Feuille d'exercices 10

Éléments irréductibles, premiers, associés

Exercice 1. Soit $\mathbb{C}[x,y,z,w]$ un anneau des polynômes à 4 indéterminées, $I = \langle xw - yz \rangle$ (l'idéal engendré par $xw - yz$) et

$$A = \mathbb{C}[x,y,z,w]/I = \mathbb{C}[x,y,z,w]/\langle xw - yz \rangle .$$

a. Montrer que les éléments

$$\overline{x} = x + I \qquad \overline{y} = y + I \qquad \overline{z} = z + I \qquad \overline{w} = w + I$$

sont irréductibles dans A.

Solution. ...

b. Montrer que les éléments $\overline{x}$, $\overline{y}$, $\overline{z}$, $\overline{w}$ ne sont pas associés les uns des autres.

Solution. ...

c. Montrer que $\overline{xw}$ admet deux factorisations en produit des éléments irréductibles.

Solution. $\overline{xw} = \overline{x} \cdot \overline{w} = \overline{y} \cdot \overline{z}$.

d. Montrer que $A / \langle \overline{x} \rangle \cong \mathbb{C}[x,y,z,w]/\langle x, yz \rangle$.

Solution.

$$A/\langle \overline{x} \rangle \cong \mathbb{C}[x,y,z,w] \Big/ \langle x, xw - yz \rangle = \mathbb{C}[x,y,z,w] \Big/ \langle x, yz \rangle .$$

e. En déduire que $A/\langle \overline{x} \rangle$ n'est pas intégre, et que $\overline{x}$ n'est pas un élément premier.

Solution.

— $A/\langle \overline{x} \rangle$ n'est pas intègre, car il possède des diviseurs de zéro : $\overline{y} \neq \overline{0}$ et $\overline{z} \neq \overline{0}$ mais $\overline{y} \cdot \overline{z} = \overline{0}$.

— $\overline{x}$ n'est pas premier : en effet, si $\overline{x}$ est premier, alors $A\overline{x}$ est premier et $A/A\overline{x}$ est intègre.

Anneaux euclidiens et principaux

Exercice 2. Montrer que l'anneau quotient $\mathbb{Z}[i]/I$ est fini pour tout idéal non nul I de $\mathbb{Z}[i]$.
(Indice: Rappeler que $\mathbb{Z}[i]$ est un anneau euclidien.)

Solution.

⟨1⟩ L'anneau $\mathbb{Z}[i]$ est un anneau euclidien avec valuation $z \mapsto |z|^2$.

⟨2⟩ En particulier, il est principal (*remarque : tout anneau euclidien est principal*). Donc, il existe $a \in \mathbb{Z}[i]$ non nul tel que $I = \langle a \rangle$.

⟨3⟩ Soit $b + I \in \mathbb{Z}[i]/I$. Alors, il existe $q, r \in \mathbb{Z}[i]$ tel que

$$b = qa + r \qquad \text{avec } r = 0 \text{ ou } |r|^2 < |a|^2 ;$$

d'où

$$b + I = (qa + r) + I = r + I.$$

⟨4⟩ Donc, tout élément de $\mathbb{Z}[i]/I$ s'exprime sous la forme $(x+iy)+I$ avec $x, y \in \mathbb{Z}$ et $0 \leq x^2 + y^2 < |a|^2$.

⟨5⟩ Comme il y a un nombre fini de ces éléments, on a que $\mathbb{Z}[i]/I$ est fini.

Exercice 3. Soit A un anneau euclidien de valuation $\varphi : A^* \to \mathbb{N}$ tel que les seuls éléments inversibles de A sont 1 et -1. Si a est un élément de valuation minimal parmi les éléments non inversibles de A^*, alors $A/\langle a \rangle$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$.

Solution.

— Les éléments de A/Ax sont de la forme $b + Ax$, avec $b \in A$.
— Comme x est non inversible, Ax est un idéal propre de A.
— Donc, A/Ax est de cardinalité au moins 2.
— Comme a est non nul, on peut diviser b par a :

$$\text{il existe } q, r \in A \text{ tels que } b = qa + r \text{ avec } r = 0 \text{ ou } \varphi(r) < \varphi(a).$$

— Par la minimalité de $\varphi(a)$, on a que $r = 0$ ou r est inversible : d'où $r \in \{0, \pm 1\}$.
— Tout élément de A/Ax s'exprime sous la forme $r + Ax$ avec $r \in \{0, 1, -1\}$:

$$b + Ax = (qa + r) + Ax = (q + Ax)(a + Ax) + (r + Ax) = r + Ax.$$

— D'où, $2 \leq |A/Ax| \leq 3$:
  — si $1 + Ax = -1 + Ax$, alors $A/Ax \cong \mathbb{Z}/2\mathbb{Z}$;
  — et si $1 + Ax \neq -1 + Ax$, alors $A/Ax \cong \mathbb{Z}/3\mathbb{Z}$.

Exercice 4. Soit A un anneau intègre et $\psi : A^* \to \mathbb{N}$ une fonction vérifiant les propriétés suivantes :

(1) $\psi(a) > 0$ pour tout $a \in A^*$;

(2) pour tous $a, b \in A^*$, si $\psi(a) \geq \psi(b)$, alors soit b divise a soit il existe $s, t \in A$ tels que

$$\psi(sa - tb) < \psi(b).$$

Montrer que A est un anneau principal.

Solution.

— Soit I un idéal non nul de A.

— On considère l'ensemble $\mathcal{E} = \{\varphi(a) : a \in A^*\} \subseteq \mathbb{N}$.

  — $\mathcal{E}$ est non vide car I est non nul.

  — Par la propriété du bon ordre de $\mathbb{N}$, $\mathcal{E}$ possède un élément minimal $m > 0$.

— Soit $b \in A^*$ tel que $\varphi(b) = m$.

— Montrons que I est engendré par b ; c'est-à-dire, $I = Ab$.

  — Soit $a \in I$ un élément non nul.

  — Alors, $\varphi(a) \geq \varphi(b)$. D'où,

    (1) b divise a ; ou

    (2) il existe $s, t \in A$ tels que $\varphi(sa - tb) < \varphi(b) = m$.

  — Le deuxième cas est impossible : en effet, $sa - tb \in I$, car $a, b \in I$, et donc $0 < \varphi(sa - tb) < m$ est en contradiction avec la minimalité de m.

  — Donc, b divise a. Autrement dit, $a \in Ab$.

Non existence d'un pgcd

Exercice 5. Soit $\alpha = \sqrt{-5}$.

a. Montrer que $1+\alpha$ divise $3+3\alpha$ et $3-3\alpha$ dans $\mathbb{Z}[\alpha]$.

Solution.

$$(1+\alpha)\times 3 = 3+3\alpha$$
$$(1+\alpha)\times(-2-\alpha) = 3-3\alpha$$

b. Montrer que $1-\alpha$ divise $3+3\alpha$ et $3-3\alpha$ dans $\mathbb{Z}[\alpha]$.

Solution.

$$(1-\alpha)\times 3 = 3-3\alpha$$
$$(1-\alpha)\times(-2+\alpha) = 3+3\alpha$$

c. En déduire que $3+3\alpha$ et $3-3\alpha$ ne possèdent pas un pgcd dans $\mathbb{Z}[\alpha]$.

Solution.

⟨3.1⟩ Par contradiction. Soit d un pgcd de $3+3\alpha$ et $3-3\alpha$.

⟨3.2⟩ Comme 3 divise $3+3\alpha$ et $3-3\alpha$, on a que 3 divise d. Donc, $|3|^2 = 9$ divise $|d|^2$.

⟨3.3⟩ Comme $1-\alpha$ divise $3+3\alpha$ et $3-3\alpha$, on a que $1-\alpha$ divise d. Donc, $|1-\alpha|^2 = 6$ divise $|d|^2$.

⟨3.4⟩ Comme d divise $3+3\alpha$ et $3-3\alpha$, on a que $|d|^2$ divise 54.

⟨3.5⟩ D'où, $|d|^2 \in \{18, 54\}$. Il n'est pas possible que $|d|^2 = 18$:
Écrivons $d = x+y\alpha$, avec $x, y \in \mathbb{Z}$. Si $|d|^2 = x^2+5y^2 = 18$, alors $|y| \leq 1$: si $|y| = 0$, alors $x^2 = 18$ n'admet pas de solutions dans $\mathbb{Z}$; si $|y| = 1$, alors $x^2 = 18-5 = 13$ n'admet pas de solutions dans $\mathbb{Z}$.

⟨3.6⟩ D'où, $|d|^2 = 54$. Soit $e \in \mathbb{Z}[\alpha]$ tel que $de = 3+3\alpha$. Comme $|3\pm 3\alpha|^2 = 54 = |d|^2$, il faut que $|e|^2 = 1$. Mais, $|e|^2 = 1$ ssi $e = \pm 1$.

⟨3.7⟩ D'où, d et $3+3\alpha$ sont associés. De même, d et $3-3\alpha$ sont associés. Comme la relation d'association est une relation d'équivalence, on a que $3+3\alpha$ et $3-3\alpha$ sont associés dans $\mathbb{Z}[\alpha]$. Ceci est une contradiction : dans $\mathbb{C}$ on a que

$$\frac{3+3\alpha}{3-3\alpha} = -\frac{2}{3}+\frac{1}{3}\alpha,$$

Donc, $3-3\alpha$ ne divise pas $3+3\alpha$ dans $\mathbb{Z}[\alpha]$.

d. Conclure que $\mathbb{Z}[\alpha]$ n'est pas un anneau euclidien et qu'il n'est pas un anneau principal.

Solution. Si $\mathbb{Z}[\alpha]$ est un anneau euclidien ou un anneau principal, alors toute paire d'éléments de $\mathbb{Z}[\alpha]$ possèdent un pgcd.