et on obtient : $r-1=s-1$; quitte à renuméroter les q_i, p_i et q_i sont associés et $\alpha_i=\beta_i$ pour $i<r$. Comme on avait déjà $p_r=q_r$ et $\alpha_r=1=\beta_r$, l'unicité de la décomposition est prouvée.

Conclusion. Un anneau principal est factoriel. ◁

L'exercice suivant rappelle la définition d'un anneau euclidien, montre qu'un anneau euclidien est principal et s'intéresse aux anneaux euclidiens dans lesquels la division euclidienne est unique.

3.11. Anneaux euclidiens

A étant un anneau intègre, on dit que A est euclidien lorsqu'il existe une application $\varphi : \mathrm{A}\backslash\{0\} \longrightarrow \mathbb{N}$ telle que, pour $a \in \mathrm{A}$ et $b \in \mathrm{A}\setminus\{0\}$. il existe $(q,r) \in \mathrm{A}^2$ tel que

$$a = bq + r \text{ et } r = 0 \text{ ou } \varphi(r) < \varphi(b). \quad (*)$$

1. Donner des exemples d'anneaux euclidiens.

2. Montrer qu'un anneau euclidien est principal.

3. On suppose de plus que A n'est pas un corps et que, pour tout a et b le couple (q,r) défini par $(*)$ est unique. Montrer que A est isomorphe à l'anneau des polynômes sur un certain corps.

(**École normale supérieure**)

▷ **Solution.**

1. • On peut prendre $\mathrm{A}=\mathbb{Z}$ et $\varphi : x \longmapsto |x|$. En effet, soit $a \in \mathbb{Z}$, $b \in \mathbb{Z}\backslash\{0\}$. Si q et r désignent respectivement le quotient et le reste de la division euclidienne de a par $|b|$, on a bien

$$a = b\varepsilon q + r \text{ et } r = 0 \text{ ou } 0 \leqslant r < |b|,$$

avec $|b| = \varepsilon b$ et $\varepsilon = \pm 1$.

• L'autre exemple du cours est K[X] où K est un corps commutatif : la division euclidienne donne le couple q et r et pour l'application φ, il suffit de prendre la fonction degré.

• L'exercice 3.12 montre que l'anneau $\mathbb{Z}[i]$ des entiers de Gauss est euclidien.

2. Soit A un anneau euclidien. Par définition, A est intègre. Considérons un idéal I de A et montrons que I est principal. C'est clair si I est nul. Si $\mathrm{I} \neq \{0\}$, considérons l'ensemble $\mathrm{F} = \{\varphi(a) \in \mathbb{N}, a \in \mathrm{I}, a \neq 0\}$. C'est une partie non vide de $\mathbb{N}$, qui admet donc un plus petit élément. Il existe donc un élément a_0 non nul de I tel que $\varphi(a_0) = \min \mathrm{F}$. On a, bien entendu, $a_0\mathrm{A} \subset \mathrm{I}$.

Réciproquement, si $a \in \mathrm{I}$, il existe $(q, r) \in \mathrm{A}^2$ tel que $a = qa_0 + r$ avec $r = 0$ ou $\varphi(r) < \varphi(a_0)$. On en déduit que $r = a - a_0 q$ est dans I, puisque I est un idéal. Si r n'est pas nul, on obtient $\varphi(r) < \varphi(a_0) = \min \mathrm{F}$, ce qui est impossible. On a donc nécessairement $r = 0$ et $a = a_0 q \in a_0\mathrm{A}$. On conclut que $\mathrm{I} = a_0\mathrm{A}$: l'idéal I est principal.

On note que les exemples d'anneaux principaux les plus importants du cours sont des anneaux euclidiens. Il est assez difficile d'exhiber des anneaux principaux non euclidiens mais cela existe[2].

3. Il s'agit de sortir de notre chapeau le corps K dont A serait l'anneau des polynômes. Or, dans K[X], le corps K est composé de 0 et des éléments de degré minimal (à savoir 0). Cela nous donne une piste pour définir K : il serait constitué, outre 0, des éléments x non nuls de A, pour lesquels $\varphi(x)$ est minimal.

• Avant d'entrer dans le détail, nous allons introduire plusieurs notations et faire quelques remarques simples. A^* désigne comme d'habitude $\mathrm{A} \setminus \{0\}$ et $\mathrm{A}^\times$ l'ensemble des éléments inversibles de A. Deux éléments a et b de A sont dits associés s'il existe u inversible dans A tel que $a = bu$ (être associés est une relation d'équivalence). Enfin, si dans A, $a = bq + r$ avec $b \neq 0$, $r = 0$ ou $\varphi(r) < \varphi(b)$, on dira qu'il s'agit d'une division euclidienne de a par b. Par hypothèse, une division de a par b est unique.

Lemme. *Si a et b appartiennent à A et si $a|b$, alors $\varphi(a) \leqslant \varphi(b)$.*
Si a et b sont associés dans A^*, $\varphi(a) = \varphi(b)$.

Démonstration. En effet, si $a|b$ et si $\varphi(a) > \varphi(b)$, on a deux divisions euclidiennes de b par a : $b = a \times c + 0$ et $b = a \times 0 + b$, où $c = \dfrac{b}{a}$, ce qui est contraire à l'hypothèse. Si a et b sont associés, on a $a|b$ et $b|a$, d'où résultent les relations $\varphi(a) \leqslant \varphi(b)$ et $\varphi(b) \leqslant \varphi(a)$ et l'égalité annoncée. ◇

• Pour tout $a \in \mathrm{A}^*$, 1 divise a ; on a donc $\varphi(1) \leqslant \varphi(a)$. Il s'ensuit que $m_0 = \varphi(1) = \min \varphi$. Puisque 1 est associé à tout inversible de A, on obtient

$$\mathrm{A}^\times \subset \{x \in \mathrm{A}^*,\ \varphi(x) = m_0\}$$

Réciproquement, si $x \in \mathrm{A}^*$ et $\varphi(x) = m_0$, x est inversible. En effet, il existe q et r dans A tels que $1 = xy + r$ avec $r = 0$ ou $\varphi(r) < \varphi(x)$. Comme $\varphi(x) = m_0 = \min \varphi$, cette seconde condition est impossible, et on a $1 = xy$ et $x \in \mathrm{A}^\times$. On conclut :

$$\mathrm{A}^\times = \{x \in \mathrm{A}^*, \varphi(x) = m_0\}$$

2. PERRIN (D.), *Cours d'algèbre*, Ellipses, 1996, p. 53-54.

• Tout nous pousse à poser $K = A^\times \cup \{0\}$. Montrons que K est un corps commutatif.

⋆ Comme $K^* = A^\times$, nous savons déjà que $(K^*, \times)$ est un groupe commutatif.

Montrons que K est un sous-anneau de A.

⋆ K^* et donc K sont stables par multiplication.

⋆ $1 \in K$ et si $a \in K$, alors $-a \in K$.

⋆ Il reste à montrer la stabilité par addition. Soit a et b dans K. Si a ou b est nul, il est clair que $a + b$ est dans K. Supposons $a \neq 0$ et $b \neq 0$. Étant donné que $a + b = a(1 + a^{-1}b)$ et que K est stable par multiplication, il suffit de prouver le résultat suivant : si $u \in K^*$, alors $1 + u \in K$.

Raisonnons par l'absurde et supposons que $1 + u \notin K$. Alors, $1 + u$ est non nul, $\varphi(1 + u) > m_0 = \varphi(1) = \varphi(-u^{-1})$ et on peut écrire

$$1 = (1 + u) \times 0 + 1, \text{ mais aussi } 1 = (1 + u) \times u^{-1} + (-u^{-1}).$$

On a donc deux divisions euclidiennes de 1 par $1+u$, ce qui est contraire à l'hypothèse.

Établissons un bilan provisoire : K est corps commutatif, sous-anneau de A. Comme A n'est par un corps, $K \subsetneq A$.

• Dans $K[X]$, X est un polynôme de degré 1, *i.e.* de degré minimal parmi les polynômes non constants. Il est donc naturel de considérer ici un élément de $A \setminus K$, où φ est minimale. L'entier $m_1 = \min_{x \in A \setminus K} \varphi(x)$ est bien défini (car $A \setminus K \neq \emptyset$) et il existe $X_0 \in A \setminus K$ tel que $\varphi(X_0) = m_1$. Introduisons la fonction

$$\Psi : \begin{array}{ccc} K[X] & \longrightarrow & A \\ P & \longmapsto & P(X_0) \end{array}$$

Il s'agit d'un morphisme de K-algèbres. Montrons que Ψ est un isomorphisme.

• Prouvons l'injectivité de Ψ : montrons par récurrence sur $n \in \mathbb{N}$, que si $\deg P \leqslant n$ et $P(X_0) = 0$, alors $P = 0$.

⋆ C'est bon si $P = 0$ ou $\deg P = 0$ (car alors $P(X_0) = P \in K$).

⋆ Supposons $n \geqslant 1$ et la propriété vraie jusqu'au rang $n - 1$. Soit $P \in K[X]$ tel que $P(X_0) = 0$. En écrivant $P = a_n X^n + \cdots + a_1 X + a_0$, on obtient

$$0 = P(X_0) = (a_n X_0^{n-1} + \cdots + a_1)X_0 + a_0$$

On reconnaît là une division euclidienne de 0 par X_0. En effet soit $a_0 = 0$, soit $a_0 \in A^\times$ et $\varphi(a_0) = m_0 < \varphi(X_0) = m_1$. Puisque $0 = 0 \times X_0 + 0$, on obtient par unicité $a_0 = 0$ et $Q(X_0) = 0$ avec $Q = a_n X^{n-1} + \cdots + a_1$.

Comme $\deg Q \leqslant n-1$, par l'hypothèse de récurrence, on obtient $Q = 0$. Il en résulte que $P = 0$.

• La surjectivité est plus délicate. On veut montrer que les éléments de A sont dans $K[X_0] = \operatorname{Im}\Psi$. C'est vrai pour les éléments $x \in A^*$ tels que $\varphi(x) = m_0$: ils sont dans K. On va tenter une récurrence sur « $\varphi(x)$» que l'on pourrait diminuer par une division euclidienne par X_0. Plus précisément, montrons par récurrence sur $n \in \mathbb{N}$ que si $x \in A^*$ et $\varphi(x) \leqslant n$, alors $x \in K[X_0]$.

C'est vrai si $n \leqslant m_0$.

Supposons $n > m_0$, et la propriété vérifiée jusqu'à l'entier $n-1$. Prenons $x \in A^*$ avec $\varphi(x) \leqslant n$. On peut supposer $\varphi(x) > m_0$ *i.e.* $x \notin K$. Divisons x par X_0 : il existe q et r dans A tels que $x = X_0 q + r$ avec $r = 0$ ou $\varphi(r) < \varphi(X_0)$. Par conséquent, r appartient à K. Pour montrer que x est dans $K[X]$, il suffit de montrer que q est dans $K[X_0]$. D'après l'hypothèse de récurrence, c'est vrai si $\varphi(q) \leqslant n-1$. Or, on a $\varphi(X_0 q) = \varphi(x-r)$. Puisque $\varphi(x) \leqslant n$, l'inégalité $\varphi(q) \leqslant n-1$ va résulter des deux inégalités suivantes : $\varphi(x-r) = \varphi(x)$ et $\varphi(q) < \varphi(X_0 q)$ (ce qui est le cas lorsque φ est la fonction degré dans $K[X]$). On les déduit de deux lemmes.

Lemme. *Si $x \notin K$ et $a \in K$, alors $\varphi(x+a) = \varphi(x)$.*

Démonstration. C'est évident si $a = 0$. Sinon, a est inversible, $a + x$ est associé à $1 + a^{-1}x$ et x à $a^{-1}x$. On en déduit que

$$\varphi(a+x) = \varphi(1 + a^{-1}x) \quad \text{et} \quad \varphi(a^{-1}x) = \varphi(x).$$

On peut donc se ramener à montrer que si $u \notin K$, alors $\varphi(1+u) = \varphi(u)$. On remarque que $1+u$ n'est pas dans K, sinon u y serait (K est un corps et contient 1). On a donc $1 + u \neq 0$ et

$$1 = (1+u) \times 1 - u = (1+u) \times 0 + 1.$$

Comme $\varphi(1+u) > \varphi(1)$, on a nécessairement, par unicité de la division, $\varphi(u) \geqslant \varphi(1+u)$. En remplaçant u par $-(1+u)$, qui lui aussi n'est pas dans K, on obtient de même $\varphi(-(1+u)) \geqslant \varphi(1-(1+u))$. On a donc $\varphi(1+u) = \varphi(-(1+u)) \geqslant \varphi(-u) = \varphi(u)$. On conclut que $\varphi(1+u) = \varphi(u)$. Le lemme est prouvé. ◇

Lemme. *Si $x \neq 0$, $\varphi(xX_0) > \varphi(x)$.*

Démonstration. Raisonnons par l'absurde et supposons $\varphi(xX_0) \leqslant \varphi(x)$. Comme x divise xX_0, on a $\varphi(xX_0) \geqslant \varphi(x)$ et donc $\varphi(xX_0) = \varphi(x)$. Divisons x par $X_0 x$: il existe q et r dans A tels que

$$x = xX_0 q + r \quad \text{et} \quad r = 0 \text{ ou } \varphi(r) < \varphi(xX_0) = \varphi(x).$$

On remarque que x divise r, ce qui implique, si $r \neq 0$, que $\varphi(x) \leqslant \varphi(r)$. Cette inégalité n'est pas vérifiée. On a donc $r = 0$. On obtient alors $x = x\mathrm{X}_0 q$ et, par intégrité, $1 = \mathrm{X}_0 q$, ce qui montre que X_0 est inversible, donc dans K. C'est faux, par hypothèse. $\diamondsuit$

Résumons : $\varphi(q) < \varphi(\mathrm{X}_0 q) = \varphi(x)$ et donc $\varphi(q) \leqslant n-1$. D'après l'hypothèse de récurrence, $q \in \mathrm{K}[\mathrm{X}_0]$ et finalement $x \in \mathrm{K}[\mathrm{X}_0]$. $\lhd$

Conclusion. L'anneau $\mathrm{A} = \mathrm{K}[\mathrm{X}_0]$ est isomorphe à l'anneau des polynômes $\mathrm{K}[\mathrm{X}]$.

On retiendra des exercices précédents la chaîne d'implications : pour un anneau commutatif et intègre A,

$$\mathrm{A}\ \textit{euclidien} \Longrightarrow \mathrm{A}\ \textit{principal} \Longrightarrow \mathrm{A}\ \textit{factoriel}.$$

Nous allons, dans les deux exercices qui suivent, nous intéresser aux entiers de Gauss, exemple historiquement important, qui donne le coup d'envoi de la théorie algébrique des nombres. Le premier démontre que $\mathbb{Z}[i]$ est euclidien (donc principal et factoriel), ce qui conduit à une arithmétique proche de celle de $\mathbb{Z}$. Le lecteur aura intérêt, avant de l'aborder, à affermir ses connaissances sur les anneaux factoriels en traitant l'exercice 3.10.

3.12. Anneau des entiers de Gauss (1)

On considère l'anneau $\mathbb{Z}[i] = \{u + iv \in \mathbb{C},\ (u,v) \in \mathbb{Z}^2\}$ et l'application $\varphi : a \in \mathbb{Z}[i] \longmapsto a\overline{a} \in \mathbb{N}$.

1. Déterminer le groupe multiplicatif des éléments inversibles de $\mathbb{Z}[i]$.

2. Montrer que $\mathbb{Z}[i]$ est euclidien pour φ, c'est-à-dire que pour tout $(a,b) \in \mathbb{Z}[i] \times \mathbb{Z}[i]^*$, il existe $(q,r) \in \mathbb{Z}[i]^2$ tel que $a = bq + r$ avec $\varphi(r) < \varphi(b)$.

3. En déduire que $\mathbb{Z}[i]$ est factoriel.

4. Montrer que si $\varphi(a)$ est premier, alors a est irréductible dans $\mathbb{Z}[i]$.

5. Soit p un nombre premier. Montrer l'équivalence entre les propriétés suivantes :

(*i*) p est irréductible dans $\mathbb{Z}[i]$;

(*ii*) $p \equiv 3 \pmod 4$;

(*iii*) il n'existe pas $a \in \mathbb{Z}[i]$ tel que $p = \varphi(a)$.

On admettra que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si p n'est pas congru à 3 modulo 4.

6. En déduire tous les irréductibles de $\mathbb{Z}[i]$.

(École normale supérieure)

I · **Solution.**

1. Soit a un élément inversible de $\mathbb{Z}[i]$. Il existe b dans $\mathbb{Z}[i]$ tel que $ab = 1$. Comme φ est multiplicative, il vient $\varphi(a)\varphi(b) = 1$. L'entier naturel $\varphi(a)$ est inversible dans $\mathbb{Z}$ et donc égal à 1. Réciproquement si $\varphi(a) = 1$, alors $a\overline{a} = 1$ et $\overline{a}$, qui appartient à $\mathbb{Z}[i]$, est l'inverse de a.

Un élément $a \in \mathbb{Z}[i]$ est donc inversible si et seulement si $\varphi(a) = 1$. En posant $a = u + iv$, avec $(u, v) \in \mathbb{Z}^2$, on obtient $u^2 + v^2 = 1$. Les éléments inversibles de $\mathbb{Z}[i]$ sont donc $1, -1, i$ et $-i$: il s'agit du groupe des racines quatrième de l'unité.

2. Soit $(a, b) \in \mathbb{Z}[i] \times \mathbb{Z}[i]^*$. Considérons le nombre complexe $\dfrac{a}{b}$ qui s'écrit $\dfrac{a}{b} = x + iy$, avec $(x, y) \in \mathbb{R}^2$, u (resp. v) l'entier le plus proche de x (resp. y) et posons $q = u + iv$.

On a alors

$$\left|\frac{a}{b} - q\right|^2 = (u - x)^2 + (v - y)^2 \leqslant \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 < 1.$$

On en déduit $|a - bq|^2 < |b|^2$. Posons $r = a - bq$; a, b, q appartenant à $\mathbb{Z}[i]$, r appartient également à $\mathbb{Z}[i]$ et on a $|r|^2 < |b|^2$, c'est-à-dire $\varphi(r) < \varphi(b)$.

Nous avons déterminé $(q, r) \in \mathbb{Z}[i]^2$ tel que $a = bq + r$ et $\varphi(r) < \varphi(b)$.

Conclusion. L'anneau $\mathbb{Z}[i]$ est un anneau euclidien.

3. D'après l'exercice 3.11, $\mathbb{Z}[i]$ est un anneau principal et d'après l'exercice 3.10, il est alors factoriel.

4. Soit $a \in \mathbb{Z}[i]$ tel que $\varphi(a)$ soit premier. Supposons que a s'écrive $a = bc$, avec b et c dans $\mathbb{Z}[i]$. On a alors $\varphi(a) = \varphi(b)\varphi(c)$. L'entier $\varphi(a)$ étant premier, on en déduit que $\varphi(b) = 1$ ou $\varphi(c) = 1$, c'est-à-dire que b ou c est inversible. Donc a est irréductible.

5. Supposons (i) et montrons (ii) en raisonnant par l'absurde. Si p n'est pas congru à 3 modulo 4, alors -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ et il existe $x \in \mathbb{Z}$ tel que $-1 \equiv x^2 \pmod{p}$. On obtient alors que p divise $x^2 + 1 = (x + i)(x - i)$ dans $\mathbb{Z}$ et donc dans $\mathbb{Z}[i]$. Puisque p est irréductible, il divise $x + i$ ou $x - i$. Mais ceci est impossible, car ni $\dfrac{x}{p} + \dfrac{i}{p}$, ni $\dfrac{x}{p} - \dfrac{i}{p}$ ne sont des éléments de $\mathbb{Z}[i]$.

Supposons (ii) et montrons (iii), toujours par l'absurde. Si $p = \varphi(a)$, alors $p = u^2 + v^2$, où u et v sont deux entiers tels que $a = u + iv$. Mais un carré étant toujours congru à 0 ou 1 $\pmod{4}$, p ne peut être congru qu'à $0, 1$ ou $2 \pmod{4}$, ce qui contredit (ii).

Supposons (iii) et démontrons (i). Soit a et b dans $\mathbb{Z}[i]$ tels que $p = ab$. On a $p^2 = \varphi(p) = \varphi(a)\varphi(b)$. Si ni a, ni b ne sont inversibles, on a $\varphi(a)$ et $\varphi(b)$ différents de 1. On obtient, puisque p est premier, $\varphi(a) = \varphi(b) = p$, ce qui contredit l'hypothèse. On conclut que a ou b est inversible : p est irréductible.

6. D'après les questions précédentes, les entiers premiers congrus à 3 modulo 4 et les éléments a de $\mathbb{Z}[i]$ tels que $\varphi(a)$ soit premier sont irréductibles. Montrons que ce sont les seuls, à multiplication par un inversible près.

Soit a un élément irréductible de $\mathbb{Z}[i]$. On remarque que a divise $\varphi(a) > 1$. L'entier $\varphi(a)$ est un produit d'entiers premiers. Puisque a est irréductible, il divise (dans $\mathbb{Z}[i]$) un de ces entiers premiers, p. Il existe $b \in \mathbb{Z}[i]$ tel que $p = ab$ et donc $p^2 = \varphi(a)\varphi(b)$. Si b est inversible, a est associé à p et nécessairement p est congru à 3 modulo 4, d'après la question 5. Sinon, on a, puisque $\varphi(a) > 1$, $\varphi(a) = p$ et a est un irréductible du type étudié dans la question 4. $\lhd$

On remarque que la condition (iii) de la question 5 de l'exercice équivaut à dire que p n'est pas somme de deux carrés. On obtient donc qu'un entier premier est somme de deux carrés si et seulement s'il n'est pas congru à 3 modulo 4. On trouvera dans le chapitre 4 (arithmétique) deux autres preuves de ce résultat (cf. 4.34 et 4.35).

L'exercice 3.13, qui étudie certaines sommes d'entiers de Gauss, suppose connus les résultats de l'exercice 3.12.

3.13. Anneau des entiers de Gauss (2)

Soit $k \in \mathbb{N}^*$ et $n \in \mathbb{N}$. On pose $s_n = \dfrac{1}{4} \displaystyle\sum_{\substack{a \in \mathbb{Z}[i] \\ a\overline{a}=n}} a^k$.

1. Montrer que $s_n \in \mathbb{Z}$ et que, si k n'est pas un multiple de 4, on a $s_n = 0$.

2. Calculer s_5, s_{13} et s_{65} pour $k = 4$. Que constate t-on ?

3. Généraliser le résultat de la question précédente.

(**École normale supérieure**)

$\rhd$ **Solution.**

1. Si $n = 0$, alors $s_n = 0$ pour tout k. Dans la suite, nous supposerons donc $n \neq 0$.

Comme dans l'exercice précédent, on note, pour $a \in \mathbb{Z}[i]$, $\varphi(a) = a\overline{a}$. On rappelle que deux éléments a et b de $\mathbb{Z}[i]$ sont associés s'il existe c, élément inversible de $\mathbb{Z}[i]$, tel que $b = ac$ et que la relation «être associés» est une relation d'équivalence. Il a été démontré dans l'exercice précédent, que les inversibles de $\mathbb{Z}[i]$ sont les éléments a tels que $\varphi(a) = 1$, c'est-à-dire $-1, 1, i, -i$. Si a est non nul, la classe de a contient donc quatre éléments distincts $a, -a, ia, -ia$.

On remarque que si a et b sont associés, alors $\varphi(a) = \varphi(b)$. L'ensemble des éléments a de $\mathbb{Z}[i]$ tels que $\varphi(a) = n$ se compose donc