1}} \times \cdots \times \underbrace{z_1 \cdots z_{q_n}}_{\in \mathfrak{m}_n{}^{q_n}}.$$

D'après ce qu'on vient de dire, $x_1 \cdots x_{q_1}$ peut s'écrire $x^N x'$, avec $x, x' \in \mathfrak{m}_1$ ; et de même pour les autres éléments. Ainsi, $a$ peut s'écrire

$$a = (y_1 \cdots y_n)^N t,$$

où $y_i \in \mathfrak{m}_i$ et $t \in \mathbb{A}$.

Comme on a démontré dans la proposition précédente que

$$\mathfrak{m}_1 \mathfrak{m}_2 \cdots \mathfrak{m}_n = \mathrm{Nil}(\mathbb{A}) \ ;$$

on a donc $a = 0$. D'où le résultat. ***cqfd***

***Remarque : cas infini***

La proposition 3 est une version finie du résultat suivant.

**Exercice 8.** Soit $\mathbf{A}$ est un anneau. Montrer que l'intersection de tous les idéaux premiers de $\mathbf{A}$ égale le nilradical de $\mathbf{A}$.

## 4. Structure des anneaux finis

On va avoir besoin du résultat suivant, qu'on laisse en exercice.

**Exercice 9.** Soit $\mathbf{A}$ un anneau.

1. Soit $I$ un idéal de $\mathbf{A}$. Alors, les idéaux de $\mathbf{A}/I$ sont en bijection croissante avec les idéaux de $\mathbf{A}$ contenant $I$.

2. Soit $\mathfrak{m}$ un idéal maximal de $\mathbf{A}$ et soit $i$ un entier non nul. Alors, $\mathbf{A}/\mathfrak{m}^i$ est un anneau local.

### 4.1. *Théorème de dévissage des anneaux finis*

On peut maintenant démontrer le résultat principal de ce texte :

**Théorème 1.** *Tout anneau fini commutatif s'écrit comme produit fini d'anneaux locaux.*

***Démonstration.*** On choisit des entiers $q_i$ comme dans la proposition 4. D'après l'exercice 5, les $\mathfrak{m}_i^{q_i}$ sont deux à deux comaximaux. On a donc

$$\bigcap_{i=1}^{n} \mathfrak{m}_i^{q_i} = \prod_{i=1}^{n} \mathfrak{m}_i^{q_i} = (0).$$

Le théorème chinois nous dit que donc $\mathbb{A} \simeq \mathbb{A}/(0) \simeq \prod_{i=1}^{n} \mathbb{A}/\mathfrak{m}_i^{q_i}$. De plus, d'après l'exercice précédent, les $\mathbb{A}/\mathfrak{m}_i^{q_i}$ sont des anneaux locaux. ***cqfd***

### 4.2. *Anneaux finis locaux*

On aimerait en savoir davantage sur les anneaux finis locaux commutatifs. Commençons par montrer :

**Proposition 5.** *Soit $\mathbb{A}$ un anneau local fini, alors $|\mathbb{A}|$ est une puissance d'un nombre premier.*

On va utiliser :

**Lemme 3.** *Un anneau local* **A** *a pour caractéristique zéro ou la puissance d'un nombre premier.*

***Démonstration.*** Soit **A** un anneau local et $\mathfrak{m}$ son unique idéal maximal. Supposons que **A** soit de caractéristique non nulle $k = ab$, avec $a, b > 1$ et $\operatorname{pgcd}(a, b) = 1$. Alors $a, b \in \mathfrak{m}$, donc $1 \in \mathfrak{m}$ ce qui est impossible. ***cqfd***

**Lemme 4.** *Soient $G$ un groupe abélien fini et $p$ un nombre premier divisant $|G|$. Alors $G$ possède un élément d'ordre $p$.*

***Démonstration.*** Soient $x_1, \ldots, x_k$ des éléments de $G$ qui l'engendrent.

Notons $G_i$ le sous-groupe cyclique engendré par $x_i$ et $\psi$ le morphisme de $\prod_{i=1}^{k} G_i$ dans $G$ qui à $(t_1, \ldots, t_k)$ associe le produit $t_1 \cdots t_k$.

D'après le premier théorème d'isomorphisme, on a $\prod_{i=1}^{k} |G_i| = |G| \times |\operatorname{Ker} \psi|$.

De plus $p$ divise $|G|$, donc il divise l'un des $|G_i|$, ainsi une des puissances de l'un des $x_i$ est d'ordre $p$. ***cqfd***

Au passage, remarquons que le lemme 4 est encore vrai quand $G$ n'est pas abélien ; dans ce cas, il s'appelle théorème de Cauchy.

***Démonstration de la proposition 5.*** Soit $\mathbb{A}$ un anneau local fini ; notons $p^n$ sa caractéristique, où $p$ est un nombre premier et où $n \in \mathbb{N}^*$.

Supposons que $|\mathbb{A}|$ ne soit pas une puissance de $p$ et considérons $q$ un nombre premier divisant $|\mathbb{A}|$ tel que $q \neq p$. On considère maintenant le groupe fini $(\mathbb{A}, +)$. D'après le lemme 4, on sait qu'il existe $x \in \mathbb{A}$ dont l'ordre (additif) vaut $q$. On a donc $qx = 0$ ; on a aussi $p^n x = 0$. Avec une relation de Bézout, on a donc $x = 0$ ; c'est absurde car l'ordre de $x$ vaut $q \neq 1$.

Ainsi, $|\mathbb{A}|$ est une puissance de $p$. ***cqfd***

La proposition 5 nous donne une condition nécessaire pour qu'un anneau fini soit local, mais cette condition n'est pas suffisante. En effet, l'anneau $\left(\mathbb{Z}/p\mathbb{Z}\right)^2$ n'est pas local ; cela découle de la première question de l'exercice suivant.

**Exercice 10.** Soient $\mathbf{A}_1, \ldots, \mathbf{A}_n$ des anneaux. On considère $\mathbf{B} = \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$.

1. Montrer que les idéaux maximaux de $\mathbf{B}$ sont tous du type

$$\mathbf{A}_1 \times \cdots \times \mathbf{A}_{i-1} \times \mathfrak{m}_i \times \mathbf{A}_{i+1} \times \cdots \times \mathbf{A}_n,$$

   où $\mathfrak{m}_i$ est un idéal maximal de $\mathbf{A}_i$.

2. Décrire les idéaux premiers de $\mathbf{B}$.

Ainsi, compter le nombre d'éléments ne suffit pas. En revanche si l'on compte le nombre d'éléments de l'anneau et le nombre de diviseurs de zéro, on peut dire si un anneau fini est local.

**Théorème 2.** *Un anneau fini $\mathbb{A}$ est local si, et seulement si, il existe un nombre premier $p$ et deux entiers $m, n$ avec $m < n$, tels que $|\mathbb{A}| = p^n$ et $\mathbb{A}$ a $p^m$ diviseurs de zéro.*

On peut trouver des preuves dans [1, Theorem 3] ou [4, Theorem 2].

## 5. Application aux groupes des éléments inversibles d'un anneau fini

Le point de départ de cet article était pour les auteurs la résolution de la question Q556 d'Hervé Pépin :

**Question.** Soit $n$ un entier pair. Existe-t-il un anneau commutatif fini $\mathbb{A}$ dont le groupe $\mathrm{U}(\mathbb{A})$ des éléments inversibles possède exactement $n$ éléments ?

Dans la RMS 128-4, Philippe Bonnet fournit une caractérisation complète des cardinaux de $\mathrm{U}(\mathbb{A})$ possibles. Notre approche, qui repose sur le dévissage des anneaux finis, est plus élémentaire — mais moins complète — que celle de Philippe Bonnet.

**Proposition 6.** *Il n'existe pas d'anneau commutatif fini $\mathbb{A}$ dont le groupe $\mathrm{U}(\mathbb{A})$ des éléments inversibles possède exactement $34$ éléments. De plus, $34$ est le plus petit entier pair ayant cette propriété.*

***Démonstration.*** On procède en deux parties :

**• L'entier 34 convient.**

Supposons qu'il existe un anneau commutatif fini $\mathbb{A}$ dont le groupe des inversibles $\mathrm{U}(\mathbb{A})$ possède exactement 34 éléments.

Appliquons le théorème 1 à $\mathbb{A}$ : on écrit $\mathbb{A} \simeq \prod_{i=1}^{m} \mathbb{A}_i$, où les $\mathbb{A}_i$ sont des anneaux locaux, et on note $\mathfrak{m}_i$ leurs uniques idéaux. On a $|\mathrm{U}(\mathbb{A})| = \prod_{i=1}^{m} |\mathrm{U}(\mathbb{A}_i)|$.

Il existe donc au plus deux $\mathbb{A}_i$ tels que $|\mathrm{U}(\mathbb{A}_i)| > 1$. On distingue deux cas.

a) **Il y a deux anneaux $\mathbb{A}_i$ tels que $|\mathrm{U}(\mathbb{A}_i)| > 1$.**

Dans ce cas, alors, pour l'un d'entre eux on a $|\mathrm{U}(\mathbb{A}_i)| = 17$.
On a $\mathbb{A}_i = \mathfrak{m}_i \sqcup \mathrm{U}(\mathbb{A}_i)$ donc $|\mathbb{A}_i| = |\mathfrak{m}_i| + |\mathrm{U}(\mathbb{A}_i)|$. Comme $|\mathfrak{m}_i|$ divise $|\mathbb{A}_i|$, on a donc $|\mathfrak{m}_i|$ divise $|\mathrm{U}(\mathbb{A}_i)|$. Donc, $|\mathfrak{m}_i| \in \{1, 17\}$.
Examinons ces deux cas.

- Si $|\mathfrak{m}_i| = 1$, alors $\mathfrak{m}$ est réduit à $\{0\}$ et $\mathbb{A}_i$ est un corps. De plus $|\mathbb{A}_i| = 18$, ce qui est impossible car 18 n'est pas une puissance entière d'un nombre premier.
- Si $|\mathfrak{m}_i| = 17$, alors $|\mathbb{A}_i| = 51$ ce qui contredit la proposition 5.

b) **Il y a un seul anneau $\mathbb{A}_i$ tel que $|\mathrm{U}(\mathbb{A}_i)| > 1$.**

Fixons cet anneau $\mathbb{A}_i$. On a $|\mathrm{U}(\mathbb{A}_i)| = 34$.

Comme précédemment, on a $|\mathbb{A}_i| = |\mathfrak{m}_i| + |\mathrm{U}(\mathbb{A}_i)|$ et l'entier $|\mathfrak{m}_i|$ divise $|\mathrm{U}(\mathbb{A}_i)|$.
Donc $|\mathfrak{m}_i| \in \{1, 2, 17, 34\}$. Examinons chacun de ces cas.

- Si $|\mathfrak{m}_i| = 1$, alors $\mathfrak{m}_i$ est réduit à $\{0\}$ et $\mathbb{A}_i$ est un corps. De plus $|\mathbb{A}_i| = 35$, ce qui est impossible car 35 n'est pas une puissance entière d'un nombre premier.
- Si $|\mathfrak{m}_i| = 2$, alors le corps $\mathbb{A}_i/\mathfrak{m}_i$ possède 18 éléments, ce qui est aussi impossible.
- Si $|\mathfrak{m}_i| = 17$ (resp. 34), alors $|\mathbb{A}_i| = 51$ (resp. 68), ce qui contredit la proposition 5.

Ainsi, un anneau fini $\mathbb{A}$ ne peut pas être tel que $|\mathrm{U}(\mathbb{A})| = 34$.

**• L'entier 34 est le plus petit entier pair qui convient.**

Notons $\varphi$ la fonction indicatrice d'Euler, et si $p$ est un nombre premier, $\mathbb{F}_{p^r}$ « le » corps à $p^r$ éléments.

Soit $n$ un entier pair tel que l'équation $\varphi(x) = n$ d'inconnue $x$ admette au moins une solution, qu'on note $m$. Dans ce cas, l'anneau $\mathbb{Z}/m\mathbb{Z}$ est tel que son groupe des inversibles possède exactement $n$ éléments.

On dit qu'un entier naturel $n$ est un anti-indicateur si l'équation $\varphi(x) = n$ d'inconnue $x$ n'admet pas de solution. Les premiers anti-indicateurs pairs sont : 14, 26, 34.

Pour trouver un entier pair $n$, tel qu'il n'existe aucun anneau fini $\mathbb{A}$ dont le groupe des inversibles $\mathrm{U}(\mathbb{A})$ possède exactement $n$ éléments, il faut nous tourner vers les anti-indicateurs.

L'entier $n = 14$ ne convient pas car $\left|\mathrm{U}\left(\mathbb{F}_{2^3} \times \mathbb{Z}/3\mathbb{Z}\right)\right| = 14$.

L'entier $n = 26$ ne convient pas non plus car $|\mathrm{U}(\mathbb{F}_{3^3})| = 26$. ***cqfd***

## 6. Anneaux artiniens, noethériens et géométrie algébrique

### 6.1. *Anneaux artiniens, noethériens*

Le théorème 1 est un cas particulier d'un théorème plus général.

**Définition.** Un anneau $\mathbf{A}$ est dit *artinien*[3] quand toute suite décroissante d'idéaux est stationnaire ; il est dit *noethérien*[4] quand toute suite croissante d'idéaux est stationnaire.

**Exercice 11.** Montrer que $\mathbf{A}$ est artinien (resp. noethérien) si, et seulement si, toute partie non vide d'idéaux de $\mathbf{A}$ admet un élément minimal (resp. maximal) pour la relation d'inclusion.

On a le résultat suivant :

**Théorème 3.** *Un anneau artinien est un produit fini d'anneaux locaux artiniens.*

Ce théorème peut se montrer en utilisant des techniques de localisation. On pourra par exemple consulter [3, Théorème 26 page 75].

Parmi les résultats intermédiaires qu'on a montrés dans le cas des anneaux finis, un certain nombre est encore vrai pour les anneaux artiniens :

- les idéaux premiers et maximaux y coïncident ;
- un anneau artinien n'a qu'un nombre fini d'idéaux maximaux : $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ ;
- il existe $q_1, \ldots, q_n$ des entiers non nuls tels que ${\mathfrak{m}_1}^{q_1} \cdots {\mathfrak{m}_n}^{q_n} = (0)$.

### 6.2. *Exemples d'anneaux locaux artiniens*

- Tout corps $k$ est un anneau local artinien.
- Si $p$ est un nombre premier et $n \in \mathbb{N}^*$, $\mathbb{Z}/p^n\mathbb{Z}$ est un anneau local artinien, d'idéal maximal $(p)$.

---

[3] Ces anneaux sont nommés d'après le mathématicien Emil Artin (1898 – 1962), qui a découvert que la condition de la chaîne descendante pour les idéaux généralise simultanément les anneaux finis et les anneaux qui sont des espaces vectoriels de dimension finie.

[4] Ces anneaux sont nommés d'après la mathématicienne Emmy Noether (1882 – 1935), et le terme d'anneau noethérien apparaît pour la première fois en 1943 sous la plume de Claude Chevalley.

– Plus généralement, tout anneau fini local est artinien.

– Si $k$ est un corps et $n \in \mathbb{N}^*$, alors ${}^{k[X]}/_{(X^n)}$ est un anneau local artinien, d'idéal maximal $(X)$.

**Exercice 12.** Soient $p$ un nombre premier et $n, m \in \mathbb{N}$, $n \geqslant 2$. L'anneau

$$\left({}^{\mathbb{Z}}/_{p^n\mathbb{Z}}\right)[X]/_{(X^m)}$$

est-il artinien ? Local ? Si oui, quel est son idéal maximal ?

### 6.3. *Géométrie algébrique (théorie des schémas)*

La théorie des schémas ([EGA1], développée par Alexandre Grothendieck et ses collaborateurs à partir de la fin des années 1950) permet de voir les anneaux comme des « espaces géométriques » : si $\mathbf{A}$ est un anneau, on lui associe son *spectre*, noté $\mathrm{Spec}\,\mathbf{A}$, qui est un « espace »[5], appelé *schéma affine*. La catégorie des anneaux (commutatifs unitaires) est équivalente à la catégorie des schémas affines. Ce dictionnaire anneaux–espaces fonctionne à merveille. Les anneaux locaux artiniens apparaissent, dans ce dictionnaire, comme les analogues algébriques des points[6].

## Références

[1] BEHBOODI M., BEYRANVAND R., *On the Structure of Commutative Rings with* $p_1^{k_1} \cdots p_n^{k_n}$, $(1 \leqslant k_i \leqslant 7)$ *Zero-Divisors*, European Journal of Pure and Applied Mathematics, Vol. 3, No. 2, 2010, 303-316.

[2] BOURBAKI N., *Éléments de Mathématique, Algèbre commutative Chapitres 1 à 4*. Masson, 1985.

[3] GOBLOT R., *Algèbre commutative. Cours et exercices résolus*, Masson 1996, ISBN 2-225-85308-8.

[4] GONZÁLEZ M. J., *On Distinguishing Local Finite Rings from Finite Rings Only by Counting Elements and Zero Divisors*, European Journal of Pure and Applied Mathematics, Vol. 7, No. 1, 2014, 109-113.

[EGA1] GROTHENDIECK, A., Éléments de géométrie algébrique. I. Le langage des schémas. *Inst. Hautes Études Sci. Publ. Math.*, (4):228, 1960.

[5] $\mathrm{Spec}\,\mathbf{A}$ est l'ensemble des idéaux premiers de $\mathbf{A}$ muni d'une topologie adéquate et d'une structure supplémentaire appelée *faisceau*.

[6] Du moins pour les espaces localement de dimension finie ; cette restriction est raisonnable : en géométrie différentielle par exemple, une variété est toujours localement de dimension finie. Algébriquement, cela veut dire que les anneaux peuvent être supposés noethériens sans trop de remords.