Anneaux eidéniens [*]

Colas Bardavid[*] et Éric Pité

11 juillet 2020

Dans ce texte, tous les anneaux considérés sont commutatifs et unitaires. Les morphismes d'anneaux $f : A \longrightarrow B$ vérifient $f(1_A) = 1_B$.

Introduction

L'exercice suivant a été donné à l'oral des ENS plusieurs années de suite [*].

Exercice 1. Soit A un anneau fini possédant $n \geqslant 2$ diviseurs de zéro, alors $|A| \leqslant n^2$.

En prolongement, dans la RMS 128-4, Jean-Denis Eiden pose la question suivante : pour $n \geqslant 2$, quels sont les anneaux A ayant exactement n diviseurs de zéro (0 inclus) et tels que $|A| = n^2$.

Cette question fut notre point de départ, elle nous a permis de visiter des contrées qui nous étaient inconnues et de découvrir que ces anneaux recellent de nombreuses propriétés remarquables, que l'on a souhaité partager avec les lecteurs.

On appellera *eidénien* les anneaux A qui satisfont la condition demandée dans la question de Jean-Denis Eiden [†].

Les techniques utilisées sont nombreuses : étude de fonctions à plusieurs variables, théorie des corps et théorie des corps finis, théorie des groupes, point de vue géométrique sur les anneaux locaux, relèvements de zéros et de factorisation « à la Hensel », résultats de perfection.

Le résultat principal

Le résultat principal est une caractérisation complète des anneaux eidéniens sous la forme du

Théorème. Un anneau A est eidénien si, et seulement si, il est isomorphe à un des deux anneaux suivants :

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

∗. Un corrigé apparait dans l'exercice 21 de la RMS 129-3. On en donne une autre forme dans la proposition 3.

†. Voir paragraphe 2.4 pour une reprise de cette définition.

- $\mathbb{Z}/p^2\mathbb{Z}[X]/(Q)$, où p est premier et $Q \in \mathbb{Z}[X]$ irréductible sur $\mathbb{Z}/p\mathbb{Z}$.
- $\mathbb{F}_{p^n}[X]/(X^2)$, où p est premier et $n \in \mathbb{N}^*$.

Pour p nombre premier, et $n \in \mathbb{N}^*$, on note $\mathbb{F}_{p^n}$ « le » corps fini de cardinal p^n. Remarquons que $\mathbb{F}_{p^n}$ est un corps de décomposition au-dessus de $\mathbb{Z}/p\mathbb{Z}$ du polynôme $X^{p^n} - X$.

Plan de l'article

▷ Dans la partie 1, on caractérise les anneaux eidéniens de la forme $\mathbb{Z}/n\mathbb{Z}$.

▷ Dans la partie 2, on donne une démonstration de l'exercice de l'ENS et on redonne une définition des anneaux eidéniens.

▷ Dans la partie 3, on prouve que les anneaux eidéniens sont locaux.

▷ Dans la partie 4, on prouve que les anneaux eidéniens sont de caractéristique p ou p^2.

▷ Dans la partie 5, on étudie les anneaux eidéniens de caractéristique p.

▷ Dans la partie 6, on étudie les anneaux eidéniens de caractéristique p^2. Pour cela on prouve un résultat de type « lemme de Hensel » pour les anneaux eidéniens, puis un lemme de décomposition et un lemme de perfection.

▷ Dans la partie 7, on fait la synthèse de ces résultats et on ouvre quelques perspectives.

1 Cas des anneaux $\mathbb{Z}/n\mathbb{Z}$

Dans cette partie, on fixe un entier $n \geqslant 2$. On s'intéresse, en guise d'échauffement, à l'anneau $\mathbb{Z}/n\mathbb{Z}$, et on détermine dans quels cas il est eidénien. Déjà, comme le cardinal d'un anneau eidénien est le carré du nombre de ses diviseurs de zéro, il faut que n soit un carré pour que $\mathbb{Z}/n\mathbb{Z}$ soit eidénien.

On note $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}$ la fonction indicatrice d'Euler et, si $k \in \mathbb{Z}$, on note $\overline{k}$ la classe de k modulo n.

Lemme 1. *On a $\varphi(n^2) = n(n-1)$ si, et seulement si, n est premier.*

Démonstration. Déjà, on sait que pour tout nombre premier p, on a $\varphi(p^2) = p(p-1)$.

Réciproquement, supposons que $\varphi(n^2) = n(n-1)$. On traite deux cas.

- Si $n = p^\alpha$, avec p premier et $\alpha > 1$, alors $\varphi(n^2) = n^2(1-n^{1-1/2\alpha}) < n(n-1)$.
- Si n s'écrit $n = ab$, avec $a, b \geqslant 2$ premiers entre eux, alors $\varphi(n^2) = \varphi(a^2)\varphi(b^2)$. De plus, on a

$$\varphi(a^2)\varphi(b^2) \leqslant (a^2-1)(b^2-1) = n^2 - (a^2+b^2) + 1.$$

Or, $a^2 + b^2 > 2ab = n$. Comme de plus $n^2 - 2n + 1 < n^2 - n$, on a

$$\varphi(n^2) < n^2 - n.$$

Par conséquent, n est premier. ***cqfd***

Lemme 2. *Soit $k \in \mathbb{Z}$. Alors,*

$$\overline{k} \text{ divise zéro dans } \mathbb{Z}/_{n\mathbb{Z}} \iff \text{pgcd}(k,n) > 1.$$

Démonstration. On raisonne par double-implication.

- On suppose que $\overline{k}$ divise zéro dans $\mathbb{Z}/_{n\mathbb{Z}}$. Soit donc $\ell \in \mathbb{Z}$ tel que

$$\begin{cases} \overline{k} \times \overline{\ell} = \overline{0} \\ \overline{\ell} \neq \overline{0}. \end{cases}$$

  Raisonnons par l'absurde et supposons $\text{pgcd}(k,n) = 1$. Dans ce cas, on sait que $\overline{k}$ est inversible dans $\mathbb{Z}/_{n\mathbb{Z}}$, et l'égalité $\overline{k} \times \overline{\ell} = \overline{0}$ entraîne alors que $\overline{\ell} = \overline{0}$, ce qui est absurde.

- Réciproquement, on suppose que $\text{pgcd}(k,n) > 1$. On pose $\ell := \dfrac{n}{\text{pgcd}(k,n)}$. Comme $\ell \in [\![1, n-1]\!]$, on a $\overline{\ell} \neq 0$. De plus, on a

$$k \times \ell = \frac{k}{\text{pgcd}(k,n)} \times n$$

  donc $\overline{k} \times \overline{\ell} = \overline{0}$. Ainsi, $\overline{k}$ divise zéro dans $\mathbb{Z}/_{n\mathbb{Z}}$. ***cqfd***

Proposition 1. *L'anneau $\mathbb{Z}/_{n\mathbb{Z}}$ est eidénien si, et seulement si, $n = p^2$ avec p est premier.*

Démonstration. Déjà, d'après le lemme 2, le nombre de diviseurs de zéro dans $\mathbb{Z}/_{n\mathbb{Z}}$ vaut $n - \varphi(n)$.

Ainsi, si p est un nombre premier, alors l'anneau $\mathbb{Z}/_{p^2\mathbb{Z}}$ possède $p^2 - p(p-1) = p$ diviseurs de zéro : il est donc eidénien.

Réciproquement, considérons l'anneau $\mathbb{Z}/_{n^2\mathbb{Z}}$. Son nombre de diviseurs de zéro est égal à $n^2 - \varphi(n^2)$. Donc, s'il est eidénien, on a $n^2 = \left(n^2 - \varphi(n^2)\right)^2$, donc $n = n^2 - \varphi(n^2)$ et donc $\varphi(n^2) = n(n-1)$. Donc n est un nombre premier d'après le lemme 1. ***cqfd***

Exercice 2. Soit l'anneau $A := \left\{ \begin{pmatrix} a & b \\ 0 & a^2 \end{pmatrix} \middle| \, a, b \in \mathbb{F}_4 \right\}$.

1. Déterminer $|A|$.
2. Déterminer le cardinal de $\left\{ x \in A \middle| \, \exists y \in A \setminus \{0_A\} : x \times y = 0_A \right\}$.
3. Conclure.

2 Définition des anneaux eidéniens

2.1 Diviseurs de zéro

Définition 1. Soit A un anneau. On note

$$\delta(A) := \left\{ x \in A \middle| \, \exists y \in A \setminus \{0_A\} : x \times y = 0_A \right\}.$$

Si $x \in \delta(A)$, on dit que x *est un diviseur de zéro.*[‡]

2.2 Les diviseurs de zéro sont exactement les non-inversibles

Voici une proposition fondamentale, qui généralise le lemme 2.

Proposition 2. *Si A est un anneau fini, alors $\delta(A) = A \setminus A^\times$.*

Démonstration. On propose deux preuves.

Première preuve. Soit $a \in A$. On note

$$\lambda_a : \begin{cases} A \longrightarrow A \\ x \longmapsto ax \end{cases} ;$$

il s'agit d'un morphisme de groupes abéliens.

- L'élément a est inversible si, et seulement si, λ_a est bijectif et donc, si, et seulement si, λ_a est injectif.
- De plus, λ_a est non injectif si, et seulement si, $\operatorname{Ker} \lambda_a \neq \{0\}$.
- Enfin, par définition, $a \in \delta(A)$ si, et seulement si, $\operatorname{Ker} \lambda_a \neq \{0\}$.

Deuxième preuve. Soit $x \in A$. Comme A est fini, soient $n, m \in \mathbb{N}$ tels que $1 < m < n$ et $x^m = x^n$. On a donc

$$(x^{n-m} - 1) \times x^m = 0.$$

Supposons que x ne soit pas un diviseur de 0 et montrons par récurrence que pour tout $k \in \mathbb{N}^*$, x^k n'est pas un diviseur de zéro.

- Soit $k \in \mathbb{N}^*$ tel que x^k n'est pas un diviseur de zéro.
- Supposons que x^{k+1} est un diviseur de zéro ; soit donc $y \in A \setminus \{0\}$ tel que
$$yx^{k+1} = 0 ;$$
on a donc $(yx^k)x = 0$. Comme x^k n'est pas un diviseur de zéro, on a $yx^k \neq 0$.
- Ceci est en contradiction avec le fait que x n'est pas un diviseur de zéro.

Ainsi, x^m n'est pas un diviseur de zéro. Donc, on a $x^{n-m} = 1$. En particulier, x est inversible. ***cqfd***

Exercice 3. Trouver un anneau A et un élément $x \in A$ qui ne soit ni inversible ni diviseur de zéro.

‡. Attention, cette terminologie n'est pas cohérente avec la définition de « a divise b dans A », puisque $\forall x \in A, x \mid 0_A$. Ainsi, si x divise 0_A, x n'est pas nécessairement un diviseur de zéro.

2.3 Une minoration du nombre de diviseurs de zéro

Reprenons le résultat de l'exercice 1, sous la forme d'une

Proposition 3. *Soit A un anneau fini. Alors,*
- *ou bien $|\delta(A)| = 1$, auquel cas A est un corps ;*
- *ou bien $|\delta(A)| \geqslant \sqrt{|A|}$, ce qui s'écrit aussi $\dfrac{|\delta(A)|}{|A|} \geqslant \dfrac{1}{\sqrt{|A|}}$.*

Démonstration. On suppose que $|\delta(A)| \neq 1$. Soit donc a un diviseur de zéro de A non nul. On considère le morphisme de groupes abéliens ℓ_a défini par

$$\ell_a : \begin{cases} A \longrightarrow (a) \\ x \longmapsto ax \end{cases}$$

où (a) est l'idéal de A engendré par a ; il est surjectif. On a ${}^{A}/_{\operatorname{Ker} \ell_a} \simeq (a)$, donc

$$|A| = |(a)| \times |\operatorname{Ker} \ell_a| .$$

Or, comme a est un diviseur de zéro, on a $(a) \subset \delta(A)$; et, comme $a \neq 0$, on a $\operatorname{Ker} \ell_a \subset \delta(A)$.

Donc, on a $|A| \leqslant |\delta(A)|^2$. ***cqfd***

Exercice 4. Montrer que $\sup\limits_{A \text{ anneau fini}} \dfrac{|\delta(A)|}{|A|} = 1$.

Exercice 5. A-t-on $\sup\limits_{A \text{ anneau local fini}} \dfrac{|\delta(A)|}{|A|} = 1$?

2.4 Définition des anneaux eidéniens

Définition 2. Un anneau A est dit *eidénien* lorsque A est fini et $|A| = |\delta(A)|^2$.

3 Les anneaux eidéniens sont locaux

Commençons cette partie par des rappels sur les anneaux locaux. On intoduit des notations qui seront beaucoup utilisées dans la suite. Enfin, on donne un exemple fondamental d'anneau local.

3.1 Anneaux locaux

3.1.1 Définition

Définition 3. Un anneau A est *local* s'il ne possède qu'un seul idéal maximal.

Exercice 6. Montrer qu'un anneau A est local si, et seulement si, $A \setminus A^\times$ est un idéal de A.

Le concept d'anneau local apparaît en premier en 1938 chez Krull [5] sous le nom de *Stellenringe*. Zariski utilise pour la première fois le terme *local ring* en 1943, [11, p. 497]. Remarquons que le nom allemand est désormais *lokaler Ring*. La justification de cette terminologie apparaitra clairement dans le paragraphe 3.1.3.

3.1.2 Notations

Soit A un anneau local.

On notera $\mathfrak{M}_A$ son unique idéal maximal. L'anneau quotient ${}^{A}/_{\mathfrak{M}_A}$ est un corps, appelé *corps résiduel de l'anneau local* A. On le notera k_A ; enfin, on notera

$$\pi_A : A \longrightarrow k_A := {}^{A}/_{\mathfrak{M}_A}$$

la projection canonique.

Si $x, y \in A$, on notera $x \equiv_{k_A} y$ si $\pi_A(x) = \pi_A(y)$, *i.e.* si $x - y \in \mathfrak{M}_A$; dans le cas contraire, on notera $x \not\equiv_{k_A} y$.

Exercice 7. Soit p un nombre premier. On note

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z} \text{ et } b \notin (p) \right\}.$$

Montrer que $\mathbb{Z}_{(p)}$ est local et que son corps résiduel est isomorphe à ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$.

Exercice 8. Soit A un anneau local. Montrer que

$$A^\times = \Big\{ x \in A \mid x \not\equiv_{k_A} 0 \Big\}.$$

3.1.3 Un exemple fondamental d'anneau local

Dans ce paragraphe, on donne un exemple d'anneau local qui est très utile (fondamental même) pour enrichir ses intuitions de tels objets. Comme les résultats qu'on y énonce ne seront pas utilisés dans la suite, on s'autorise une présentation moins formelle et détaillée que dans le reste de l'article, et on omet les preuves. Les lecteurs souhaitant plus de détails pourront se référer à [2, chap II §3, p. 103].

Soit X un espace topologique non vide et soit $a \in X$. On se place initialement sur l'anneau $A := \mathscr{C}(X, \mathbb{R})$ des fonctions continues définies sur X.

On considère ensuite « l'ensemble des fonctions continues définies au voisinage de a » ; plus précisément, on pose

$$E := \Big\{ (U, f) \mid U \text{ est voisinage de } a \text{ et } f \in \mathscr{C}(U, \mathbb{R}) \Big\},$$

qu'on munit de la relation d'équivalence définie par

$$(U, f) \sim (V, g) \iff f\big|_{U \cap V} = g\big|_{U \cap V}.$$

On note $\mathscr{O}_{X,a} := {}^{E}/_{\sim}$ l'ensemble quotient.

Les éléments de $\mathscr{O}_{X,a}$ sont appelés *germes de fonctions continues définies sur X au voisinage de a*. L'ensemble $\mathscr{O}_{X,a}$ peut être muni d'une structure d'anneau. De plus, si $f \in \mathscr{O}_{X,a}$ est un germe de fonction au voisinage de a, on peut définir la valeur de f en a, qu'on note $f(a)$. En effet, si $(U, f_U), (V, f_V) \in E$ sont deux représentants de f, alors on a $f_U(a) = f_V(a)$. On peut donc considérer l'application

$$\text{éval}_a : \begin{cases} \mathscr{O}_{X,a} \longrightarrow \mathbb{R} \\ f \longmapsto f(a). \end{cases}$$

Il s'agit d'un morphisme d'anneaux.

Proposition 4. *On note $A := \mathscr{O}_{X,a}$.*

(i) L'anneau $\mathscr{O}_{X,a}$ est local.

(ii) L'idéal maximal de $\mathscr{O}_{X,a}$ est

$$\mathfrak{M}_A = \Big\{ f \in \mathscr{O}_{X,a} \mid f(a) = 0 \Big\}.$$

(iii) Les inversibles de $\mathscr{O}_{X,a}$ sont

$$A^\times = \Big\{ f \in \mathscr{O}_{X,a} \mid f(a) \neq 0 \Big\}.$$

(iv) Le corps résiduel de $\mathscr{O}_{X,a}$ est « l'ensemble des valeurs que peut prendre $f(a)$ pour $f \in \mathscr{O}_{X,a}$ » ; autrement dit, le corps résiduel de $\mathscr{O}_{X,a}$ est (isomorphe à) $\mathbb{R}$.

(v) Modulo cette identification, le morphisme $\pi_A : A \longrightarrow k_A$ est exactement

$$éval_a : \mathscr{O}_{X,a} \longrightarrow \mathbb{R}.$$

(vi) On a

$$\forall f, g \in \mathscr{O}_{X,a}, \quad f \equiv_{k_A} g \iff f(a) = g(a).$$

Démonstration. Laissée au lecteur.

Exercice 9. Soit U un voisinage de a. Montrer que l'application

$$\begin{aligned} \mathscr{C}(U, \mathbb{R}) &\longrightarrow \mathscr{O}_{X,a} \\ f &\longmapsto \overline{(U, f)} \end{aligned}$$

est un morphisme d'anneaux, où on a noté $\overline{(U, f)}$ la classe de (U, f) dans $\mathscr{O}_{X,a}$.

3.2 Structure des anneaux locaux finis

Nous utiliserons deux résultats, précédemment montrés dans [1].

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

Proposition 5. *Si A un anneau local fini, alors $|A|$ est une puissance d'un nombre premier.*

3.3 Diviseurs de zéro dans un anneau produit

Proposition 6. *Soient A et B deux anneaux. On a :*
(i) $(A \times B)^\times = A^\times \times B^\times$;
(ii) $\delta(A \times B) = \big(\delta(A) \times B\big) \cup \big(A \times \delta(B)\big)$.

Démonstration. Soit $(a, b) \in A \times B$.
(i) Alors, d'une part, on a

$$\begin{aligned}(a,b) \in (A \times B)^\times &\iff \exists (\alpha, \beta) \in A \times B : (a,b) \times (\alpha, \beta) = (1_A, 1_B) \\ &\iff \exists (\alpha, \beta) \in A \times B : (a \times \alpha, b \times \beta) = (1_A, 1_B) \\ &\iff \big(\exists \alpha \in A : a \times \alpha = 1_A\big) \text{ et } \big(\exists \beta \in B : b \times \beta = 1_B\big) \\ &\iff a \in A^\times \text{ et } b \in \times B^\times.\end{aligned}$$

(ii) D'autre part, on a

$$\begin{aligned}(a,b) \in \delta(A \times B) &\iff (a,b) \notin (A \times B)^\times \\ &\iff (a,b) \notin A^\times \times B^\times \\ &\iff a \notin A^\times \text{ ou } b \notin B^\times \\ &\iff a \in \delta(A) \text{ ou } b \in \delta(B) \\ &\iff (a,b) \in \delta(A) \times B \ \text{ ou } \ (a,b) \in A \times \delta(B).\end{aligned}$$

cqfd

Corollaire 1. *Soient A et B deux anneaux finis. Alors, on a*

$$\frac{|\delta(A \times B)|}{|A \times B|} = \frac{|\delta(A)|}{|A|} + \frac{|\delta(B)|}{|B|} - \frac{|\delta(A)|}{|A|} \times \frac{|\delta(B)|}{|B|}.$$

Démonstration. En passant le (ii) la proposition 6 au cardinal, on obtient

$$\big|\delta(A \times B)\big| = \big|\delta(A) \times B\big| + \big|A \times \delta(B)\big| - \big|\big(\delta(A) \times B\big) \cap \big(A \times \delta(B)\big)\big|.$$

De plus, $\big(\delta(A) \times B\big) \cap \big(A \times \delta(B)\big) = \delta(A) \times \delta(B)$. Donc, on a

$$\big|\delta(A \times B)\big| = \big|\delta(A)\big| \times \big|B\big| + \big|A\big| \times \big|\delta(B)\big| - \big|\delta(A)\big| \times \big|\delta(B)\big|.$$

D'où le résultat, en divisant par $|A \times B|$. ***cqfd***

3.4 Les anneaux eidéniens sont locaux

Lemme 3. *Soient $a, b \in]0, 1]$. On note $D := [a, 1[\times [b, 1[$. On considère la fonction*

$$\varphi : \begin{cases} D \longrightarrow \mathbb{R} \\ (x, y) \longmapsto x + y - xy \end{cases}.$$

Alors, φ atteint son minimum sur D en (a, b) et uniquement en ce point.

Démonstration. Soit $(x,y) \in D$. On a

$$\begin{aligned}
\varphi(x,y) &= x + \underbrace{(1-x)}_{>0} y \\
&\geqslant x + (1-x)b && (\text{car } y \geqslant b) \\
&= b + \underbrace{(1-b)}_{>0} x \\
&\geqslant b + (1-b)a && (\text{car } x \geqslant a) \\
&= \varphi(a,b).
\end{aligned}$$

De plus, dans le calcul qui précède, les deux inégalités sont des égalités seulement si $x = a$ et $y = b$. ***cqfd***

Proposition 7. *Soient A et B deux anneaux finis non nuls qui ne sont pas des corps. Alors, $A \times B$ n'est pas eidénien.*

Démonstration. En gardant les notations du lemme 3, on a

$$\frac{|\delta(A \times B)|}{|A \times B|} = \varphi(x,y)$$

avec

$$x := \frac{|\delta(A)|}{|A|} \in \left[\frac{1}{\sqrt{|A|}}, 1\right[\quad \text{et} \quad y := \frac{|\delta(B)|}{|B|} \in \left[\frac{1}{\sqrt{|B|}}, 1\right[.$$

On note $D := \left[\frac{1}{\sqrt{|A|}}, 1\right[\times \left[\frac{1}{\sqrt{|B|}}, 1\right[$ et $m := \min_{(x,y)\in D} \varphi(x,y)$.

Si on montre que $m > \dfrac{1}{\sqrt{|A|\,|B|}}$, alors on aura montré que $A \times B$ ne peut pas être eidénien.

Or, on a les équivalences suivantes

$$\begin{aligned}
m > \frac{1}{\sqrt{|A|\,|B|}} &\iff \frac{1}{\sqrt{|A|}} + \frac{1}{\sqrt{|B|}} - \frac{1}{\sqrt{|A|\,|B|}} > \frac{1}{\sqrt{|A|\,|B|}} \\
&\iff \frac{1}{\sqrt{|A|}} + \frac{1}{\sqrt{|B|}} > \frac{2}{\sqrt{|A|\,|B|}} \\
&\iff \sqrt{|B|} + \sqrt{|A|} > 2,
\end{aligned}$$

cette dernière inégalité étant vraie car $|A| \geqslant 2$ et $|A| \geqslant B$. D'où le résultat. ***cqfd***

Proposition 8. *Soient A un anneau fini non nul et B un corps fini. Alors, $A \times B$ n'est pas eidénien.*

Démonstration. On a $\big|\delta(A\times B)\big| = \big|\delta(A)\big|\times|B|+|A|-|\delta(A)|$ car $|\delta(B)| = 1$.

- Si $|B| = 2$, alors $\big|\delta(A \times B)\big| = \big|\delta(A)\big| + |A| > \sqrt{|A|}$, donc $A \times B$ n'est pas eidénien.

- Si $|B| \geqslant 3$, alors $|B| - 1 > \sqrt{|B|}$, donc $\left|\delta(A \times B)\right| > \sqrt{|A|}\sqrt{|B|} + |A|$, et ainsi $A \times B$ n'est pas eidénien. ***cqfd***

Théorème 2. *Tout anneau eidénien est local et d'ordre une puissance paire d'un nombre premier.*

Démonstration. Soit A un anneau eidénien. D'après le théorème 1, A s'écrit comme produit fini d'anneaux locaux $\prod_{i=1}^{m} A_i$. D'après les propositions 7 et 8, on a nécessairement $m = 1$. Ainsi, A est local.

D'après la proposition 5, $|A|$ est une puissance d'un nombre premier. Comme A est eidénien, on a $|A| = \left|\delta(A)\right|^2$. Ainsi, $|A|$ est une puissance paire d'un nombre premier. ***cqfd***

4 Généralités sur les anneaux eidéniens

4.1 Systèmes de représentants

On aura besoin dans la suite de la notion suivante.

Définition 4. Soit A un anneau local. *Un système de réprésentants de k_A dans A* est une famille $(\alpha_i)_{i \in k_A}$ telle que

$$\forall i \in k_A,\ \pi_A(\alpha_i) = i.$$

On dira qu'un tel système est *normalisée* quand par ailleurs on a $\alpha_{0_{k_A}} = 0_A$ et $\alpha_{1_{k_A}} = 1_A$.

Autrement dit, un système de représentants $(\alpha_i)_{i \in k_A}$ est une application

$$\begin{aligned} k_A &\longrightarrow A \\ i &\longmapsto \alpha_i \end{aligned}$$

qui est une section de π_A. Attention, il n'y aucune raison pour qu'une telle application soit un morphisme d'anneaux ou même puisse l'être. Comme π_A est surjective, A admet toujours un système de représentants, qu'on peut si nécessaire supposer normalisé.

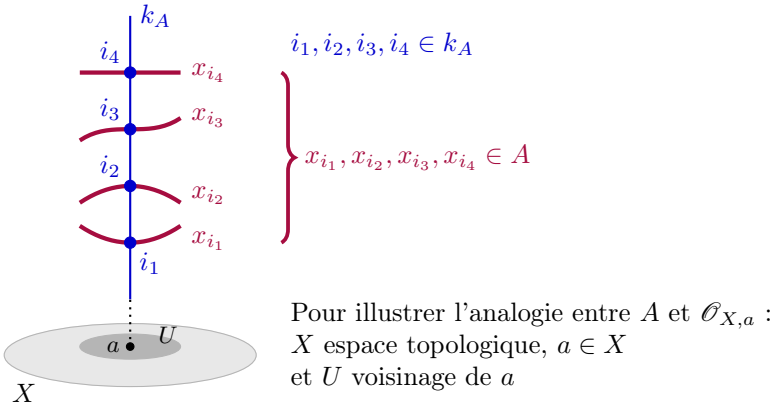

Illustration d'un système de représentants de k_A dans A

Exercice 10. Trouver un anneau local A tel qu'aucun système de représentants $k_A \longrightarrow A$ ne soit un morphisme d'anneaux.

4.2 L'idéal $\mathfrak{M}_A$ est principal et nilpotent d'ordre 2

Proposition 9. *Soit A un anneau eidénien. Alors, on a*

(i) $\mathfrak{M}_A = \delta(A)$;

(ii) $\mathfrak{M}_A$ *est un idéal principal ;*

(iii) mieux : $\forall x \in \mathfrak{M}_A \setminus \{0\}$, $\mathfrak{M}_A = (x)$;

(iv) $\forall x \in \mathfrak{M}_A$, $x^2 = 0$;

(v) mieux : $\forall x, y \in \mathfrak{M}_A$, $xy = 0$.

Démonstration. L'anneau A, étant eidénien, est local. On se donne un système de représentants $(\alpha_i)_{i \in k_A}$ de k_A dans A, qu'on suppose de plus normalisé.

(i) Cette propriété est vraie pour tout anneau local A. Par exemple, si A est local, on sait que $A = \mathfrak{M}_A \sqcup A^\times$. La proposition 2 permet alors de conclure.

(iii) On démontre directement (iii) dont (ii) est une conséquence immédiate. D'après le théorème 2, soient p premier et $n \in \mathbb{N}^*$ tels que $|A| = p^{2n}$. Comme A est eidénien, on sait que $|\mathfrak{M}_A| = |\delta(A)| = p^n$. On a donc

$$|k_A| = \frac{|A|}{|\mathfrak{M}_A|} = \frac{p^{2n}}{p^n} = p^n.$$

Soit maintenant $x \in \mathfrak{M}_A$ tel que $x \neq 0$. On a

$$\Big\{\alpha_i \times x \mid i \in k_A\Big\} \subset (x) \subset \mathfrak{M}_A.$$

Montrons que l'application

$$m : \begin{cases} k_A \longrightarrow (x) \\ i \longmapsto \alpha_i \times x \end{cases}$$

est injective. Soient $i, j \in k_A$ tels que $i \neq j$. Alors, $\alpha_i - \alpha_j$ est inversible. En effet, on a $\pi_A(\alpha_i - \alpha_j) = i - j \neq 0$; donc, $\alpha_i - \alpha_j \notin \mathfrak{M}_A$; d'après la proposition 2, on a donc $\alpha_i - \alpha_j \in A^\times$. Donc, $(\alpha_i - \alpha_j) \times x \neq 0$: l'application m est injective.
Donc, $\left\{\alpha_i \times x \mid i \in k_A\right\}$ est de cardinal p^n. Ainsi, on a

$$\left\{\alpha_i \times x \mid i \in k_A\right\} = (x) = \mathfrak{M}_A.$$

(v) On démontre directement (v) dont (iv) est une conséquence immédiate.
Soient $x, y \in \mathfrak{M}_A$, on a $xy \in (x)$. D'après ce qui précède, soit donc $i \in k_A$ tel que $xy = \alpha_i \times x$. On a $x(y - \alpha_i) = 0$. Comme $x \neq 0$, on ne peut avoir $y - \alpha_i$ inversible. Donc, $y - \alpha_i \in \mathfrak{M}_A$. Ainsi, $\pi_A(y - \alpha_i) = 0$. Comme $y \in \mathfrak{M}_A$, on a $\pi_A(\alpha_i) = 0$. Donc, $i = 0_{k_A}$. Comme on a supposé notre système de représentants normalisé, on a donc $\alpha_i = 0$ et $xy = 0$. ***cqfd***

4.3 Idéaux des anneaux eidéniens

Corollaire 2. *Soit A un anneau eidénien. Alors A possède un unique idéal non trivial.*

Démonstration. Soit I un idéal non trivial de A et soit $x \in I \setminus \{0\}$. D'après la proposition 2, on a $\delta(A) = A \setminus A^\times$. Comme $I \neq A$, on a $x \notin A^\times$ et donc $x \in \delta(A)$.

Or, d'après la proposition 9, on a $\mathfrak{M}_A = \delta(A)$ et $\mathfrak{M}_A = (x)$. Donc, on a $\mathfrak{M}_A \subset I$.

Comme $\mathfrak{M}_A$ est maximal et $I \neq A$, on a $I = \mathfrak{M}_A$. ***cqfd***

4.4 Caractéristique des anneaux eidéniens

Corollaire 3. *Soit A un anneau eidénien. Alors, il existe un nombre premier p tel que A est de caractéristique p ou p^2.*

Démonstration. D'après le théorème 2, soient p et $n \in \mathbb{N}^*$ tels que $|A| = p^{2n}$.

Notons N la caractéristique de A. On a un morphisme injectif de $\mathbb{Z}/N\mathbb{Z}$ dans A. Donc, N est de la forme p^ℓ, avec $\ell \leqslant 2n$.

Comme $p^\ell = 0$, p n'est pas inversible, d'où $p \in \mathfrak{M}_A$. Donc, d'après la proposition 9, $p^2 = 0$. Ainsi, $N = p$ ou $N = p^2$. ***cqfd***

5 Anneaux eidéniens de caractéristique p

Théorème 3. *Soit A un anneau eidénien de caractéristique p première et de cardinal p^{2n}, où $n \in \mathbb{N}^*$. Alors, A est isomorphe à $\mathbb{F}_{p^n}[X]/(X^2)$.*

Démonstration. Pour faire un pas vers ce résultat, il faut déjà trouver un sous-anneau de A isomorphe à $\mathbb{F}_{p^n}$. On définit

$$L := \Big\{ x \in A \;\Big|\; x^{p^n} = x \Big\}.$$

Pour commencer, montrons que L est un corps.

- Déjà, comme A est de caractéristique p, si $x, y \in A$, on a $(x+y)^p = x^p + y^p$. Donc, L est stable par somme.
- Ensuite, si $x, y \in L$, on a $(xy)^{p^n} = x^{p^n} y^{p^n} = xy$ et donc $xy \in L$.
- Évidemment, $1 \in L$.
- Maintenant, soit $x \in L \setminus \{0\}$. Montrons que $x \in A^\times$. Si ce n'était pas le cas, d'après le (iv) de la proposition 9, on aurait $x^2 = 0$. Comme $p^n \geqslant 2$, on aurait donc $x^{p^n} = 0$, ce qui est absurde. Donc, x est inversible. Si on note $1/x$ l'inverse de x, on a alors

  $$(1/x)^{p^n} = 1/x$$

  et donc $1/x \in L$.
- Enfin, si $x \in L$, on a bien $-x \in L$. En effet, si $p \neq 2$ alors p est impair et $(-1)^{p^n} = -1$. Sinon, $p = 2$ et $-x = x$.

Montrons maintenant que L est de cardinal p^n. On sait que k_A est de cardinal p^n ; rappelons que l'on dispose de $\pi_A : A \longrightarrow k_A$.

- En composant l'inclusion $L \subset A$ par π_A, on obtient un morphisme d'anneaux $L \longrightarrow k_A$. Comme L est un corps et k_A est non nul, ce morphisme est injectif. Donc, $|L| \leqslant p^n$.
- Montrons que ce morphisme $L \longrightarrow k_A$ est surjectif. Soit $i \in k_A$ et soit $x_i \in A$ tel que $\pi_A(x_i) = i$. On a

  $$\begin{aligned} \pi_A\Big((x_i)^{p^n}\Big) &= i^{p^n} \\ &= i && (\text{car } \forall a \in k_A,\ a^{p^n} = a) \\ &= \pi_A(x_i). \end{aligned}$$

  Donc, $(x_i)^{p^n} \equiv_{k_A} x_i$. Soit donc $\delta_i \in \mathfrak{M}_A$ tel que

  $$(x_i)^{p^n} = x_i + \delta_i.$$

  On a

  $$\begin{aligned} (x_i + \delta_i)^{p^n} &= (x_i)^{p^n} + (\delta_i)^{p^n} && (\text{car } A \text{ est de caractéristique } p) \\ &= (x_i)^{p^n} && (\text{car } {\delta_i}^2 = 0 \text{ d'après la proposition 9}) \\ &= x_i + \delta_i. && (\text{par définition de } \delta_i) \end{aligned}$$

  Donc, $x_i + \delta_i \in L$. De plus, $\pi_A(x_i + \delta_i) = i$. Donc, $L \longrightarrow k_A$ est surjectif.
- Ainsi, on a bien $|L| = p^n$.

- Donc L est isomorphe à $\mathbb{F}_{p^n}$.

Enfin, montrons le résultat principal. Soit $x \in \delta(A)$ tel que $x \neq 0$. On considère le morphisme d'anneaux

$$\text{éval}_x : L[X] \longrightarrow A$$

induit par l'inclusion $L \subset A$ et défini par $\text{éval}_x(X) = x$. Comme $x^2 = 0$, on a

$$(X^2) \subset \text{Ker}(\text{éval}_x).$$

Comme $x \neq 0$, on a $\text{Ker}(\text{éval}_x) \neq (X)$. Donc, $\text{Ker}(\text{éval}_x) = (X^2)$ et éval_x induit un morphisme

$$\varphi : {}^{L[X]}/_{(X^2)} \longrightarrow A$$

qui est injectif. Or, l'anneau ${}^{L[X]}/_{(X^2)}$ est de cardinal $(p^n)^2$. En effet, pout tout élément y de ${}^{L[X]}/_{(X^2)}$, il existe un unique $\alpha \in L$ et un unique $\beta \in L$ tels que y égale $\alpha + \beta X$ modulo (X^2). Ainsi, φ est une injection entre deux anneaux finis de même cardinal.

Donc, A est isomorphe à ${}^{L[X]}/_{(X^2)}$, lui-même isomorphe à ${}^{\mathbb{F}_{p^n}[X]}/_{(X^2)}$. ***cqfd***

6 Anneaux eidéniens de caractéristique p^2

Commençons par trois lemmes qui nous seront utiles.

6.1 Un lemme de Hensel pour les anneaux eidéniens

Lemme 4. *Soit A un anneau eidénien et soit $P \in A[X]$.*

Soit $a \in A$ tel que

$$\begin{cases} P(a) \equiv 0 \\ P'(a) \not\equiv 0. \end{cases}$$

Alors, il existe $\alpha \in A$ tel que $P(\alpha) = 0$ et $a \equiv \alpha$.

Démonstration. Commençons par remarquer que

$$\forall k \in \mathbb{N},\ \forall \delta \in \mathfrak{M}_A,\ \ (a+\delta)^k = a^k + k a^{k-1}\delta.$$

En effet, rappelons que d'après la proposition 9, on a $\forall \delta \in \mathfrak{M}_A, \delta^2 = 0$. Ainsi, on a

$$\forall \delta \in \mathfrak{M}_A,\ \ P(a+\delta) = P(a) + P'(a) \times \delta.$$

Ici, on a fait l'hypothèse que $P'(a) \not\equiv 0$; autrement dit, $P'(a) \notin \mathfrak{M}_A$. D'après, la proposition 2, on a donc $P'(a) \in A^\times$. Notons $\dfrac{1}{P'(a)}$ l'inverse dans A de $P'(a)$. On a alors

$$\begin{aligned} P\left(a - \frac{P(a)}{P'(a)}\right) &= P(a) - P'(a) \times \frac{P(a)}{P'(a)} \\ &= 0. \end{aligned}$$

De plus, comme $P(a) \in \mathfrak{M}_A$, on a également $\dfrac{P(a)}{P'(a)} \in \mathfrak{M}_A$ et donc

$$a - \frac{P(a)}{P'(a)} \equiv a.$$

Ainsi, $\alpha := a - \dfrac{P(a)}{P'(a)}$ convient. ***cqfd***

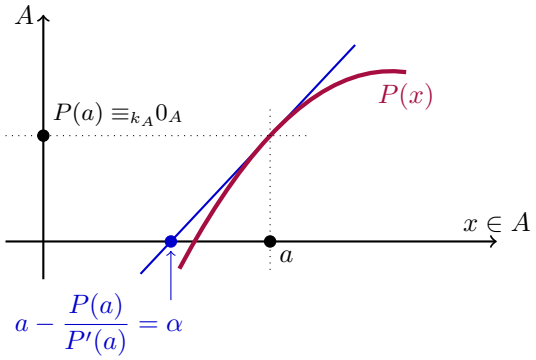

Illustration de la preuve : il s'agit d'une version algébrique de la méthode de Newton.

Remarque. Ce lemme est dans la même veine que le lemme de Hensel, voir [7, II §2 p. 42], dont voici une version, qu'on laisse en exercice. Les lecteurs intéressés par une formulation plus générale pourront consulter [2, chap. III §4, p. 259].

Exercice 11. Soit $P \in \mathbb{Z}[X]$. Soient p un nombre premier et $N \in \mathbb{N}^*$. Soit $a \in \mathbb{Z}$ tel que

$$\begin{cases} P(a) \equiv 0 \quad (p^N) \\ P'(a) \not\equiv 0 \quad (p^N). \end{cases}$$

Alors, il existe $\alpha \in \mathbb{Z}$ tel que

$$P(\alpha) \equiv 0 \ \ (p^{N+1}) \quad \text{et} \quad \alpha \equiv a \ \ (p^{N+1}).$$

6.2 Un lemme de décomposition

Lemme 5. *Soit A un anneau eidénien de caractéristique p^2 et soit $(\alpha_i)_{i \in k_A}$ un système de représentants de k_A dans A. Alors,*

$$A = \Big\{ \alpha_i + p\alpha_j \mid i, j \in k_A \Big\}.$$

Mieux, il y a unicité ; on a : $\forall x \in A,\ \exists!(i,j) \in k_A \times k_A :\ x = \alpha_i + p\alpha_j$.

Démonstration. On considère l'application

$$\varphi : \begin{cases} k_A \times k_A \longrightarrow A \\ (i,j) \longmapsto \alpha_i + p\alpha_j \end{cases} .$$

Montrons qu'elle est injective. Soient $i, i', j, j' \in k_A$ tels que

$$\alpha_i + p\alpha_j = \alpha_{i'} + p\alpha_{j'}.$$

On a donc $\alpha_i - \alpha_{i'} = p\,(\alpha_{j'} - \alpha_j)$ et donc $\alpha_i \equiv_{k_A} \alpha_{i'}$ et donc $i = i'$. On a donc

$$p\,(\alpha_{j'} - \alpha_j) = 0.$$

Supposons $j \neq j'$. On a donc $\alpha_{j'} - \alpha_j \not\equiv_{k_A} 0$ et donc $\alpha_{j'} - \alpha_j \in A^\times$. Donc, on a $p = 0$, ce qui est absurde. Donc, $j = j'$.

Ainsi, φ est injective. Comme par ailleurs on a $|k_A \times k_A| = |A|$ car A est eidénien, φ est bijective. D'où le résultat. ***cqfd***

Exercice 12. Proposer une généralisation de ce lemme au cas des anneaux eidéniens quelconques.

6.3 Un lemme de perfection

Lemme 6. *Soit $P \in {}^{\mathbb{Z}}/_{p\mathbb{Z}}[X]$ un polynôme irréductible et soit K une extension de ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$. Alors,*

$$\forall \alpha \in K,\ \ P(\alpha) = 0 \implies P'(\alpha) \neq 0.$$

Démonstration. Déjà, montrons que $P' \neq 0$. En effet, si P' était nul, alors P pourrait s'écrire

$$P = \sum_{i=0}^{N} a_i X^{ip}$$

où $N := \deg P$ et où $\forall i,\ a_i \in {}^{\mathbb{Z}}/_{p\mathbb{Z}}$. Or, $\forall x \in {}^{\mathbb{Z}}/_{p\mathbb{Z}},\ x^p = x$. Donc, on pourrait écrire

$$\begin{aligned} P &= \sum_{i=0}^{N} a_i (X^i)^p = \sum_{i=0}^{N} (a_k)^p (X^i)^p \\ &= \sum_{i=0}^{N} (a_i X^i)^p = \left(\sum_{i=0}^{N} a_i X^i \right)^p , \end{aligned}$$

ce qui contredirait l'irréductibilité de P.

Par conséquent, le pgcd de P et P' vaut 1. Soit maintenant $\alpha \in K$. Si on avait $P'(\alpha) = 0$, alors on aurait à la fois

$$(X - \alpha) \mid P \quad \text{et} \quad (X - \alpha) \mid P'.$$

C'est absurde car on aurait alors $(X - \alpha) \mid \text{pgcd}(P, P')$. Donc, $P'(\alpha) = 0$. ***cqfd***

Remarque. Voici un exemple de polynôme irréductible dont les racines ne sont pas simples (et donc la dérivée est nulle). On se place sur le corps $k := \mathbb{Z}/p\mathbb{Z}(t)$ des fractions rationnelles et on considère le polynôme $P := X^p - t$. Sa dérivée est nulle et, si $k \to K$ est une extension de k où $\theta \in K$ est une racine de P, on a

$$P = (X - \theta)^p.$$

Exercice 13. Montrer que le polynôme P défini ci-dessus est irréductible dans $k[X]$.

Le lemme 6 est en fait lié à la notion de *corps parfait*. Le lecteur intéressé pourra consulter [4, p. 296], [6, V. §6, p. 252] ou encore [10, p. 40].

6.4 Couples compatibles

Avant d'énoncer et de démontrer le principal résultat de cette partie, introduisons une notation. Considérons les réductions modulo p^2 et modulo p sur $\mathbb{Z}$:

$$\begin{array}{ccc} & & \mathbb{Z}/p^2\mathbb{Z} \\ & \nearrow & \downarrow \\ \mathbb{Z} & & \\ & \searrow & \\ & & \mathbb{Z}/p\mathbb{Z}\ ; \end{array}$$

elles s'étendent naturellement aux anneaux de polynômes

$$\begin{array}{ccc} & \overset{[\cdot]_{p^2}}{\nearrow} & \mathbb{Z}/p^2\mathbb{Z}[X] \\ \mathbb{Z}[X] & & \downarrow \pi_p \\ & \underset{[\cdot]_p}{\searrow} & \\ & & \mathbb{Z}/p\mathbb{Z}[X], \end{array}$$

et ces diagrammes sont commutatifs. Dans le théorème 5, on va faire des raisonnement avec des polynômes dans $\mathbb{Z}/p\mathbb{Z}[X]$ qu'on relève en des polynômes dans $\mathbb{Z}/p^2\mathbb{Z}[X]$.

On dira qu'un couple (P, P_p) est *compatible* quand $P \in \mathbb{Z}/p^2\mathbb{Z}[X]$, $P_p \in \mathbb{Z}/p\mathbb{Z}[X]$ et

$$\pi_p(P) = P_p.$$

On notera $\mathbb{Z}_{p^2/p}[X]$ l'ensemble des couples (P, P_p) compatibles.

6.5 Classification des anneaux eidéniens de caractéristique p^2

Venons-en au résultat principal de cette partie.

Théorème 4. *Soit A un anneau eidénien de caractéristique p^2 et de cardinal p^{2n}, avec p premier et $n \in \mathbb{N}^*$. Alors, pour tout polynôme $P \in \mathbb{Z}[X]$ irréductible modulo p et de degré n,*

$$A \text{ est isomorphe à } {}^{\left(\mathbb{Z}/p^2\mathbb{Z}[X]\right)}/_{(P)}.$$

Démonstration. Soit P un polynôme irréductible modulo p et degré n. On note

$$P_{p^2} := [P]_{p^2} \quad \text{et} \quad P_p := [P]_p$$

les réductions de P modulo p^2 et p. Par hypothèse, $P_p \in {}^{\mathbb{Z}}/_{p\mathbb{Z}}[X]$ est irréductible.

Pour commencer, montrons que P_p possède une racine $x_0 \in k_A$. Comme P_p est irréductible, on sait que ${}^{\left(\mathbb{Z}/p\mathbb{Z}[X]\right)}/_{(P_p)}$ est un corps et que c'est une extension de degré n de ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$ (voir par exemple [9, III. 2.] ou [3, §9.3]). Donc, c'est un corps de cardinal p^n, comme l'est k_A. Donc, k_A est isomorphe à ${}^{\mathbb{Z}}/_{p\mathbb{Z}}[X]/(P_p)$. Comme ce dernier est un corps où P_p possède une racine, il en est de même pour k_A. Dans la suite, on fixe donc $x_0 \in k_A$ une racine de P_p.

On relève x_0 dans A : soit $a_0 \in A$ tel que $\pi_A(a_0) = x_0$. Maintenant, d'après le lemme 6, on sait que $P'_p(x_0) \neq 0$ donc $P'_p(a_0) \not\equiv 0$. Le lemme 4 nous fournit donc un élément $\alpha_0 \in A$ tel que $P_{p^2}(\alpha_0) = 0$ et $\pi_A(\alpha_0) = x_0$: on a trouvé une racine de P_{p^2} dans A.

Considérons le morphisme d'anneaux

$$\text{éval}_{\alpha_0} : \begin{cases} {}^{\mathbb{Z}}/_{p^2\mathbb{Z}}[X] \longrightarrow A \\ \quad Q \longmapsto Q(\alpha_0) \end{cases}$$

et montrons qu'il est surjectif.

Soit $i \in k_A$. On sait que $k_A = {}^{\mathbb{Z}}/_{p\mathbb{Z}}[x_0]$. Soit donc $(R^{[i]}, R_p^{[i]}) \in \mathbb{Z}_{p^2/p}[X]$ tel que $R_p^{[i]}(x_0) = i$. Notons $\beta_i := R^{[i]}(\alpha_0)$. On a alors

$$\pi_A(\beta_i) = \pi_A\left(R^{[i]}(\alpha_0)\right) = R_p^{[i]}(x_0) = i.$$

Autrement dit $(\beta_i)_{i \in k_A}$ est un sytème de représentants de k_A dans A.

Soit maintenant $\beta \in A$. D'après le lemme 5, soient $i, j \in k_A$ tels que $\beta = \beta_i + p\beta_j$. On a alors

$$\text{éval}_{\alpha_0}\left(R^{[i]} + pR^{[j]}\right) = R^{[i]}(\alpha_0) + pR^{[j]}(\alpha_0) = \beta_i + p\beta_j = \beta.$$

Ainsi, éval_{α_0} est surjectif. Par conséquent, on a

$$A \simeq {}^{\left(\mathbb{Z}/p^2\mathbb{Z}[X]\right)}/_{\text{Ker}(\text{éval}_{\alpha_0})}.$$

Pour terminer cette preuve, montrons que $\text{Ker}(\text{éval}_{\alpha_0}) = (P_{p^2})$.

- Déjà, on a $(P_{p^2}) \subset \text{Ker}(\text{éval}_{\alpha_0})$, puisque $P_{p^2}(\alpha_0) = 0$, par définition.

- Réciproquement, soit $(Q, Q_p) \in \mathbb{Z}_{p^2/p}[X]$ tel que $Q \in \mathrm{Ker}(\mathrm{éval}_{\alpha_0})$. On veut montrer que $Q \in (P_{p^2})$.
  On a $Q_p(x_0) = 0$. Donc, $Q_p \in (P_p)$. Soit donc $(T, T_p) \in \mathbb{Z}_{p^2/p}[X]$ tel que

$$Q_p = P_p \times T_p.$$

  On peut donc trouver $U \in {}^{\mathbb{Z}}/_{p^2\mathbb{Z}}[X]$ tel que

$$Q = P_{p^2} \times T + pU \tag{1}$$

  et qu'on inclut dans un couple $(U, U_p) \in \mathbb{Z}_{p^2/p}[X]$. En évaluant cette égalité en α_0, on obtient $p \times U(\alpha_0) = 0$. Donc, comme $p \neq 0$, on a $U(\alpha_0) \notin A^\times$. Donc $U_p(x_0) = 0$. Donc, $U_p \in (P_p)$ et on recommence. Soit $(R, R_p) \in \mathbb{Z}_{p^2/p}[X]$ tel que $U_p = P_p \times R_p$. On peut donc trouver $V \in {}^{\mathbb{Z}}/_{p^2\mathbb{Z}}[X]$ tel que

$$U = P_{p^2} \times R + pV. \tag{2}$$

  En combinant (1) et (2), on obtient :

$$\begin{aligned} Q &= P_{p^2} \times T + p\left(P \times R + pV\right) \\ &= P_{p^2} \times (T + pR) + p^2 V \\ &= P_{p^2} \times (T + pR), \end{aligned}$$

  puisque $p^2 = 0$. Ainsi, $Q \in (P_{p^2})$. ***cqfd***

Remarque. On sait que si K un corps fini. Alors, $(K^\times, \times)$ est un groupe cyclique : c'est un exercice classique.

Fixons $n \in \mathbb{N}^*$. Ainsi, le groupe $(\mathbb{F}_{p^n}^\times, \times)$ est un groupe cyclique. Si x_0 est un générateur de ce groupe, on peut vérifier que le polynôme minimal de x_0 au-dessus de ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$ est irréductible et de degré n.

Cela prouve donc l'existence d'un tel polynôme d'un polynôme irréductible dans ${}^{\mathbb{Z}}/_{p\mathbb{Z}}[X]$ de degré n.

Remarque. C'est aussi un exercice classique de montrer que l'ensemble des polynômes irréductibles unitaires de degré n de $\mathbb{F}_p$ est de cardinal $\dfrac{1}{n}\displaystyle\sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$,

où μ est la fonction de Möbius définie sur $\mathbb{N}^*$ par

$$\mu(n) = \begin{cases} 0 & \text{si } n \text{ est divisible par un carré parfait différent de 1} \\ 1 & \text{si } n \text{ est le produit d'un nombre pair de nombres premiers distincts} \\ -1 & \text{si } n \text{ est le produit d'un nombre impair de nombres premiers distincts} \end{cases}$$

En montrant que $\displaystyle\sum_{d|n,\, d\neq n} p^d < p^n$ on obtient l'existence d'un polynôme irréductible unitaire de degré n de $\mathbb{F}_p$.

7 Conclusion

7.1 Classification des anneaux eidéniens

On peut maintenant énoncer et démontrer :

Théorème 5. *Un anneau A est eidénien si, et seulement si, il est isomorphe à un des deux anneaux suivants :*

- $\left({}^{\mathbb{Z}}/_{p^2\mathbb{Z}}[X]\right)/_{(P)}$*, où p est premier et $P \in \mathbb{Z}[X]$ irréductible sur* ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$.
- ${}^{\mathbb{F}_{p^n}[X]}/_{(X^2)}$*, où p est premier et $n \in \mathbb{N}^*$.*

Démonstration. Soit A un anneau eidénien.

D'après la proposition 3, A est soit de caractéristique p ou p^2.

Si A est de caractéristique p, d'après le théorème 3, A est isomorphe à ${}^{\mathbb{F}_{p^n}[X]}/_{(X^2)}$ pour un certain entier $n \in \mathbb{N}^*$.

Si A est de caractéristique p^2, d'après le théorème 4, il existe P un polynôme irréductible sur ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$ tel que A est isomorphe à ${}^{\mathbb{Z}}/_{p^2\mathbb{Z}}[X]/_{(P)}$. ***cqfd***

Remarque. Soient $n \in \mathbb{N}^*$ et $Q \in \mathbb{Z}[X]$ un polynôme de degré n, irréductible sur ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$. Les anneaux ${}^{\mathbb{F}_{p^n}[X]}/_{(X^2)}$ et ${}^{\mathbb{Z}}/_{p^2\mathbb{Z}}[X]/_{(Q)}$ ne sont pas isomorphes. En effet :

- Déjà, l'anneau ${}^{\mathbb{F}_{p^n}[X]}/_{(X^2)}$ est de caractéristique p.
- Montrons que $\left({}^{\mathbb{Z}}/_{p^2\mathbb{Z}}[X]\right)/_{(Q)}$ est de caractéristique p^2.
  Supposons qu'il est de caractéristique p ; on a alors $p \in (Q)$, l'idéal engendré par Q dans ${}^{\mathbb{Z}}/_{p^2\mathbb{Z}}[X]$. Soient donc $R, S \in \mathbb{Z}[X]$ tels que $p = QR + p^2T$. En réduisant cette égalité modulo p, on obtient
  $$0 = QR \text{ modulo } p.$$
  Comme ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$ est intègre, on en déduit $R = 0$, modulo p. Soit donc $U \in \mathbb{Z}[X]$ tel que $R = pU$. On a :
  $$p = pQU + p^2T.$$
  En divisant par p, il vient $1 = QU + pT$ et donc
  $$1 = QU \text{ modulo } p,$$
  ce qui est absurde.

7.2 Une formulation intrinsèque

Le théorème 5 peut s'énoncer de façon intrinsèque de la façon suivante :

Théorème 6. *Soit A un anneau eidénien. Alors, il existe p un nombre premier et A_0 une $\mathbb{Z}$-algèbre finie, plate où p est non ramifié et inerte tels que*

$$A \simeq \mathbb{F}_p[X]/X^2 \otimes_{\mathbb{Z}} A_0 \quad \textit{ou} \quad A \simeq \mathbb{Z}/(p^2) \otimes_{\mathbb{Z}} A_0.$$

On dit que la $\mathbb{Z}$-algèbre A_0 est finie si A_0, est un $\mathbb{Z}$-module de type fini, *i.e.* engendré par une partie finie ; on dit qu'elle est plate si A_0, en tant que $\mathbb{Z}$-module, est plat (voir [2, Chap. I]). Pour les notions de ramifications inertes, on pourra consulter [10, Chap. V].

7.3 Quelques contre exemples

Il existe de nombreux anneaux locaux d'ordre p^{2n} et de caractéristique p ou p^2 (avec p premier) qui ne sont pas eidéniens.

Exercice 14. Montrer que les anneaux suivants ne sont pas eidéniens

- $\left(\mathbb{Z}/4\mathbb{Z}[X]\right)/(X^2+a)$, pour tout $a \in [\![0,3]\!]$.
- $\left(\mathbb{Z}/2\mathbb{Z}[X]\right)/(X^2)$.

Pour une liste exhaustive des anneaux locaux d'ordre p^n, avec $p \in \{2,3,5,7\}$ et $n \in [\![1,5]\!]$, à isomorphisme près, on pourra consulter [8].

7.4 Perspectives

On a vu — c'est l'un des premiers résultats qu'on a établi — que si A est un anneau eidénien, alors

$$\forall x \in \delta(A),\ x^2 = 0. \qquad (*)$$

On a d'abord pensé qu'il pouvait s'agir là d'une caractérisation des anneaux eidéniens. Malheursement, ce n'est pas le cas. Par exemple, l'anneau

$$A := \left(\mathbb{Z}/p^2\mathbb{Z}[X]\right)/(pX, X^2)$$

vérifie $(*)$ mais n'est pas eidénien. Cependant, les anneaux vérifiant $(*)$ sont locaux. On peut naturellement chercher à caractériser les anneaux finis vérifiant $(*)$. En prolongement de cette question, on peut vouloir s'intéresser aux anneaux finis tels que, pour $p \in \mathbb{N}$ fixé : $\forall x \in \delta(A),\ x^p = 0$.

Autre perspective : notre étude clôt la question des anneaux eidéniens en en donnant une caractérisation complète. Il serait intéressant de mettre en évidence d'autres familles d'anneaux finis locaux en considérant l'invariant $|\delta(A)|/|A|$. Les anneaux eidéniens sont ceux pour lesquels cet invariant est minimal. On s'attend à ce que les valeurs possibles pour cet invariant s'échelonnent de façon discrète, en un sens à préciser. Il serait intéressant d'étudier les anneaux finis tels que $|\delta(A)|/|A|$ est minimal parmi les anneaux non eidéniens, qui ne sont pas des corps et qui sont non nuls.

Références

[1] Colas Bardavid, Éric Pité, *Structures des anneaux commutatifs finis*, RMS 130 4

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

[3] Michel Demazure, *Cours d'algèbre*, Cassini, 2008

[4] Régine et Adrien Douady, *Algèbre et théories galoisiennes*, Cassini, 1999

[5] Wolfgang Krull, *Dimensionstheorie in Stellenringen.* J. Reine Angew. Math. 1938 (179) : 204

[6] Serge Lang, *Algebra*, Springer GTM, revised third edition, 2011

[7] Serge Lang, *Algebraic number theory*, Springer GTM, second edition, 2000

[8] Andrzej Nowicki, *Tables of finite commutative local rings of small orders*, `http://www-users.mat.umk.pl/~anow/ps-dvi/tab-05w.pdf`

[9] Daniel Perrin, *Cours d'algèbre*, Ellipse, 1998

[10] Pierre Samuel, *Théorie algébrique des nombres*, Hermann, 1997

[11] Oscar Zariski, *Foundations of a General Theory of Birational Correspondences*. Trans. Amer. Math. Soc. American Mathematical Society. 1943, 53 (3) : 490–542