Agrégation Externe

Anneaux et idéaux

Pour ce problème, sauf précision contraire, $\mathbb{A}$ désigne un anneau commutatif, unitaire et on note :
- 0 et 1 les éléments neutres pour l'addition et la multiplication de $\mathbb{A}$, avec $0 \neq 1$;
- $\mathbb{A}^* = \mathbb{A} \setminus \{0\}$ l'ensemble des éléments non nuls de $\mathbb{A}$;
- $\mathbb{A}^\times$ le groupe multiplicatif des éléments inversibles (ou des unités) de $\mathbb{A}$.

On suppose que les sous anneaux de $\mathbb{A}$ contiennent l'unité 1 et qu'un morphisme d'anneaux commutatifs unitaires $\varphi : \mathbb{A} \to \mathbb{B}$ est tel que $\varphi(1_\mathbb{A}) = 1_\mathbb{B}$.

Les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$, $\mathbb{K}$ désignant un corps commutatif, sont supposés connus.

On rappelle qu'un corps commutatif est un anneau commutatif unitaire dans lequel tout élément non nul est inversible (on a donc $\mathbb{A}^\times = \mathbb{A}^*$).

On peut aussi considérer des anneaux non commutatifs. En pratique nous rencontrerons l'anneau $\mathcal{M}_n(\mathbb{K})$ des matrices carrées d'ordre $n \geq 2$ (pour $n = 1$, $\mathcal{M}_n(\mathbb{K}) = \mathbb{K}$) à coefficients dans un corps commutatif $\mathbb{K}$ ou encore l'anneau $\mathcal{L}(E)$ des endomorphismes d'un $\mathbb{K}$-espace vectoriel E.

– 0 – Quelques rappels

- L'anneau $\mathbb{A}$ est intègre s'il n'admet pas de diviseurs de 0, c'est-à-dire que pour a, b dans $\mathbb{A}$, on a :
$$a \cdot b = 0 \Leftrightarrow a = 0 \text{ ou } b = 0$$
ou encore :
$$a \cdot b \neq 0 \Leftrightarrow a \neq 0 \text{ et } b \neq 0$$
Un sous-anneau d'un anneau intègre est intègre.
Un corps est intègre.
- Deux éléments a, b de $\mathbb{A}$ sont dits associés s'il existe un élément inversible $u \in \mathbb{A}^\times$ tel que $b = ua$.
Les unités de $\mathbb{A}$ sont les éléments associés à 1.
a et b sont associés si, et seulement si, a divise b et b divise a.
La relation « être associés » est une relation d'équivalence.
- Un élément p de $\mathbb{A}$ intègre est dit irréductible si $p \neq 0$, p n'est pas inversible et :
$$(p = uv) \Rightarrow (u \text{ ou } v \text{ est inversible})$$
(les seuls diviseurs de p sont les éléments inversibles ou les éléments de $\mathbb{A}$ associés à p).
- Un élément p de $\mathbb{A}$ intègre est dit premier si $p \neq 0$, p n'est pas inversible et :
$$(p \text{ divise } uv) \Rightarrow (p \text{ divise } u \text{ ou } p \text{ divise } v)$$
- On dit que l'anneau $\mathbb{A}$ est factoriel s'il est intègre et si tout élément non nul et non inversible $a \in \mathbb{A}$ s'écrit de manière unique $a = u\prod_{k=1}^{r} p_k^{\alpha_k}$, où u est inversible, les p_k sont irréductibles deux à deux non associés et les α_k sont des entiers naturels non nuls.
- Un idéal de $\mathbb{A}$ est un sous-ensemble I de $\mathbb{A}$ tel que :
$$\begin{cases} I \text{ est un sous-groupe de } (\mathbb{A}, +) \\ \forall (a, b) \in I \times \mathbb{A},\ ab \in I \end{cases}$$
(la deuxième condition se traduit en disant que I est absorbant pour le produit).
Dans le cas d'un anneau unitaire non commutatif, on définit les notions d'idéal à droite (pour $(a, b) \in I \times \mathbb{A},\ ab \in I$), à gauche (pour $(a, b) \in I \times \mathbb{A},\ ba \in I$) ou bilatère (pour $(a, b) \in I \times \mathbb{A},\ ab \in I$ et $ba \in I$).

– On vérifie facilement qu'une intersection quelconque d'idéaux est un idéal.
– Pour tout $a \in \mathbb{A}$, l'ensemble :

$$(a) = a \cdot \mathbb{A} = \{qa \mid q \in \mathbb{A}\}$$

des multiples de a dans $\mathbb{A}$ est un idéal. Un tel idéal est dit principal et on dit que c'est l'idéal engendré par a.
On a, pour tous a, b dans $\mathbb{A}$:

$$(a \text{ divise } b) \Leftrightarrow ((b) \subset (a))$$

Pour $\mathbb{A}$ intègre, on a :

$$(a \text{ et } b \text{ sont associés}) \Leftrightarrow ((a) = (b))$$

– Plus généralement, pour toute famille $(a_k)_{1 \leq k \leq p}$ d'éléments de $\mathbb{A}$, l'ensemble :

$$(a_1, \cdots, a_p) = \left\{ \sum_{k=1}^{p} q_k a_k \mid (q_1, \cdots, q_p) \in \mathbb{A}^p \right\}$$

est un idéal. On dit que c'est l'idéal engendré par $a_1, \cdots, a_p$ et qu'il est de type fini.
– L'anneau $\mathbb{A}$ est dit principal s'il est intègre et si tout idéal de $\mathbb{A}$ est principal.
En utilisant le théorème de division euclidienne, on vérifie facilement que les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$, $\mathbb{K}$ désignant un corps commutatif, sont principaux.
Ce sont en fait des cas particuliers d'anneaux euclidiens (voir la partie **II**).
– Si $(I_k)_{1 \leq k \leq p}$ est une famille d'idéaux de $\mathbb{A}$, l'ensemble :

$$I = \sum_{k=1}^{p} I_k = \left\{ \sum_{k=1}^{p} x_k \mid (x_1, \cdots, x_p) \in I_1 \times \cdots \times I_p \right\}$$

est un idéal. Pour $I_k = (a_k)$, on a :

$$\sum_{k=1}^{p} (a_k) = (a_1, \cdots, a_p)$$

– Soit I un idéal de $\mathbb{A}$. On dit que a est congru à b modulo I dans $\mathbb{A}$ si $b - a \in I$. On note alors $a \equiv b \ (I)$.
Cette relation de congruence modulo I est une relation d'équivalence sur $\mathbb{A}$ et pour tout $a \in \mathbb{A}$, on note :

$$\overline{a} = \{b \in \mathbb{A} \mid b \equiv a \ (I)\} = a + I$$

la classe d'équivalence correspondante.
L'ensemble de toutes ces classes d'équivalence modulo I est noté $\dfrac{\mathbb{A}}{I}$.
On vérifie qu'il existe une unique structure d'anneau commutatif unitaire sur $\dfrac{\mathbb{A}}{I}$ telle que la surjection canonique $\pi_I : a \in \mathbb{A} \to \overline{a} = a + I \in \dfrac{\mathbb{A}}{I}$ soit un morphisme d'anneaux.
– Un idéal I de $\mathbb{A}$ est dit maximal s'il est distinct de $\mathbb{A}$ et si I et $\mathbb{A}$ sont les seuls idéaux de $\mathbb{A}$ qui contiennent I.
– Un idéal I de $\mathbb{A}$ est dit premier s'il est distinct de $\mathbb{A}$ et si $ab \in I$ si, et seulement si, $a \in I$ ou $b \in I$.

– I – Généralités sur les anneaux et les idéaux

1. Soit I un idéal (à gauche ou à droite ou bilatère) de $\mathbb{A}$ (commutatif ou pas). Montrer que $I = \mathbb{A}$ si, et seulement si, I contient un élément inversible.

2. Soit $\varphi : \mathbb{A} \to \mathbb{B}$ un morphisme d'anneaux.
   (a) Montrer que pour tout idéal J de $\mathbb{B}$, $\varphi^{-1}(J)$ est un idéal de $\mathbb{A}$.
   (b) On suppose que φ est surjectif. Montrer que pour tout idéal I de $\mathbb{A}$, $\varphi(I)$ est un idéal de $\mathbb{B}$, puis que l'application Φ qui associe à tout idéal J de $\mathbb{B}$ l'idéal $\varphi^{-1}(J)$ de $\mathbb{A}$ réalise une bijection de l'ensemble des idéaux de $\mathbb{B}$ dans l'ensemble des idéaux de $\mathbb{A}$ qui contiennent $\ker(\varphi)$.
3. Montrer que les idéaux de $\mathbb{A}$ sont les noyaux de morphismes d'anneaux $\varphi : \mathbb{A} \to \mathbb{B}$ où $\mathbb{B}$ est un anneau commutatif, unitaire.
4. Soit I un idéal de $\mathbb{A}$. Montrer qu'il y a une bijection entre les idéaux de $\dfrac{\mathbb{A}}{I}$ et les idéaux de $\mathbb{A}$ qui contiennent I.
5. **Idéaux de $\mathbb{Z}_n = \dfrac{\mathbb{Z}}{n\mathbb{Z}}$.**
   (a) Soient $\mathbb{A}$ un anneau principal et I est un idéal non trivial de $\mathbb{A}$ (i. e. $I \neq \{0\}$ et $I \neq \mathbb{A}$). Montrer que tous les idéaux de $\dfrac{\mathbb{A}}{I}$ sont principaux. L'anneau $\dfrac{\mathbb{A}}{I}$ est-il principal ?
   (b) Montrer que, pour tout entier naturel n, les idéaux de l'anneau $\mathbb{Z}_n = \dfrac{\mathbb{Z}}{n\mathbb{Z}}$ sont ses sous-groupes additifs.
   (c) Déterminer tous les idéaux de $\mathbb{Z}_n$, où $n \geq 2$ est un entier.
6. **Idéaux de $\mathcal{L}(E)$.**
   E désigne un espace vectoriel sur un corps commutatif $\mathbb{K}$.
   (a) On suppose que E est de dimension finie. Montrer que ses seuls idéaux bilatères sont $\{0\}$ et $\mathcal{L}(E)$.
   (b) Soient E, F deux $\mathbb{K}$-espaces vectoriels de dimension finie. Montrer que tout morphisme d'anneaux $\varphi : \mathcal{L}(E) \to \mathcal{L}(F)$ est injectif.
   (c) On suppose que E est un $\mathbb{R}$-espace vectoriel de dimension $n \geq 2$. Montrer que si p est une semi-norme non nulle sur $\mathcal{L}(E)$ telle que $p(u \circ v) \leq p(u)\, p(v)$ pour tous u, v dans $\mathcal{L}(E)$, c'est alors une norme.
   (d) On suppose que E est de dimension infinie. Montrer que :
   $$I_0 = \{u \in \mathcal{L}(E) \mid \mathrm{rg}(u) \text{ est fini}\}$$
   est un idéal bilatère non trivial de $\mathcal{L}(E)$, puis que tout idéal bilatère non réduit à $\{0\}$ de $\mathcal{L}(E)$ contient I_0.
   (e) On suppose que E est de dimension infinie dénombrable. Montrer que I_0 est l'unique idéal bilatère non trivial de $\mathcal{L}(E)$. Dans le cas où E est de dimension infinie non dénombrable, donner un exemple d'idéal bilatère non trivial de $\mathcal{L}(E)$ qui contient strictement I_0.
   (f) Soit E un espace vectoriel de dimension finie.
   On se propose de montrer que les idéaux à droite de $\mathcal{L}(E)$ sont de la forme :
   $$I_F = \{u \in \mathcal{L}(E) \mid \mathrm{Im}(u) \subset F\}$$
   où F est un sous-espace vectoriel de E.
   Pour tout sous-espace vectoriel F de E, on note :
   $$I_F = \{u \in \mathcal{L}(E) \mid \mathrm{Im}(u) \subset F\}$$
   et pour tout idéal à droite I de $\mathcal{L}(E)$, on note :
   $$F_I = \sum_{u \in I} \mathrm{Im}(u)$$

i. Soit $I \neq \{0\}$ un idéal à droite de $\mathcal{L}(E)$. Montrer que I est sous-espace vectoriel de $\mathcal{L}(E)$ et qu'il existe une famille finie $(v_k)_{1\leq k\leq p}$ d'éléments de I telle que :

$$F_I = \sum_{k=1}^{p} \mathrm{Im}(v_k)$$

ii. Soit $F \neq \{0\}$ un sous-espace vectoriel de E. Montrer que I_F est un idéal à droite de $\mathcal{L}(E)$ et que $F_{I_F} = F$.

iii. Soit $I \neq \{0\}$ un idéal à droite de $\mathcal{L}(E)$. Montrer que $I \subset I_{F_I}$.

iv. Soient $I \neq \{0\}$ un idéal à droite de $\mathcal{L}(E)$, $(v_k)_{1\leq k\leq p}$ une famille d'éléments de I telle que $F_I = \sum_{k=1}^{p} \mathrm{Im}(v_k)$ et $\mathcal{B} = (e_j)_{1\leq n}$ une base de E.

Justifier, pour tout $u \in I_{F_I}$, l'existence d'une famille $(x_{j,k})_{\substack{1\leq j\leq n\\1\leq k\leq p}}$ de vecteurs de E telle que :

$$u(e_j) = \sum_{k=1}^{p} v_k(x_{j,k}) \ (1 \leq j \leq n)$$

puis en désignant par $\varphi : E \to E^p$ l'application linéaire définie par :

$$\varphi(e_j) = (x_{j,1}, \cdots, x_{j,p}) \ (1 \leq j \leq n)$$

et par $v : E^p \to E$ l'application linéaire définie par :

$$v(x_1, \cdots, x_p) = \sum_{k=1}^{p} v_k(x_k)$$

montrer que $u = v \circ \varphi$. En déduire que $I = I_{F_I}$. Conclure.

(g) Soit E un espace vectoriel de dimension finie.
On se propose de montrer que les idéaux à gauche de $\mathcal{L}(E)$ sont de la forme :

$$I_F = \{u \in \mathcal{L}(E) \mid \ker(u) \supset F\}$$

où F est un sous-espace vectoriel de E.

i. Montrer que, pour tout sous-espace vectoriel F de E, I_F est un idéal à gauche de $\mathcal{L}(E)$.

ii. On désigne par E^* le dual de E et pour I idéal à gauche de $\mathcal{L}(E)$, on note :

$${}^tI = \left\{ {}^tu \mid u \in I \right\}$$

Montrer que ${}^tI$ est un idéal à droite de $\mathcal{L}(E^*)$ et conclure.

7. **Élément premier, irréductible ; idéal premier, maximal.**

(a) Montrer qu'un élément premier dans $\mathbb{A}$ intègre est irréductible.

(b) On se donne un entier naturel $n \geq 1$ et on note :

$$\mathbb{Z}\left[i\sqrt{n}\right] = \mathbb{Z} + i\sqrt{n}\mathbb{Z} = \left\{a + ib\sqrt{n} \mid (a,b) \in \mathbb{Z}^2\right\}$$

Pour $n = 1$, il s'agit de l'ensemble $\mathbb{Z}[i]$ des entiers de Gauss.

i. Montrer que $\mathbb{Z}[i\sqrt{n}]$ est un sous anneau de $\mathbb{C}$ stable par l'opération de conjugaison complexe.

ii. Déterminer l'ensemble $\mathbb{Z}\left[i\sqrt{n}\right]^{\times}$ des éléments inversibles de $\mathbb{Z}\left[i\sqrt{n}\right]$.

iii. Quels sont les entiers naturels $p \geq 2$ qui sont premiers dans $\mathbb{Z}$ et réductibles dans $\mathbb{Z}\left[i\sqrt{n}\right]$?

iv. Montrer que, pour $n \geq 3$, 2 est irréductible non premier dans $\mathbb{Z}\left[i\sqrt{n}\right]$.

(c) On suppose que $\mathbb{A}$ est principal. Montrer qu'un élément a de $\mathbb{A}$ est irréductible si, et seulement si, il est premier.

(d) Montrer qu'un idéal I de $\mathbb{A}$ est maximal si, et seulement si, l'anneau quotient $\dfrac{\mathbb{A}}{I}$ est un corps.

(e) Montrer qu'un idéal I de $\mathbb{A}$ est premier si, et seulement si, l'anneau quotient $\dfrac{\mathbb{A}}{I}$ est intègre.

(f) Montrer qu'un idéal maximal est premier.

(g) Montrer qu'un idéal premier n'est pas nécessairement maximal.

(h) On suppose que $\mathbb{A}$ est intègre. Montrer qu'un élément p de $\mathbb{A}$ est premier si, et seulement l'idéal (p) est premier.

(i) On suppose que $\mathbb{A}$ est principal et on se donne $p \in \mathbb{A}$. Montrer que :

$$((p) \text{ premier}) \Leftrightarrow (p \text{ premier}) \Leftrightarrow (p \text{ irréductible}) \Leftrightarrow ((p) \text{ maximal})$$

(j) Quels sont les idéaux premiers, maximaux de $\mathbb{Z}$; de $\mathbb{Z}_n = \dfrac{\mathbb{Z}}{n\mathbb{Z}}$ pour $n \geq 2$?

(k) Montrer que $\dfrac{\mathbb{A}[X]}{(X)}$ est isomorphe à $\mathbb{A}$. À quelle condition l'idéal (X) de $\mathbb{A}[X]$ est-il premier ? maximal ?

(l) Montrer que pour tout nombre premier p, l'idéal (p, X) est maximal dans $\mathbb{Z}[X]$.

8. Soit $\varphi : \mathbb{A} \to \mathbb{B}$ un morphisme d'anneaux.

(a) Si J est un idéal maximal de $\mathbb{B}$, l'idéal $\varphi^{-1}(J)$ de $\mathbb{A}$ est-il maximal ?

(b) Si J est un idéal maximal de $\mathbb{B}$, montrer que si $\varphi^{-1}(J) \neq \mathbb{A}$, cet idéal est alors premier.

(c) Si φ est surjectif, montrer alors pour tout idéal maximal J de $\mathbb{B}$, $\varphi^{-1}(J)$ est un idéal maximal de $\mathbb{A}$.

9. **Anneaux de fonctions continues sur un compact.**
Pour cette question, on se donne deux réels $a < b$ et $\mathbb{A} = \mathcal{C}^0([a,b], \mathbb{R})$ est la $\mathbb{R}$-algèbre des fonctions continues de $[a,b]$ dans $\mathbb{R}$. On munit cette algèbre de la norme de la convergence uniforme $f \mapsto \|f\|_\infty = \sup_{x \in [a,b]} |f(x)|$.

(a) L'anneau $\mathbb{A}$ est-il intègre ?

(b) Quels sont les morphismes d'anneaux de $\mathcal{C}^0([a,b], \mathbb{R})$ dans $\mathbb{R}$?

(c) Montrer que, pour tout réel $x \in [a,b]$ l'ensemble :

$$I_x = \{f \in \mathbb{A} \mid f(x) = 0\}$$

est un idéal maximal de $\mathbb{A}$.

(d) Montrer qu'un idéal maximal de $\mathbb{A}$ est fermé.

(e) Soit I un idéal maximal de $\mathbb{A}$. Montrer que l'ensemble $Z(I) = \{x \in [a,b] \mid \forall f \in I,\ f(x) = 0\}$ est un fermé non vide de $[a,b]$.

(f) Montrer que les idéaux maximaux de $\mathbb{A}$ sont les I_x où $x \in [a,b]$.

(g) Montrer que les idéaux I_x ne sont pas principaux (l'anneau $\mathbb{A}$ n'est pas principal puisque non intègre).

10. **Éléments nilpotents, radical d'un idéal.**

(a) Montrer que l'ensemble :

$$\mathrm{Nil}\,(\mathbb{A}) = \{a \in \mathbb{A} \mid \exists n \in \mathbb{N}^* \,;\; a^n = 0\}$$

est un idéal de $\mathbb{A}$. Les éléments de $\mathrm{Nil}\,(\mathbb{A})$ sont dits nilpotents et $\mathrm{Nil}\,(\mathbb{A})$ est le nilradical de $\mathbb{A}$.

(b) Que vaut $\mathrm{Nil}\left(\dfrac{\mathbb{A}}{\mathrm{Nil}\,(\mathbb{A})}\right)$?

(c) Soit $n \geq 2$ un entier naturel. Quels sont les éléments nilpotents de l'anneau $\mathbb{Z}_n = \dfrac{\mathbb{Z}}{n\mathbb{Z}}$?

(d) Montrer que pour tout idéal I de $\mathbb{A}$, l'ensemble :

$$\sqrt{I} = \{a \in \mathbb{A} \mid \exists n \in \mathbb{N} \,;\; a^n \in I\}$$

est un idéal de $\mathbb{A}$ qui contient I. On dit que $\sqrt{I}$ est le radical de I.

(e) Que vaut $\sqrt{\{0\}}$?

(f) Montrer que $\sqrt{\sqrt{I}} = \sqrt{I}$ et $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ pour I, J idéaux de $\mathbb{A}$.

(g) Soit $p \geq 2$ un nombre premier. Que vaut $\sqrt{p\mathbb{Z}}$?

(h) Soit $n \geq 2$ un entier. Que vaut $\sqrt{n\mathbb{Z}}$?

11. **Anneaux finis.** On suppose que $\mathbb{A}$ est fini.

(a) Montrer qu'un élément non nul de $\mathbb{A}$ est soit inversible, soit un diviseur de zéro.

(b) En déduire qu'un anneau commutatif, unitaire et intègre qui est fini est un corps.

(c) Montrer que dans un anneau fini tout idéal premier est maximal.

– II – Généralités sur les anneaux euclidiens

Définition 1 *On appelle stathme sur A une application $\varphi : \mathbb{A}^* \to \mathbb{N}$.*

Définition 2 *On dit que l'anneau $\mathbb{A}$ est euclidien, s'il est intègre et s'il existe un stathme φ sur $\mathbb{A}$ tel que pour tout couple (a, b) d'éléments de $\mathbb{A} \times \mathbb{A}^*$, il existe un couple (q, r) dans $\mathbb{A}^2$ tel que :*

$$a = bq + r \text{ avec } r = 0 \text{ ou } r \neq 0 \text{ et } \varphi(r) < \varphi(b)$$

Dans ces conditions, on dit que q est un quotient et r un reste dans la division euclidienne de a par b.

On notera $(\mathbb{A}, \varphi)$ un tel anneau euclidien.

1. Soit $(\mathbb{A}, \varphi)$ un anneau euclidien. Montrer que si le stathme φ est constant, $\mathbb{A}$ est alors un corps.
2. Montrer qu'un anneau euclidien est principal.
3. Étant donné un anneau euclidien $(\mathbb{A}, \varphi)$, on définit l'application $\overline{\varphi} : \mathbb{A}^* \to \mathbb{N}$ par :

$$\forall a \in \mathbb{A}^*,\ \overline{\varphi}(a) = \min_{x \in \mathbb{A}^*} \varphi(ax)$$

(a) Montrer que $\overline{\varphi}$ est bien définie et que :

$$\forall (a,b) \in \mathbb{A}^* \times \mathbb{A}^*,\ \overline{\varphi}(ab) \geq \overline{\varphi}(a)$$

Cette propriété se traduit en disant que le stathme $\overline{\varphi}$ est croissant dans le sens où : si a, c dans $\mathbb{A}^*$ sont tels que a divise c, on a alors $\overline{\varphi}(a) \leq \overline{\varphi}(c)$.

(b) Montrer que $(\mathbb{A}, \overline{\varphi})$ est un anneau euclidien (on peut donc se ramener à un stathme croissant).

4. Pour cette question, on suppose que $(\mathbb{A}, \varphi)$ est un anneau euclidien, le stathme φ étant croissant et on s'intéresse à quelques conséquences de la croissance de φ.

(a) Montrer que pour tout $(a,b) \in \mathbb{A}^* \times \mathbb{A}^*$, on a $\varphi(ab) \geq \varphi(a)$, l'égalité étant réalisée si, et seulement si, b est inversible.
En particulier, on a $\varphi(-a) = \varphi(a)$ et $\varphi(ab) > \varphi(a)$ pour a, b non nuls avec b non inversible.

(b) Montrer que, pour tout $a \in \mathbb{A}^*$, on a :

$$\varphi(a) = \min_{x \in \mathbb{A}^*} \varphi(ax)$$

En particulier, on a :

$$\varphi(1) = \min_{x \in \mathbb{A}^*} \varphi(x)$$

(c) Montrer que :

$$\mathbb{A}^\times = \{a \in \mathbb{A}^* \mid \varphi(a) = \varphi(1)\}$$

5. On peut montrer qu'un anneau principal est factoriel et en conséquence il en est de même pour une anneau euclidien.
La démonstration directe de l'existence d'une décomposition en facteurs irréductibles de tout élément non nul et non inversible d'un anneau euclidien est plus simple. L'unicité utilise le lemme d'Euclide qui se déduit du fait qu'un anneau euclidien est principal.
Précisément, étant donné un anneau euclidien $(\mathbb{A}, \varphi)$, montrer (sans utiliser le fait qu'il est principal) qu'un élément non nul de $\mathbb{A}$ est soit inversible soit un produit fini d'éléments irréductibles.

– III – Exemples d'anneaux euclidiens

1. **L'anneau** $(\mathbb{Z}, |\cdot|)$.

(a) Soit α un réel. Montrer que pour tout couple d'entiers (a,b), avec $b \neq 0$, il existe un unique couple d'entiers (q,r) tel que $a = bq + r$ et $\alpha \leq r < \alpha + |b|$.
Pour $\alpha = 0$, on retrouve le théorème classique de division euclidienne avec un reste positif.
Pour $\alpha = -\dfrac{|b|}{2}$, le reste est dans $\left[-\dfrac{|b|}{2}, \dfrac{|b|}{2}\right[$ et c'est le reste de plus petite valeur absolue.

(b) Montrer que l'anneau $\mathbb{Z}$ des entiers relatifs est euclidien pour le stathme $\varphi : n \in \mathbb{Z}^* \mapsto |n|$.

(c) Soient $a \in \mathbb{Z}^*$ et $b \in \mathbb{N}^*$ ne divisant pas a. Montrer qu'il y a exactement deux divisions euclidiennes de a par b dans $(\mathbb{Z}, |\cdot|)$.

2. **Les anneaux** $\mathbb{A}[X]$.

(a) Montrer que l'anneau $\mathbb{K}[X]$ des polynômes à une indéterminée et à coefficients dans un corps commutatif $\mathbb{K}$ est euclidien pour le stathme $\deg : P \in \mathbb{K}[X] \setminus \{0\} \mapsto \deg(P)$. A-t-on unicité du quotient et du reste pour la division euclidienne dans $(\mathbb{K}[X], \deg)$?

(b) L'anneau $\mathbb{Z}[X]$ des polynômes à coefficients dans $\mathbb{Z}$ est-il euclidien ?

(c) On suppose que $\mathbb{A}$ n'est pas un corps. L'anneau $\mathbb{A}[X]$ des polynômes à coefficients dans $\mathbb{A}$ est-il euclidien ?

(d) Soit $\mathbb{A}$ un anneau commutatif, unitaire et intègre. Montrer qu'on a les équivalences :

$$(\mathbb{A}[X] \text{ est euclidien}) \Leftrightarrow (\mathbb{A}[X] \text{ est principal}) \Leftrightarrow (\mathbb{A} \text{ est un corps})$$

3. **L'anneau $\mathbb{D}$ des nombres décimaux.**
Soit :

$$\mathbb{D} = \left\{ \frac{a}{10^m} \mid (a, m) \in \mathbb{Z} \times \mathbb{N} \right\}$$

l'anneau des nombres décimaux (on vérifie facilement que c'est un sous-anneau de $\mathbb{Q}$).

(a) Montrer que tout nombre décimal non nul s'écrit de manière unique sous la forme $d = n2^p5^q$, où n, p, q sont des entiers relatifs avec $n \neq 0$ premier avec 10.
Une telle écriture d'un nombre décimale est appelée écriture canonique.

(b) Montrer que $\mathbb{D}$ est euclidien pour le stathme φ défini, en utilisant l'écriture canonique d'un nombre décimal, par :

$$\forall a = n2^p5^q \in \mathbb{D}^*,\ \varphi(a) = |n|$$

(c) A-t-on unicité du quotient et du reste pour la division euclidienne dans $(\mathbb{D}, \varphi)$?

4. **Les anneaux $\mathbb{Z}[i\sqrt{n}]$.**

(a) Soient u, v dans $\mathbb{Z}[i\sqrt{n}]$ avec $v \neq 0$ et $(x, y) \in \mathbb{Q}^2$ tel que $\frac{u}{v} = x + iy\sqrt{n}$.

i. Montrer qu'il existe un unique couple (a, b) d'entiers relatifs tel que :

$$(x, y) \in \left[a - \frac{1}{2}, a + \frac{1}{2}\right[\times \left[b - \frac{1}{2}, b + \frac{1}{2}\right[$$

ii. En déduire qu'il existe $q \in \mathbb{Z}[i\sqrt{n}]$ tel que $|u - qv| \leq \frac{\sqrt{n+1}}{2}|v|$.

(b) Montrer que, pour $n = 1$ ou $n = 2$, l'anneau $\mathbb{Z}[i\sqrt{n}]$ est euclidien pour le stathme :

$$\varphi : u = a + ib\sqrt{n} \in \mathbb{Z}\left[i\sqrt{n}\right] \mapsto |u|^2 = a^2 + nb^2 \in \mathbb{N}$$

(le stathme est aussi défini en 0).

(c) A-t-on unicité du quotient et du reste pour la division euclidienne dans $(\mathbb{Z}[i], \varphi)$?

(d) Effectuer la division euclidienne de $u = 11 + 7i$ par $v = 18 - i$ dans $\mathbb{Z}[i]$.

(e) On suppose que $n \geq 3$.

i. Montrer que $i\sqrt{n}$, est irréductible dans $\mathbb{Z}[i\sqrt{n}]$.

ii. On suppose que n est pair, soit que $n = 2m$ avec $m \geq 2$. Montrer que $i\sqrt{n}$ divise $2(m + i\sqrt{n})$ et en déduire que $\mathbb{Z}[i\sqrt{n}]$ n'est pas euclidien.

iii. Montrer que 2 est irréductible dans $\mathbb{Z}[i\sqrt{n}]$.

iv. On suppose que n est impair, soit que $n = 2m + 1$ avec $m \geq 1$. En utilisant le fait que 2 divise $1 + n$, montrer que $\mathbb{Z}[i\sqrt{n}]$ n'est pas euclidien.

5. Soient $\omega = x + iy$ un nombre complexe non réel (i. e. avec $x \in \mathbb{R}$ et $y \in \mathbb{R}^*$) et :

$$\mathbb{Z}[\omega] = \mathbb{Z} + \mathbb{Z}\omega = \left\{a + b\omega \mid (a, b) \in \mathbb{Z}^2\right\}$$

(a) Montrer que $\mathbb{Z}[\omega]$ est un anneau si, et seulement si, ω est un entier quadratique, c'est-à-dire racine d'un polynôme de degré 2, $P(X) = X^2 - \alpha X - \beta$ à coefficients entiers.
Dans ce cas, montrer que $\mathbb{Z}[\omega]$ est stable par l'opération de conjugaison complexe $z \mapsto \overline{z}$, que l'application $\varphi : u \mapsto |u|^2$ définit un stathme sur $\mathbb{Z}[\omega]$, que $\mathbb{Z}[\omega] = \mathbb{Z}[\overline{\omega}]$, que pour tout entier relatif n, on a $\mathbb{Z}[\omega] = \mathbb{Z}[n+\omega]$ et qu'il existe un nombre complexe $\omega' = x' + iy'$ tel que $x' \in [0, 1[$, $y' > 0$ et $\mathbb{Z}[\omega] = \mathbb{Z}[\omega']$.
Pour la suite de cette question, on suppose que $\omega = x + iy$ est un entier quadratique avec $x \in [0, 1[$, $y > 0$.

(b) Montrer que l'on soit $\omega = i\sqrt{n}$, soit $\omega = \dfrac{1}{2} + i\dfrac{\sqrt{4n-1}}{2}$ où $n \in \mathbb{N}^*$.

(c) Soient u, v dans $\mathbb{Z}[\omega]$ avec $v \neq 0$.

i. Montrer qu'il existe $(r, s) \in \mathbb{Q}^2$ tel que $\dfrac{u}{v} = r + s\omega$.

ii. Montrer qu'il existe $q \in \mathbb{Z}[\omega]$ tel que $|u - qv|^2 \leq \dfrac{1+y^2}{4}|v|^2$.

(d) Montrer que, pour $x \in [0, 1[$ et $y \in \left]0, \sqrt{3}\right[$, l'anneau $\mathbb{Z}[\omega]$ est euclidien pour le stathme :

$$\varphi : u = a + b\omega \in \mathbb{Z}[\omega] \mapsto |u|^2$$

Préciser les valeurs possibles de ω.

6. **Un anneau principal non euclidien.**

Pour cette question, $\omega = \dfrac{1+i\sqrt{19}}{2}$ (cas $n = 5$ du deuxième cas de figure de **III.5b**) et on se propose de montrer que l'anneau $\mathbb{Z}[\omega]$ est principal, mais non euclidien.

(a) Montrer que :

$$(\mathbb{Z}[\omega])^\times = \{-1, 1\}$$

(b) On suppose qu'il existe un stathme $\varphi : \mathbb{A}^* \to \mathbb{N}$ qui fasse de $\mathbb{Z}[\omega]$ un anneau euclidien.

i. Justifier l'existence de $u \in \mathbb{Z}[\omega] \setminus \{0\}$ tel que :

$$\varphi(u) = \min\{\varphi(v) \mid v \in \mathbb{Z}[\omega] \setminus \{-1, 0, 1\}\}$$

ii. Montrer que pour tout $v \in \mathbb{Z}[\omega] \setminus \{0\}$, l'entier $|u|^2$ divise l'un des entiers $|v|^2$, $|v-1|^2$ ou $|v+1|^2$ dans $\mathbb{N}$.

iii. Montrer qu'on aboutit à une contradiction et conclure.

(c) Montrer que pour tout $z \in \mathbb{C}$, il existe $u \in \mathbb{Z}[\omega]$ tel que :

$$|z - u| < 1 \text{ ou } |2z - u| < 1$$

(d) Montrer que l'anneau $\mathbb{Z}[\omega]$ est principal.

– IV – Anneaux euclidiens pour lesquels il y a unicité de la division

Pour cette partie, $(\mathbb{A}, \varphi)$ est un anneau euclidien.
On dira que le quotient et le reste sont uniquement déterminés pour la division euclidienne dans $(\mathbb{A}, \varphi)$ si :

$$\forall (a, b) \in \mathbb{A} \times \mathbb{A}^*,\ \exists!\,(q, r) \in \mathbb{A}^2 \mid \begin{cases} a = bq + r \\ (r = 0) \text{ ou } (r \neq 0 \text{ et } \varphi(r) < \varphi(b)) \end{cases}$$

Cette partie est consacrée à la démonstration du résultat suivant.

Théorème 3 *Le quotient et le reste sont uniquement déterminés pour la division euclidienne dans* $(\mathbb{A}, \varphi)$ *si, et seulement si, l'anneau* $\mathbb{A}$ *est isomorphe à un anneau* $\mathbb{K}[X]$ *de polynômes à une indéterminée et à coefficients dans un corps commutatif* $\mathbb{K}$.

1. Montrer que le quotient et le reste sont uniquement déterminés pour la division euclidienne dans $(\mathbb{A}, \varphi)$ si, et seulement si, le stathme φ est tel que :

$$\forall (a,b) \in \mathbb{A}^* \times \mathbb{A}^*,\ \varphi(ab) \geq \varphi(a) \tag{1}$$

et :

$$\forall (a,b) \in \mathbb{A}^* \times \mathbb{A}^*,\ a \neq b \Rightarrow \varphi(a-b) \leq \max(\varphi(a), \varphi(b)) \tag{2}$$

2. Les propriétés (1) et (2) sont-elles vérifiées pour $\varphi = \deg$ sur $\mathbb{K}[X]$? pour $|\cdot|$ sur $\mathbb{Z}$? pour φ défini en **III.3b** sur $\mathbb{D}$? pour φ défini en **III.4b** sur $\mathbb{Z}[i]$?

   On suppose, pour la suite de cette partie que le quotient et le reste sont uniquement déterminés pour la division euclidienne dans $(\mathbb{A}, \varphi)$, *ce qui équivaut à dire que les propriétés* (1) *et* (2) *sont vérifiées.*

3. Montrer que $\mathbb{K} = \mathbb{A}^\times \cup \{0\}$ est un corps. On en déduit alors que $\mathbb{A}$ est un $\mathbb{K}$-espace vectoriel.

4. Soient $a \neq b$ dans $\mathbb{A}^*$. Montrer que si $\varphi(a) < \varphi(b)$, on a alors $\varphi(b-a) = \varphi(b)$.

   On suppose, pour la suite de cette partie ***III****, que* $\mathbb{A}$ *n'est pas un corps. On a donc* $\mathbb{K} \subsetneq \mathbb{A}$ *et il existe* $x \in \mathbb{A} \setminus \mathbb{K}$ *tel que :*

$$\varphi(x) = \min_{y \in \mathbb{A} \setminus \mathbb{K}} \varphi(y)$$

5.

   (a) Montrer que $\varphi(x) > \varphi(1)$.

   (b) Montrer que la suite $(\varphi(x^n))_{n \in \mathbb{N}}$ est strictement croissante dans $\mathbb{N}$.

   (c) Montrer que la famille $\mathcal{B}_x = (x^n)_{n \in \mathbb{N}}$ est libre dans le $\mathbb{K}$-espace vectoriel $\mathbb{A}$.

   (d) Montrer que pour tout $a \in \mathbb{A}^*$, il existe un unique entier naturel n tel que $\varphi(a) = \varphi(x^n)$.

   (e) Montrer que $\mathcal{B}_x$ est une base de $\mathbb{A}$, c'est-à-dire que pour tout $a \in \mathbb{A}$, il existe un unique entier naturel n et une unique suite $(a_k)_{0 \leq k \leq n}$ d'éléments de $\mathbb{K}$ telle que $a = \sum_{k=0}^{n} a_k x^k$, les a_k étant dans $\mathbb{K}$ avec $a_n \in \mathbb{A}^\times$. Ce que l'on peut noter $\mathbb{A} = \mathbb{K}[x]$.

   (f) En déduire que l'anneau $\mathbb{A}$ est isomorphe à l'anneau $\mathbb{K}[X]$ des polynômes à une indéterminée et à coefficients dans le corps commutatif $\mathbb{K}$.