# L'ART DU CONTRE-EXEMPLE EN THÉORIE DES ANNEAUX

GRÉGORY BERHUY

Table des matières

1. Introduction . . . . . 1
2. Un anneau non intégralement clos n'est pas principal . . . . . 5
3. Un anneau non intégralement clos n'est pas factoriel . . . . . 5
4. Un anneau non factoriel n'est pas principal . . . . . 9
Annexe A. Théorèmes d'existence d'une décomposition en irréductibles . . . . . 12

## 1. Introduction

Avant toute chose, rappelons les notions avec lesquelles nous allons travailler.

Si $A$ est un annneau intègre, un élément $\pi \in A$ est dit *irréductible* s'il est non nul, non inversible, et si, pour tous $a, b \in A$ tels que $\pi = ab$, on a $a \in A$ ou $b \in A$. Autrement dit, $\pi$ est irréductible s'il est non nul et non inversible, et si tout diviseur de $\pi$ est soit inversible, soit associé à $\pi$.

On dit qu'un élément $a \in A \setminus \{0\}$ possède une *décomposition en irréductibles* s'il existe $u \in A^\times$ et des éléments irréductibles $\pi_1, \dots, \pi_r \in A$ tels que

$$a = u\pi_1 \cdots \pi_r.$$

On dit qu'un anneau $A$ est *factoriel* s'il est intègre et s'il vérifie les deux conditions suivantes :

(1) tout $a \in A \setminus \{0\}$ possède une décomposition en irréductibles
(2) Pour tous $r, s \geq 0$, tous $u, u' \in A^\times$ et tous éléments irréductibles $\pi_1, \dots, \pi_r, \pi'_1, \dots, \pi'_s \in A$ tels que

$$u\pi_1 \cdots \pi_r = u'\pi'_1 \cdots \pi'_s,$$

*Date*: 6 mars 2024.

on a $r = s$ et il existe $\sigma \in \mathfrak{S}_r$ tel que pour tout $i \in [\![1, r]\!]$, $\pi_i$ et $\pi'_{\sigma(i)}$ sont associés.

Autrement dit, $A$ est factoriel s'il est intègre, et si tout élément de $A$ non nul possède une décomposition en irréductibles, unique à permutation et association près des facteurs.

On démontre alors l'implication

$$A \text{ principal } \Longrightarrow A \text{ factoriel.}$$

La motivation première de cet article est le constat suivant. Bien souvent, pour démontrer qu'un anneau de la forme $\mathbb{Z}[\sqrt{d}]$ n'est pas principal, on cherche plutôt à démontrer qu'il n'est pas factoriel, par exemple en exhibant un élément qui possède deux décompositions en irréductibles distinctes, ou un élément irréductible qui n'est pas premier.

Donnons un exemple concret. Soit $A = \mathbb{Z}[i\sqrt{5}]$. On commence par constater que si $z = a + ib\sqrt{5},\ a, b \in \mathbb{Z}$, alors $|z|^2 = a^2 + 5b^2 \in \mathbb{N}$. En particulier, si $b \neq 0$, alors $|z|^2 \geq 5$ si $b \neq 0$ (En effet, dans ce cas, on a $b^2 \geq 1$.)

Cela implique aisément que les éléments $z \in A$ vérifiant $|z|^2 = 1$ sont $1$ et $-1$. On a alors l'équivalence des trois propriétés suivantes :

(i) $z \in A^\times$

(ii) $|z|^2 \leq 3$

(iii) $z = \pm 1$.

En effet, si $z \in A^\times$, il existe $z' \in A$ tel que $zz' = 1$, et ainsi $|z|^2|z'|^2 = 1 \in \mathbb{N}$. Par conséquent, $|z|^2 = 1 < 5$. Si $z = a + bi\sqrt{5}$ vérifie $|z|^2 \leq 3$, alors on a $b = 0$ d'après ce qui précède. Mais alors, on obtient $a^2 = 1, 2$ ou $3$. Seul le premier cas est possible, et on a alors $z = a = \pm 1$. L'implication manquante est triviale.

On en déduit alors que les éléments $2, 3, 1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ sont irréductibles non associés deux à deux. En effet, ils sont clairement non nuls, non inversibles, et non associés deux à deux. De plus, leurs modules au carré sont respectivement $4, 9$ et $6$. Si $z = z_1 z_2$, alors un des facteurs, disons $z_1$, vérifie $|z_1|^2 \leq \dfrac{|z|^2}{2}$. Dans les trois cas, On a $|z_1|^2 < 5$, et donc $z_1 \in A$. Dans le premier et troisième cas, on a même $|z_2|^2 \leq 3$, et donc $z_1 \in A^\times$. Dans le deuxième cas, on a $|z_1|^2 \leq 4$, mais comme $|z_1|^2$ divise $|z|^2 = 9$, on a $|z_1|^2 \leq 3$ et on a encore $z_1 \in A^\times$.

En revanche, on a $6 = 2{\cdot}3 = (1+i\sqrt{5})(1-i\sqrt{5})$. Par conséquent, $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel, donc il n'est pas principal non plus. Il existe donc au moins un idéal de $\mathbb{Z}[i\sqrt{5}]$ qui n'est pas principal. Un tel exemple est donné par l'idéal $I = (2, 1 - i\sqrt{5})$.

Si $I$ était principal, engendré par $\alpha$, alors on aurait $\alpha \mid 2$ et $\alpha \mid 1-i\sqrt{5}$, et ainsi $|\alpha|^2 \mid 4$ et $|\alpha|^2 \mid 6$ dans $\mathbb{Z}$, d'où $|\alpha|^2 \mid 2$. D'après ce qui précède, $\alpha = \pm 1$ et $I = A$. À partir de là, plusieurs options sont possibles pour obtenir une contradiction : démontrer par le calcul que $I \subset \{u+vi\sqrt{5} \mid u \equiv v\ [2]\}$, et donc que $1 \notin I$, soit constater que si $1 = 2z_1+(1+i\sqrt{5})z_2$, alors $1+i\sqrt{5} = 2(1+i\sqrt{5})z_1 + 4z_2 \in 2A$, ce qui n'est pas le cas.

On est en droit de se demander d'où sort l'idéal $I$, même si on se doute que cela doit avoir un rapport étroit avec les deux décompositions de 6 ci-dessus.

Le but de ce qui suit est de démystifier ce genre d'exemples, et de proposer une démonstration unifiée du fait qu'un anneau non factoriel est non principal, en exhibant systématiquement un idéal non principal.

Tant qu'à faire, nous explorerons les liens entre factorialité et principalité avec une autre propriété, à savoir qu'un anneau factoriel (et donc en particulier, un anneau principal) est intégralement clos, dont on rappelle maintenant la définition.

**Définition 1.1.** Soit $A$ un anneau intègre, et soit $K$ son corps des fractions. On dit que $x \in K$ est *entier sur* $A$ s'il existe un polynôme $P \in A[X]$ **unitaire** tel que $P(x) = 0$.

En particulier, tout élément de $A$ est entier sur $A$.

On dit que $A$ est *intégralement clos* si les seuls éléments de $K$ qui sont entiers sur $A$ sont les éléments de $A$.

**Remarque 1.2.** On peut démontrer que l'ensemble des éléments de $K$ entiers sur $A$ est un sous-anneau de $K$ contenant $A$.

Dans la suite, nous aurons uniquement besoin d'un résultat plus faible, à savoir que si $x \in K$ est entier sur $A$, alors pour tous $u_1, u_2 \in A$, $u_1x + u_2$ est entier sur $A$.

En effet, soit $x \in K$ un élément de $K$ entier sur $A$. Il existe donc $a_0, \dots, a_{n-1} \in A$ tels que $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$. En multipliant par $u_1^n$, on obtient

$$(u_1x)^n + u_1a_{n-1}(u_1x)^{n-1} + \cdots + u_1^{n-1}a_1(u_1x) + a_0u_1^n = 0.$$

Cela se récrit $P(u_1x) = 0$, où $P \in A[X]$ est un polynôme unitaire. Mais alors, $Q = P(X - u_2)$ est un polynôme unitaire de $A[X]$ vérifiant $Q(u_1x + u_2) = 0$, et $u_1x + u_2$ est donc entier sur $A$.

Donnons maintenant une famille d'exemples d'anneaux intégralement clos. On commence par un petit lemme calculatoire.

**Lemme 1.3.** *Soit $A$ un anneau intègre, de corps des fractions $K$, et soit $x = \dfrac{a}{s} \in K$. Supposons qu'il existe un polynôme $P \in A[X]$ unitaire de degré $n \geq 1$ tel que $P(x) = 0$. Alors, $s \mid a^n$.*

*Plus précisément, si* $P = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$*, on a* $a^n = sa'$*, avec*

$$a' = -(a_{n-1}a^{n-1} + sa_{n-2}a^{n-2} + \cdots + a_1as^{n-2} + a_0s^{n-1}).$$

*Démonstration.* Il suffit de multiplier l'égalité $P(x) = 0$ par $s^n$ pour obtenir le résultat souhaité. □

On peut maintenant donner la famille d'exemples voulue.

**Exemple 1.4.** Tout anneau factoriel est intégralement clos.

En effet, soit $A$ un anneau factoriel (donc intègre), et soit $K$ son corps des fractions. Soit $x = \dfrac{a}{s} \in K$. Quitte à simplifier par un pgcd de $a$ et $s$, on peut supposer sans perte de généralité que $a$ et $s$ sont premiers entre eux (ce simple constat utilise la factorialité, d'une part pour affirmer l'existence d'un pgcd $d$ de $a$ et $s$, et d'autre part pour constater que les éléments $a'$ et $s'$ définis par $a = da'$ et $s = ds'$ sont premiers entre eux).

Supposons que $x$ soit entier sur $A$. Il existe donc un polynôme unitaire $P \in A[X]$ tel que $P(x) = 0$. Si $n \geq 1$ est le degré de $P$, le lemme 1.3 montrer que $s \mid a^n$. Comme $a$ et $s$ sont premiers entre eux, le lemme de Gauss (qui est valable car $A$ est factoriel) implique aisément que $s \mid a$. Comme $a$ et $s$ sont premiers entre eux, cela entraîne que $s$ est inversible, et donc que $x \in A$.

On a donc

$$A \text{ principal} \implies A \text{ factoriel} \implies A \text{ intégralement clos},$$

ou encore

$$A \text{ non intégralement clos} \implies A \text{ non factoriel} \implies A \text{ non principal}.$$

Dans ce qui suit, on proposera une démonstration explicite et directe de chacune des trois implications. Plus précisément, si $A$ est intègre :

(1) à partir d'un élément $x \in \mathrm{Frac}(A) \setminus A$ entier sur $A$, on construira un idéal non principal de $A$

(2) à partir d'un élément $x \in \mathrm{Frac}(A) \setminus A$ entier sur $A$, on exhibera un élément de $A$ qui n'a pas de décomposition en irréductibles, ou qui possède deux décompositions distinctes

(3) à partir d'un élément de $A$ qui n'a pas de décomposition en irréductibles, ou qui possède deux décompositions distinctes, on construira un idéal non principal de $A$.

En particulier, on s'interdira d'utiliser la négation de propriétés des anneaux factoriels ou principaux, comme par exemple l' existence d'un pgcd ou d'un ppcm, ou le fait que tout élément de irréductible est premier.

## 2. Un anneau non intégralement clos n'est pas principal

Entrons tout de suite dans le vif du sujet.

**Théorème 2.1.** *Soit $A$ un anneau intègre, de corps des fractions $K$. On suppose que $x = \frac{a}{s} \in K \setminus A$ est un élément de $K$ entier sur $A$, qui n'est pas dans $A$. Alors, l'idéal $I = (a, s)$ n'est pas principal.*

*Démonstration.* Gardons les notations de l'énoncé, et supposons que $I = (\alpha)$. Alors, il existe $u_1, u_2 \in A$ tels que $\alpha = u_1 a + u_2 s$. Ainsi, $\alpha = (u_1 x + u_2)s$. Posons $u = u_1 x + u_2 \in K$, si bien que $\alpha = us$. Comme $s \in I$, on a aussi $s = v\alpha$, avec $v \in A$, et par conséquent $s = uvs$. Par intégrité, on obtient $uv = 1$.

D'après la remarque 1.2, $u$ est entier sur $A$. Il existe donc $a_0, \dots, a_{n-1} \in A$ tels que $u^n + a_{n-1}u^{n-1} + \cdots + a_1 u + a_0 = 0$. En multipliant cette égalité par $v^{n-1}$, on obtient

$$u + a_{n-1} + a_{n-2}v + \cdots + a_0 v^{n-1} = 0.$$

Comme $v \in A$, on en déduit que $u \in A$. Mais alors, puisque $uv = 1$, on a $u \in A^\times$. Il s'ensuit que $I = usA = sA$. Mais $a \in A$, et il existe donc $w \in A$ tel que $a = ws$, ce qui se récrit $x = w \in A$, d'où une contradiction. □

**Exemple 2.2.** Soit $d \in \mathbb{Z}$. On suppose que $d \equiv 1\ [4]$ et que $d$ n'est pas un carré. Alors, l'anneau $A = \mathbb{Z}[\sqrt{d}]$ n'est pas intégralement clos. En effet, son corps des fractions est $K = \mathbb{Q}(\sqrt{d})$. Mais alors, $x = \frac{-1+\sqrt{d}}{2}$ est un élément de $K \setminus A$ vérifiant

$$x^2 + x + \frac{1-d}{4} = 0,$$

si bien que $x$ est entier sur $A$ (le fait que $x$ n'appartient pas à $A$ découle du fait que 1 et $\sqrt{d}$ sont $\mathbb{Q}$-linéairement indépendants, vu l'hypothèse sur $d$) . Par conséquent, le théorème précédent implique que l'idéal $I = (-1+\sqrt{d}, 2)$ n'est pas principal.

## 3. Un anneau non intégralement clos n'est pas factoriel

On commence par introduire une définition commode.

**Définition 3.1.** Soit $A$ un anneau intègre, de corps des fractions $K$. On dit que $\frac{a}{s} \in K^\times$ est *pseudo-réduite* s'il existe $u, u' \in A^\times$ et des éléments irréductibles $\pi_1, \dots, \pi_r, \pi'_1, \dots, \pi'_s \in A$ tels que :

(i) pour tout $i \in [\![1, r]\!]$, et pour tout $j \in [\![1, s]\!]$ , $\pi_i$ et $\pi'_j$ ne sont pas associés

(ii) on a $a = u\pi_1 \cdots \pi_r$ et $s = u'\pi'_1 \cdots \pi'_s$.

**Exemples 3.2.** Soit $A$ un anneau intègre de corps des fractions $K$.

(1) Si $A$ est factoriel, il est facile de voir que $\frac{a}{s}$ est pseudo-réduite si et seulement si elle est réduite au sens classique, i.e. si et seulement si $a$ et $s$ sont premiers entre eux.

(2) Si $A = \mathbb{Z}[i\sqrt{5}]$, la fraction $\frac{(1+i\sqrt{5})(1-i\sqrt{5})}{2\cdot 3}$ est pseudo-réduite, d'après l'exemple de l'introduction. En revanche, elle n'est pas pas réduite, puisque $(1+i\sqrt{5})(1-i\sqrt{5}) = 6 = 2\cdot 3$.

**Lemme 3.3.** *Soit $A$ un anneau intègre, de corps des fractions $K$. Soient $a, s \in A \setminus \{0\}$. Si $a$ et $s$ possèdent au moins une décomposition en irréductibles, alors il existe $\alpha, \beta \in A \setminus \{0\}$ tels que $\frac{a}{s} = \frac{\alpha}{\beta}$ et $\frac{\alpha}{\beta}$ soit pseudo-réduite.*

*Démonstration.* Pour plus de commodité, choisissons un système complet de représentants irréductibles $\mathscr{P}$ de $A$.

Par hypothèse, on peut écrire $a = u \prod_{\pi \in \mathscr{P}} \pi^{m_\pi}$ et $s = v \prod_{\pi \in \mathscr{P}} \pi^{n_\pi}$, où $u, v \in A^\times$, et où les entiers $m_\pi, n_\pi \geq 0$ sont presque tous nuls. Posons

$$\alpha = u \prod_{\pi \in \mathscr{P}, m_\pi \geq n_\pi} \pi^{m_\pi - n_\pi} \quad \text{et } \beta = v \prod_{\pi \in \mathscr{P}, m_\pi < n_\pi} \pi^{n_\pi - m_\pi}.$$

Alors, $\alpha$ et $\beta$ conviennent. □

Nous allons démontrer le théorème suivant.

**Théorème 3.4.** *Soit $A$ un anneau intègre non intégralement clos, de corps des fractions $K$. On suppose que $x = \frac{a}{s} \in K \setminus A$ est un élément de $K$ entier sur $A$, qui n'est pas dans $A$. Alors :*

(1) *soit $a$ ou $s$ n'a pas de décomposition en irréductibles*

(2) *soit on peut écrire $x = \frac{\alpha}{\beta}$, où $\frac{\alpha}{\beta}$ est pseudo-réduite.*[1]

*Si $n \geq 1$ et le degré d'un polynôme $P \in A[X]$ unitaire tel que $P(x) = 0$, écrivons $\alpha^n = \beta\gamma$, $\gamma \in A$.*[2]

*Alors, soit $\gamma$ n'a pas de décomposition en irréductibles, soit $\alpha^n$ possède au moins deux décompositions en irréductibles distinctes.*

*Démonstration.* Gardons les notations de l'énoncé. Si $a$ ou $s$ n'a pas de décomposition en irréductibles, on a fini. Supposons donc que l'on soit dans le second cas. Si $\gamma$ n'a pas de décomposition en irréductibles, on a également fini.

1. C'est possible d'après le lemme 3.3.
2. C'est possible d'après le lemme 1.3.

Écrivons $\alpha = u\pi_1 \cdots \pi_r$ et $\beta = u'\pi'_1 \cdots \pi'_s$, où $u, u' \in A^\times$, $\pi_1, \ldots, \pi_r, \pi'_1, \ldots, \pi'_s$ sont irréductibles, et aucun $\pi_i$ n'est associé à aucun $\pi'_j$. Notons que $s \geq 1$, car sinon on aurait $\beta \in A^\times$, et par suite $x \in A$.

Notons que $\alpha^n = u^n \pi_1^n \cdots \pi_r^n$, et que $\pi'_1$ n'est associé à aucun $\pi_i$. Or, $\pi'_1$ apparaît dans la décomposition de $\beta\gamma = \alpha^n$ obtenue en multipliant une décomposition de $\gamma$ avec la décomposition de $\beta$ précédente. Par conséquent, $\alpha^n$ possède donc deux décompositions en irréductibles distinctes. Ceci achève la démonstration. □

**Remarque 3.5.** L'énoncé du lemme 1.3 et la démonstration du lemme 3.3 permettent d'expliciter $\alpha, \beta$ et $\gamma$ si on le souhaite.

Le fait qu'un élément non nul puisse n'avoir aucune décomposition en irréductibles complique notoirement l'énoncé précédent. Néanmoins, il existe quelques classes d'anneaux pour lesquels une telle décomposition est assurée d'exister. C'est en particulier vrai dans les cas suivants :

(1) l'anneau $A$ peut être muni d'une application $N : A \longrightarrow \mathbb{N}$ vérifiant vérifiant les propriétés suivantes :
   (i) pour tout $a \in A$, on a $N(a) = 0$ si et seulement si $a = 0$
   (ii) pour tout $a \in A$, on a $a \in A^\times$ si et seulement si $N(a) = 1$
   (iii) pour tous $a_1, a_2 \in A$, on a $N(a_1 a_2) = N(a_1)N(a_2)$.
(2) $A = \mathbb{Z}[\sqrt{d}]$, où $d \in \mathbb{Z}$ n'est pas un carré
(3) $A$ est un anneau intègre tel que $(A, +)$ est un groupe abélien de type fini
(4) $A$ est un anneau intègre tel que tout idéal de $A$ est engendré par un nombre fini d'éléments.

Les démonstrations étant un peu techniques, elles sont reléguées à l'annexe A.

On a donc le corollaire suivant.

**Corollaire 3.6.** *Soit $A$ un anneau intègre non intégralement clos, de corps des fractions $K$. On suppose que tout élément non nul de $A$ possède au moins une décomposition en irréductibles. On suppose que $x \in K \setminus A$ est un élément de $K$ entier sur $A$, qui n'est pas dans $A$.*

*Écrivons $x = \dfrac{\alpha}{\beta}$, où $\dfrac{\alpha}{\beta}$ est pseudo-réduite. Si $n \geq 1$ est le degré d'un polynôme $P \in A[X]$ unitaire tel que $P(x) = 0$, alors $\alpha^n$ possède au moins deux décompositions en irréductibles distinctes.*

**Remarque 3.7.** Bien entendu, il se peut que $\alpha$ ou $\beta$ possède déjà au moins deux décompositions en irréductibles distinctes, mais il se peut aussi que $\alpha$ et $\beta$ possède une unique décomposition, comme nous le verrons plus loin. Par conséquent, l'énoncé du corollaire précédent

donne un exemple d'élément avec deux décompositions distinctes qui fonctionne systématiquement.

**Exemple 3.8.** Soit $d \in \mathbb{Z}$un entier. On suppose que $d$ n'est pas un carré, et que $d \equiv 1$ [4]. Soit $A = \mathbb{Z}[\sqrt{d}]$. D'après l'exemple 2.2, $A$ n'est pas intégralement clos, puisque $x = \dfrac{-1+\sqrt{d}}{2}$ est un élément de corps des fractions de $A$ qui n'est pas dans $A$.

Si $z = a + b\sqrt{d}$, posons $N(z) = |a^2 - db^2| \in \mathbb{N}$. D'après l'exemple A.3, l'application $N : A \longrightarrow \mathbb{N}$ vérifiant vérifiant les propriétés suivantes :

(i) pour tout $a \in A$, on a $N(a) = 0$ si et seulement si $a = 0$

(ii) pour tout $a \in A$, on a $a \in A^\times$ si et seulement si $N(a) = 1$

(iii) pour tous $a_1, a_2 \in A$, on a $N(a_1a_2) = N(a_1)N(a_2)$.

D'après la proposition A.1, tout élément non nul de $A$ possède au moins une décomposition en irréductibles, et tout élément de $K^\times$ peut s'écrire sous la forme d'une fraction pseudo-réduite d'après le lemme 3.3.

Montrons que $\dfrac{-1+\sqrt{d}}{2}$ est déjà pseudo-réduite. Pour cela, commençons par montrer que 2 est irréductible dans $A$.

Comme $N(2) = 4$, 2 est non nul, et non inversible. Si maintenant on peut écrire $2 = z_1z_2$, alors $4 = N(z_1)N(z_2)$ et $N(z_1) \mid 4$. Si $N(z_1) = 1$, $z_1 \in A^\times$, et si $N(z_1) = 4$, alors $N(z_2) = 1$ et $z_2 \in A^\times$. Enfin, si $N(z_1) = 2$, il existe donc $a, b \in \mathbb{Z}$ tels que $a^2 - db^2 = \pm 2$. Mais $a^2$ et $b^2$ sont congrus à 0 ou 1 modulo 4. Par hypothèse sur $d$, on a alors $a^2 - db^2 = 0, 1$ ou $-1$ modulo 4, d'où une contradiction. Par conséquent, 2 est irréductible.

Mais alors, 2 ne peut apparaître dans une décomposition de $-1+\sqrt{d}$, car sinon $\dfrac{-1+\sqrt{d}}{2}$ serait un élément de $A$.

Ainsi, $\dfrac{-1+\sqrt{d}}{2}$ est pseudo-réduite, et le corollaire 3.6 montre que $(-1+\sqrt{d})^2$ possède au moins deux décompositions distinctes.

Lorsque $d \leq -3$, on peut même montrer que $1-\sqrt{d}$ est irréductible (cf. exemple 4.3). La fraction $\dfrac{-1+\sqrt{d}}{2}$ est alors réduite au sens classique, et $-1+\sqrt{d}$ et 2 possède alors tous deux une unique décomposition en irréductibles. Tout ceci découle du fait que les seuls diviseurs d'un élément irréductible $\pi$ sont les inversibles de $A$ et les éléments associés à $\pi$.

## 4. Un anneau non factoriel n'est pas principal

Nous allons démontrer le résultat suivant.

**Théorème 4.1.** *Soit $A$ un anneau intègre, non factoriel, et soit $a \in A \setminus \{0\}$.*

(1) *Si $a$ ne possède aucune décomposition en irréductibles, il existe une suite $(a_n)_{n\geq 0}$ d'éléments de $A \setminus A^\times$ vérifiant $a_0 = a$ et $(a_n) \subsetneq (a_{n+1})$ pour tout $n \geq 0$.*

*Alors, $I = (a_n,\ n \geq 0)$ n'est pas de type fini. En particulier, il est non principal.*

(2) *Si $a$ possède au moins deux décompositions en irréductibles distinctes, écrivons*

$$a = u\pi_1 \cdots \pi_r = u'\pi'_1 \cdots \pi'_s,$$

*où $u, u' \in A^\times$, $\pi_1, \ldots, \pi_r, \pi'_1, \ldots, \pi'_s$ sont irréductibles et où au moins un des $\pi_k$ n'est associé à aucun des $\pi'_\ell$.*

*Alors, il existe $i \in [\![1, r]\!]$ et $j \in [\![1, s]\!]$ tels que l'idéal $(\pi_i, \pi'_j)$ soit non principal.*

*Démonstration.* Supposons tout d'abord que $a$ ne possède aucune décomposition en irréductibles.

Pour tout $n \geq 0$, soit $(H_n)$ la propriété suivante.

$(H_n)$ il existe $a_0, \ldots, a_n \in A \setminus A^\times$ non nuls ne possédant aucune décomposition en irréductibles et tels que $(a_0) \subsetneq (a_1) \subsetneq \cdots \subsetneq (a_n)$.

Montrons que $(H_n)$ est vraie pour tout $n \geq 0$ par récurrence.

Remarquons que $a$ n'est pas inversible, car sinon il posséderait une décomposition en irréductibles. Ainsi, on peut prendre $a_0 = a$, et $(H_0)$ est vraie.

Supposons maintenant que $(H_n)$ soit vraie, et montrons que $(H_{n+1})$ est vraie. Il reste à démontrer qu'il existe $a_{n+1} \in A \setminus A^\times$ n'admettant pas de décomposition en irréductibles et tel que $(a_n) \subsetneq (a_{n+1})$.

Par construction, $a_n$ est non nul et n'a pas de décomposition en irréductibles. En particulier, $a_n$ n'est ni inversible, ni irréductible. Il existe donc $a_{n+1}, b_{n+1} \in A \setminus A^\times$ tels que $a_n = a_{n+1}b_{n+1}$. Si $a_{n+1}$ et $b_{n+1}$ avaient tous deux une décomposition en irréductibles, $a_{n+1}$ en aurait une. Quitte à changer l'ordre des facteurs, on peut donc supposer que $a_{n+1}$ n'a pas de décomposition. On a de plus $a_n \in (a_{n+1})$, et donc $(a_n) \subset (a_{n+1})$. Si on avait égalité, on aurait $a_n = ua_{n+1}$ avec $u \in A^\times$. Par intégrité, on obtient alors la contradiction $b_{n+1} = u \in A^\times$. Par conséquent, $(a_n) \subsetneq (a_{n+1})$, et ceci achève la récurrence.

L'existence de la suite $(a_n)_{n\geq 0}$ de l'énoncé étant maintenant établie, montrons que $I = (a_n,\ n \geq 0)$ n'est pas engendré par un nombre fini

d'éléments. Dans le cas contraire, chaque générateur est combinaison $A$-linéaire d'un nombre fini de $a_k$. Il existe donc un entier $n \geq 0$ tel que chaque générateur soit une combinaison $A$-linéaire de $a_0, \ldots, a_n$. On a alors $I \subset (a_0, \ldots, a_n)$. Par construction, on a $(a_k) \subset (a_n)$ pour tout $k \in [\![0, n]\!]$. Par conséquent, $I \subset (a_n)$. Mais $a_n \in I$, et par conséquent, $(a_n) \subset I$, si bien que $I = (a_n)$. Or, $a_{n+1} \in I$, et ainsi $(a_{n+1}) \subset (a_n)$. Comme $(a_n) \subset (a_{n+1})$, on obtient la contradiction $(a_n) = (a_{n+1})$. Cela démontre (1).

Avant de continuer, notons qu'un élément inversible possède une unique décomposition en irréductibles (cela découle du fait qu'un élément inversible n'est divisible par aucun élément irréductible).

Supposons maintenant que $a$ possède au moins deux décompositions en irréductibles distinctes. On peut donc écrire

$$a = u\pi_1 \cdots \pi_r = u'b = \pi'_1 \cdots \pi'_s,$$

où $u, u' \in A^\times$ et $\pi_1, \ldots, \pi_r, \pi'_1, \ldots, \pi'_s$ sont irréductibles. D'après ce qui précède, $r, s \geq 1$.

Quitte à simplifier, on peut supposer qu'aucun $\pi_i$ n'est associé à aucune $\pi'_j$.

On commence par remarquer que si $\pi$ et $\pi'$ sont deux éléments irréductibles non associés, et si $(\pi, \pi')$ est principal, alors il existe $\alpha, \alpha' \in A$ tels que $\alpha\pi + \alpha'\pi' = 1$.

En effet, supposons que $(\pi, \pi') = (\gamma)$. Comme $\pi$ est irréductible, ses diviseurs sont soit inversibles, soit associés à $\pi$. De même, les diviseurs de $\pi'$ sont soit inversibles, soit associés à $\pi'$. Mais $\gamma \mid \pi$ et $\gamma \mid \pi'$, et ainsi $\gamma$ est nécessairement inversible, d'où $(\pi, \pi') = A$. En particulier, $1 \in (\pi, \pi')$, d'où la conclusion souhaitée.

Supposons maintenant que pour tout $j \in [\![1, s]\!]$, $(\pi_1, \pi'_j)$ soit principal. Alors, pour tout $j \in [\![1, s]\!]$, il existe $\alpha_j, \alpha'_j \in A$ tels que $\alpha_j\pi_1 + \alpha'_j\pi'_j = 1$. En faisant le produit de toutes ces égalités, on constate qu'il existe $\alpha, \alpha' \in A$ tels que $\alpha\pi_1 + \alpha'\pi'_1 \cdots \pi'_s = 1$, ce qui se récrit $\alpha\pi_1 + \alpha'(u')^{-1}a = 1$. Comme $\pi_1 \mid a$, on en déduit que $\pi_1 \mid 1$, c'est-à-dire que $\pi_1$ est inversible, d'où une contradiction. Il existe donc $j \in [\![1, s]\!]$ tel que $(\pi_1, \pi'_j)$ ne soit pas principal. □

**Remarque 4.2.** Dans le cas où $a$ n'a pas de décomposition en irréductibles, on peut légitimement se demander si l'on peut trouver un idéal de $A$ non principal qui soit de type fini.

La réponse est non, en général. Par exemple, si $\mathcal{O}$ est l'anneau des nombres complexes qui sont entiers sur $\mathbb{Z}$, alors $\mathcal{O}$ n'est pas un corps et ne possède aucun élément irréductible. En particulier, un élément non inversible ne possède aucune décomposition en irréductibles.

En effet, $\frac{1}{2} \notin \mathcal{O}$, car $\mathbb{Z}$ est intégralement clos. Si maintenant $z \in A$, un nombre complexe $w$ tel que $w^2 = z$ est aussi dans $A$, puisque si $P \in \mathbb{Z}[X]$ est un polynôme unitaire tel que $P(z) = 0$, alors $Q = P(X^2)$ est un polynôme unitaire à coefficients entiers tel que $Q(w) = 0$. Mais alors $z = w^2$, et si $z$ est non nul non inversible, il en est de même de $w$. Ainsi, un élément non inversible n'est pas irréductible.

En revanche, on peut montrer (mais c'est difficile) que tout idéal de type fini est principal. Un exemple explicite d'idéal non principal de $\mathcal{O}$ est donné par $I = (\sqrt[2^n]{2}, n \geq 0)$, d'après le théorème et ce qui précède.

**Exemple 4.3.** Soit $d \in \mathbb{Z}, d \leq -3$, et soit $A = \mathbb{Z}[\sqrt{d}]$. Montrons que $A$ n'est pas factoriel.

Si $z = a + b\sqrt{d} \in A$, on pose $N(z) = |a^2 - db^2|$. On suppose connues les propriétés de $N$ décrites dans l'exemple A.3. Puisque $d < 0$, on a en fait $N(z) = a^2 - db^2$.

De plus, si $b \neq 0$, on a $N(z) \geq -d$.

On a alors $N(z) = 1$ si et seulement si $b = 0$ et $a^2 = 1$, c'est-à-dire $z = \pm 1$. Ainsi, $A^\times = \{1\}$.

Remarquons également que si $z \in A$ vérifie $N(z) < -d$, alors $z \in \mathbb{Z}$. En effet, écrivons $z = a + b\sqrt{d}$. Alors, si $b \neq 0$, on a $N(z) \geq -d$. Par conséquent $b = 0$ et $z = a \in \mathbb{Z}$.

Montrons maintenant que $2, \sqrt{d}, 1 - \sqrt{d}$ et $1 + \sqrt{d}$ sont irréductibles. Soit $z$ un de ces quatre éléments. Notons que $N(z) = 4, -d, 1 - d$ et $1 - d$ respectivement, et que $z$ est non nul et non inversible. Si $z = z_1 z_2$, avec $z_i \in A$, alors au moins un des deux facteurs possède une norme $\leq \frac{N(z)}{2}$, disons $z_1$. Comme $d < -3$, dans les quatre cas, on a $N(z_1) < -d$ , et ainsi $z_1 \in \mathbb{Z}$. Si $z = 2$, on a alors $N(z_1) = z_1^2 \leq 2$ et donc $z_1 = \pm 1 \in A^\times$. Dans les trois autres cas, en comparant les coordonnées en $\sqrt{d}$, on obtient que $z_1 \mid 1$ dans $\mathbb{Z}$, et encore une fois, $z_1 \in A^\times$.

On a donc le résultat souhaité. Mais alors,

$$d(d-1) = 2 \cdot \frac{d(d-1)}{2} = -(\sqrt{d})^2(1 - \sqrt{d})(1 + \sqrt{d}).$$

Comme 2 est clairement non associé à $\sqrt{d}, 1 - \sqrt{d}$ ou $1 + \sqrt{d}$, $d(d-1)$ possède deux décompositions en irréductibles distinctes.

Les idéaux $I = (2, \sqrt{d})$ et $J = (2, 1 - \sqrt{d})$ sont alors parmi les candidats potentiels pour être un idéal non principal.

On va montrer que $I$ est non principal si $d$ est pair, et que $J$ est non principal si $d$ est impair.

Supposons que $d$ soit pair, et montrons que $I$ n'est pas principal. D'après la démonstration du théorème précédent, il suffit de voir qu'il n'existe pas de relation de la forme $2z + \sqrt{d}z' = 1$, avec $z, z' \in A$. Supposons au contraire qu'une telle relation existe. En multipliant par cette relation par $\sqrt{d}$ et en utilisant le fait que $d$ soit pair, on obtient une relation de la forme $2t = \sqrt{d}$ avec $t \in A$, ce qui est impossible.

Si $d$ est impair, alors il n'existe pas de relation de la forme $2z + (1 - \sqrt{d})z' = 1$, avec $z, z' \in A$. En effet, si une telle relation existait, en multipliant cette fois par $1 + \sqrt{d}$, et en utilisant le fait que $1 - d$ est pair, on obtient la contradiction $2t = 1 + \sqrt{d}$, avec $t \in A$. Ainsi, $J$ est non principal.

Notons en revanche que si $d$ est pair, alors $J$ est principal , puisque

$$\frac{d}{2}\cdot 2 + (1 + \sqrt{d})(1 - \sqrt{d}) = 1.$$

De même si $d$ est impair, $I$ est principal, puisqu'alors

$$2\cdot\frac{1-d}{2} + (\sqrt{d})^2 = 1.$$

**Remarque 4.4.** Les calculs faits dans l'exemple précédent montrent que le théorème 4.1 est optimal dans le second cas, dans le sens où l'on ne peut espérer prendre n'importe quels diviseurs $\pi_i$ et $\pi'_j$, même après simplification par les irréductibles associés deux à deux.

En effet, soit $A = \mathbb{Z}[i\sqrt{21}]$. On sait que déjà $2, i\sqrt{21}$ et $1 \pm i\sqrt{21}$ sont irréductibles et non associés deux à deux. On montre de manière analogue que $3, 7$ et $11$ sont irréductibles. Mais alors, on a

$$(-21)\cdot(-22) = 2\cdot 3\cdot 7\cdot 11 = -(i\sqrt{21})^2(-1 + i\sqrt{21})(1 + i\sqrt{21}).$$

Tous les éléments irréductibles intervenant dans ces deux décompositions sont non associés deux à deux.

En revanche, l'exemple précédent montre que $(2, 1-i\sqrt{21})$ est principal, tandis que $(2, i\sqrt{21})$ ne l'est pas.

## Annexe A. Théorèmes d'existence d'une décomposition en irréductibles

Le but de cette annexe est de démontrer l'existence d'une décomposition d'un élément non nul en produit d'éléments irréductibles et d'un inversible, sous de bonnes hypothèses.

On commence par un théorème qui généralise les propriétés de factorisation des anneaux $\mathbb{Z}$ ou $K[X]$.

**Proposition A.1.** *Soit $A$ un anneau intègre. On suppose qu'il existe une application $N : A \longrightarrow \mathbb{N}$ vérifiant les propriétés suivantes :*

*(i) pour tout $a \in A$, on a $N(a) = 0$ si et seulement si $a = 0$*

*(ii) pour tout $a \in A$, on a $a \in A^\times$ si et seulement si $N(a) = 1$*

*(iii) pour tous $a_1, a_2 \in A$, on a $N(a_1 a_2) = N(a_1)N(a_2)$.*

*Alors, tout élément $a \in A \setminus \{0\}$ possède au moins une décomposition en irréductibles .*

*Démonstration.* Si $n \geq 1$, on note $(H_n)$ la propriété suivante :

$(H_n)$ tout élément $a \in A \setminus \{0\}$ tel que $N(a) \leq n$ possède au moins une décomposition en irréductibles.

On va démontrer que $(H_n)$ est vraie pour tout $n \geq 1$ par récurrence. Soit $a \in A \setminus \{0\}$. Si $N(a) \leq 1$, la propriété (i) montre que $N(a) = 1$, et la propriété (ii) entraîne alors que $a \in A^\times$. Ainsi, $a$ possède une décomposition (prendre $r = 0$), et $(H_1)$ est vraie.

Supposons que $(H_n)$ soit vraie pour un entier $n \geq 1$, et soit $a \in A \setminus \{0\}$ vérifiant $N(a) \leq n+1$. Si $N(a) \leq n$, on applique $(H_n)$ et on a fini. Supposons maintenant que $N(a) = n+1$. En particulier, $N(a) \geq 2$ et $a$ est non nul et non inversible. Si $a$ est irréductible, on a la décomposition souhaitée. Sinon, on peut écrire $a = a_1 a_2$, où $a_1$ et $a_2$ sont non inversibles. Mais alors, $N(a) = N(a_1)N(a_2)$ par (iii), et puisque $a_1$ et $a_2$ ne sont pas inversibles, on a $N(a_i) > 1$ et par conséquent $N(a_i) \leq n$. Par hypothèse de récurrence, $a_1$ et $a_2$ possèdent chacun une décomposition en irréductibles, et donc $a = a_1 a_2$ aussi. Ainsi, $(H_{n+1})$ est vraie. Ceci achève la récurrence, et la démonstration. □

**Remarque A.2.** Lorsque $A = \mathbb{Z}$ et $N$ est la valeur absolue, on retrouve le fait que tout entier est produit de nombres premiers et de $\pm 1$. Lorsque $A = K[X]$ (où $K$ est un corps), on peut prendre $N(P) = 2^{\deg(P)}$ pour tout $P \in K[X]$, avec la convention $2^{-\infty} = 0$. On obtient alors que tout polynôme non nul est produit un élément non nul et de polynômes irréductibles.

**Exemple A.3.** Soit $d \in \mathbb{Z}$. On suppose que $d$ n'est pas un carré. Soit $A = \mathbb{Z}[\sqrt{d}]$. Si $z = a + b\sqrt{d} \in A$, on pose $N(z) = |a^2 - db^2| \in \mathbb{N}$. Alors, $N$ vérifie les hypothèses du théorème précédent. En particulier, tout élément $a \in \mathbb{Z}[\sqrt{d}]$ non nul admet au moins une décomposition en irréductibles.

En effet, puisque $d$ n'est pas un carré dans $\mathbb{Z}$ (et donc pas non plus dans $\mathbb{Q}$, comme on peut le constater facilement), on a $N(z) = 0$ si et seulement si $z = 0$. De plus, un simple calcul montre que l'on a

$$N(z_1 z_2) = N(z_1)N(z_2) \quad \text{pour tous } z_1, z_2 \in A.$$

Enfin, si $z \in A^\times$, il existe $z' \in A$ tel que $zz' = 1$. On a alors

$$N(z)N(z') = N(zz') = N(1) = 1 \in \mathbb{N}.$$

Cela implique que $N(z) = 1$. Inversement, si $z = a + b\sqrt{d} \in A$ vérifie $N(z) = 1$, alors on a

$$(a + b\sqrt{d})(a - b\sqrt{d}) = \pm 1,$$

ce qui entraîne aisément que $z$ est inversible dans $A$.

On va maintenant donner une classe d'anneaux pour lesquels l'existence d'une décomposition en irréductibles est assurée.

**Définition A.4.** Un anneau commutatif $A$ est dit *noethérien* si tout idéal de $A$ est engendré par un nombre fini d'éléments.

**Exemple A.5.** Tout anneau principal est noethérien, par définition.

**Remarque A.6.** Il existe des anneaux non noethériens. Par exemple, l'anneau $A = \bigcup_{n \geq 1} \mathbb{C}[X_1, \ldots, X_n]$ n'est pas noethérien.

En effet, l'idéal $I = (X_k,\ k \geq 1)$ n'est pas de type fini.

Supposons au contraire que $I$ soit engendré par $P_1, \ldots, P_r$. Il existe alors $n \geq 1$ tel que $P_1, \ldots, P_r \in \mathbb{C}[X_1, \ldots, X_n]$. Comme $X_{n+1} \in I$, il existe $U_1, \ldots, U_r \in A$ tels que $X_{n+1} = U_1 P_1 + \cdots U_r P_r$. Il existe alors un entier $s \geq 1$ tel que $U_1, \ldots, U_r \in \mathbb{C}[X_1, \ldots, X_s]$. Si $m = \max(s, n+1)$, on peut alors regarder cette égalité dans $\mathbb{C}[X_1, \ldots, X_m]$. Comme chaque $P_i \in I$, $P_i$ a un terme constant nul et donc $P(0, \ldots, 0) = 0$. En évaluant l'égalité précédente en $X_1 = 0, \ldots, X_n = 0, X_{n+1} = 1$ et $X_k = 0$ pour tout $n + 2 \leq k \leq s$, on obtient la contradiction $1 = 0$.

La proposition suivante nous donne des caractérisations intéressantes des anneaux noethériens.

**Proposition A.7.** *Soit $A$ un anneau commutatif. Alors, les propriétés suivantes sont équivalentes :*

(1) *l'anneau $A$ est noethérien ;*
(2) *tout suite croissante d'idéaux de $A$ est stationnaire.*

   *Autrement dit, si $(\mathfrak{a}_n)_{n \geq 0}$ est une suite d'idéaux de $A$ telle que*

$$\mathfrak{a}_n \subset \mathfrak{a}_{n+1}, \qquad \textit{pour tout } n \geq 0,$$

   *alors il existe $N \geq 0$ tel que $\mathfrak{a}_n = \mathfrak{a}_N$, pour tout $n \geq N$ ;*
(3) *toute famille non vide $\mathscr{F}$ d'idéaux de $A$ admet un élément maximal pour l'inclusion.*

   *Autrement dit, il existe $\mathfrak{a} \in \mathscr{F}$ tel que pour tout $\mathfrak{a}' \in \mathscr{F}$, on a*

$$\mathfrak{a} \subset \mathfrak{a}' \quad \Longrightarrow \quad \mathfrak{a}' = \mathfrak{a}.$$

*Démonstration.*

(1) $\Longrightarrow$ (2). Supposons que $A$ soit noethérien, et soit $(\mathfrak{a}_n)_{n\geq 0}$ une suite croissante d'idéaux de $A$. Alors, $\mathfrak{a} = \bigcup_{n\geq 0} \mathfrak{a}_n$ est un idéal de $A$. Par hypothèse, il est engendré par un nombre fini d'éléments $a_1, \ldots, a_r \in \mathfrak{a}$. Par définition, pour tout $i \in [\![1, r]\!]$, il existe $n_i \geq 0$ tel que $a_i \in \mathfrak{a}_{n_i}$. Soit $N = \max_i n_i$. Alors, $a_i \in \mathfrak{a}_N$, pour tout $i \in [\![1, r]\!]$, et puisque $a_1, \ldots, a_r$ engendrent $\mathfrak{a}$, pour tout $n \geq N$, on obtient

$$\mathfrak{a} \subset \mathfrak{a}_N \subset \mathfrak{a}_n \subset \mathfrak{a}.$$

En particulier, on a $\mathfrak{a}_n = \mathfrak{a}_N$, pour tout $n \geq N$.

(2) $\Longrightarrow$ (3). Soit $\mathscr{F}$ une famille non vide d'idéaux de $A$. Supposons que $\mathscr{F}$ n'admette pas d'élément maximal pour l'inclusion, et soit $\mathfrak{a}_0 \in \mathscr{F}$. Puisque l'idéal $\mathfrak{a}_0$ n'est pas un élément maximal pour l'inclusion, il existe $\mathfrak{a}_1 \in \mathscr{F}$ tel que $\mathfrak{a}_0 \subsetneq \mathfrak{a}_1$. De même, il existe $\mathfrak{a}_2 \in \mathscr{F}$ tel que $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2$. Par récurrence, on voit qu'il existe une famille $(\mathfrak{a}_n)_{n\geq 0}$ d'éléments de $\mathscr{F}$ telle que $\mathfrak{a}_n \subsetneq \mathfrak{a}_{n+1}$ pour tout $n \geq 0$, d'où une contradiction.

(3) $\Longrightarrow$ (1). Soit $\mathfrak{a}$ un idéal de $A$, et soit $\mathscr{F}$ la famille des idéaux de $A$ de type fini contenus dans $\mathfrak{a}$. Alors, $\mathscr{F}$ est une famille d'idéaux de $A$ non vide, puisqu'elle contient l'idéal nul. Par hypothèse, $\mathscr{F}$ possède un élément maximal $\mathfrak{a}_0$. Par construction, on a $\mathfrak{a}_0 \subset \mathfrak{a}$. Supposons l'inclusion stricte, et soit $a \in \mathfrak{a} \setminus \mathfrak{a}_0$. Alors, l'idéal de $A$ engendré par $\mathfrak{a}_0$ et $a$ est de type fini et contenu dans $\mathfrak{a}$. De plus, il contient strictement $\mathfrak{a}_0$, ce qui contredit la maximalité de $\mathfrak{a}_0$. Ainsi, $\mathfrak{a} = \mathfrak{a}_0$, et $\mathfrak{a}$ est donc de type fini. $\square$

On a alors le résultat suivant.

**Proposition A.8.** *Soit $A$ un anneau intègre noethérien. Alors, tout élément $a \in A \setminus \{0\}$ admet une décomposition en irréductibles.*

*Démonstration.* Montrons par l'absurde que tout élément non nul de $A$ possède une décomposition en irréductibles. Pour cela, posons

$$\mathscr{F} = \{(a) \mid a \in A\backslash\{0\},\ a \text{ ne possède pas de décomposition en irréductibles}\}.$$

Supposons que $\mathscr{F}$ soit non vide. La proposition A.7 implique que $\mathscr{F}$ possède un élément maximal $(a_0)$.

Alors, $a_0 \neq 0$, et $a_0$ n'est ni inversible, ni irréductible, car sinon il posséderait une décomposition en irréductibles. Il existe donc deux éléments $b$, $c \in A$ non nuls et non inversibles tels que $a_0 = bc$.

Remarquons aussi que si $b$ et $c$ possédaient une décomposition en irréductibles, alors $a_0$ en aurait une. Ainsi, un de ces deux éléments n'a pas de décomposition en irréductibles, disons $b$. Alors, $(b) \in \mathscr{F}$. D'autre part, on a aussi $(a_0) \subset (b)$. Par maximalité de $(a_0)$, on obtient alors $(a_0) = (b)$. Puisque l'anneau $A$ est intègre, on en déduit que $a_0 = bu$, avec $u \in A^\times$.

Mais alors, on a

$$bc = a_0 = bu,$$

et par intégrité, on obtient $c = u \in A^\times$, d'où une contradiction. Ainsi, $\mathscr{F}$ est vide, et donc tout élément non nul et non inversible de $A$ possède une décomposition en irréductibles. □

**Remarque A.9.** Le résultat précédent devient faux si $A$ n'est pas intègre.

En effet, $A = \mathbb{Z}/6\mathbb{Z}$ ne possède aucun élément irréductible. Cela découle du fait que les inversibles de $A$ sont $\overline{1}, \overline{3}$ et $\overline{5}$, et des égalités

$$\overline{2} = \overline{2}\cdot\overline{4},\ \overline{4} = \overline{2}\cdot\overline{2}.$$

Il existe une foultitude d'anneaux noethériens qui sont intéressants. Comme il n'est pas question de faire un cours de théorie des anneaux ici, on donne seulement une famille d'exemples. Pour ce faire, nous aurons besoin d'un résultat de théorie des groupes.

**Proposition A.10.** *Soit $G$ un groupe abélien de type fini, engendré par $r$ éléments. Alors tout sous-groupe $H$ de $G$ est aussi de type fini, et engendré par au plus $r$ éléments.*

*Démonstration.* Soit $G$ un groupe abélien de type fini, que l'on notera additivement. Soient $e_1, \dots, e_r \in G$ des générateurs de $G$.

L'application

$$\begin{array}{rccl} \pi: & \mathbb{Z}^r & \longrightarrow & G \\ & (m_1, \dots, m_r) & \longmapsto & \displaystyle\sum_{k=1}^{r} m_i\cdot e_k \end{array}$$

est un morphisme de groupes surjectif. Si $H$ est un sous-groupe de $G$, alors $\pi^{-1}(H)$ un sous-groupe de $\mathbb{Z}^r$. Si on démontre que ce sous-groupe est engendré par au plus $r$ éléments, alors $H = \pi(\pi^{-1}(H))$ sera également engendré par au plus $r$ éléments, à savoir l'image des générateurs de $\pi^{-1}(H)$ par $\pi$.

On peut donc supposer que $G = \mathbb{Z}^r$. On procède alors par récurrence sur $r$. Soit $(H_r)$ la propriété suivante :

$(H_r)$ Tout sous-groupe de $\mathbb{Z}^r$ peut être engendré par au plus $r$ éléments.

Si $r = 0$, le résultat est clair, puisque $G$ est alors nul. Supposons avoir montré $(H_r)$ pour un certain entier $r \geq 0$ et montrons que $(H_{r+1})$ est vraie.

Soit $H$ un sous-groupe de $\mathbb{Z}^{r+1}$. Pour tout $h \in H$, on écrit

$$h = (m_{1h}, \dots, m_{(r+1)h}), \quad m_{ih} \in \mathbb{Z}.$$

Soit $A = \langle m_{1h}, h \in H\rangle \subset \mathbb{Z}$. C'est un sous-groupe de $\mathbb{Z}$, donc il existe $d_1 \in \mathbb{Z}$ tel que $A = d_1\mathbb{Z}$. On a par conséquent

$$m_{1h} = d_1 m'_{1h}, \quad m'_{1h} \in \mathbb{Z}, \ \text{ pour tout } h \in H.$$

Comme $d_1 \in d_1\mathbb{Z} = A$, il existe des entiers $n_h \in \mathbb{Z}$ presque tous nuls tels que

$$d_1 = \sum_{h \in H} n_h m_{1h}.$$

Posons $y_1 = \sum_{h \in H} n_h h = (\sum_{h \in H} n_h m_{1h}, \ldots, \sum_{h \in H} n_h m_{r+1h})$. Autrement dit, $y_1$ est un élément de $H$ dont la première coordonnée est égale à $d_1$. Mais alors, on a

$$H = \langle h \in H \rangle = \langle y_1,\ h \in H \rangle = \langle y_1,\ h - m'_{1h} \cdot y_1,\ h \in H \rangle.$$

Par définition de $m'_{1h}$, la première coordonnée de $h - m'_{1h} \cdot y_1$ est nulle pour tout $h \in H$. Ainsi, le sous-groupe $\langle h - m'_{1h} \cdot y_1,\ h \in H \rangle$ est de la forme $\{0\} \times H'$, où $H'$ est un sous-groupe de $\mathbb{Z}^r$. Par hypothèse de récurrence, $H'$ peut être engendré par au plus $r$ éléments, et il en est donc de même de $\{0\} \times H'$. Mais alors, $H$ peut donc être engendré par au plus $r+1$ éléments, ce qui achève la démonstration. □

**Corollaire A.11.** *Soit $A$ un anneau commutatif. On suppose que $(A, +)$ est un groupe abélien de type fini, engendré par $r$ éléments. Alors, tout idéal de $A$ peut être engendré par au plus $r$ éléments. En particulier, $A$ est noethérien.*

*Démonstration.* Un idéal de $A$ est en particulier un sous-groupe de $(A, +)$. Il suffit donc d'appliquer la proposition précédente pour conclure. □

**Exemple A.12.** L'anneau $\mathbb{Z}[\sqrt{d}]$ vérifie bien sûr les hypothèses du résultat précédent, ce qui permet de retrouver le résultat de l'exemple A.3 comme conséquence de la proposition A.8.