Anneaux, arithmétique

Anneaux et corps

Solution 1

1. Tout d'abord $1 = 1 + 0\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$.
   Soient $z_1 = a_1 + b_1\sqrt{3}$ avec $(a_1, b_1) \in \mathbb{Z}^2$ et $z_2 = a_2 + b_2\sqrt{3}$ avec $(a_2, b_2) \in \mathbb{Z}^2$. Alors
   $$z_1 - z_2 = (a_1 - a_2) + (b_1 - b_2)\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$$
   et
   $$z_1 z_2 = (a_1 a_2 + 3b_1 b_2) + (a_1 b_2 + a_2 b_1)\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$$
   $\mathbb{Z}[\sqrt{3}]$ est donc un sous-anneau de $\mathbb{R}$.

2. **a.** On reprend les notations de l'énoncé. On a donc $p^2 = 3q^2$. Ainsi 3 divise p^2. Comme 3 est premier, 3 divise p. Il existe donc $k \in \mathbb{Z}$ tel que $p = 3k$. On a alors $9k^2 = 3q^2$ i.e. $3k^3 = q^2$. On prouve comme précédement que 3 divise q. Ainsi p et q ont un facteur premier commun, ce qui contredit $p \wedge q = 1$. En conclusion, $\sqrt{3} \notin \mathbb{Q}$.

   b. On vérifie aisément que pour tout $(a, b, c, d) \in \mathbb{Z}^4$, $f((a, b) + (c, d)) = f((a, b)) + f((c, d))$, ce qui prouve que f est bien un morphisme de groupes.
   Soit $(a, b) \in \operatorname{Ker} f$. On a donc $a + b\sqrt{3} = 0$. Si on avait $b \neq 0$, $\sqrt{3}$ serait rationnel, ce qui n'est pas. Ainsi $b = 0$ puis $a = 0$. On a donc montré que $\operatorname{Ker} f = \{(0, 0)\}$. Ainsi f est injective. f est surjective par définition de $\mathbb{Z}[\sqrt{3}]$.

3. **a.** Puisque $1 = 1 + 0\sqrt{3}$, $g(1) = \tilde{1} = 1 - 0\sqrt{3} = 1$.
   Soient $z_1 = a_1 + b_1\sqrt{3}$ avec $(a_1, b_1) \in \mathbb{Z}^2$ et $z_2 = a_2 + b_2\sqrt{3}$ avec $(a_2, b_2) \in \mathbb{Z}^2$. Alors $z_1 + z_2 = (a_1 + a_2) + (b_1 + b_2)\sqrt{3}$ et donc
   $$g(z_1 + z_2) = \widetilde{z_1 + z_2} = (a_1 + a_2) - (b_1 + b_2)\sqrt{3} = (a_1 - b_1\sqrt{3}) + (a_2 - b_2\sqrt{3}) = \tilde{z}_1 + \tilde{z}_2 = g(z_1) + g(z_2)$$
   De plus, $z_1 z_2 = (a_1 a_2 + 3b_1 b_2) + (a_1 b_2 + a_2 b_1)\sqrt{3}$ donc
   $$g(z_1 z_2) = \widetilde{z_1 z_2} = (a_1 a_2 + 3b_1 b_2) - (a_1 b_2 + a_2 b_1)\sqrt{3} = (a_1 - b_1\sqrt{3})(a_2 - b_2\sqrt{3}) = \tilde{z}_1 \tilde{z}_2 = g(z_1)g(z_2)$$
   Ainsi f est un endomorphisme d'anneau.
   De plus, $f \circ f = \mathrm{Id}_{\mathbb{Z}[\sqrt{3}]}$ donc f est bijectif : c'est un automorphisme d'anneau.

   b. On a $\mathrm{N}(xy) = xy\widetilde{xy} = x\tilde{x}y\tilde{y} = \mathrm{N}(x)\mathrm{N}(y)$.

   c. Si x est inversible, il existe $y \in \mathbb{Z}[\sqrt{3}]$ tel que $xy = 1$. On a donc $\mathrm{N}(x)\mathrm{N}(y) = \mathrm{N}(1) = 1$. Or $\mathrm{N}(x)$ et $\mathrm{N}(y)$ sont des entiers donc $\mathrm{N}(x) = \pm 1$.
   Si $\mathrm{N}(x) = 1$, alors $x\tilde{x} = 1$, ce qui prouve que x est inversible d'inverse $\tilde{x}$. Si $\mathrm{N}(x) = -1$, alors $x(-\tilde{x}) = 1$, ce qui prouve que x est inversible d'inverse $-\tilde{x}$.

Solution 2

1. **a.** Si on pose $x = 2$, il n'existe pas $u \in \mathbb{Z}$ tel que $xux = x$ i.e. $2u = 1$. L'anneau $(\mathbb{Z}, +\times)$ n'est donc pas régulier.

   b. Supposons que A soit un corps. Soit $x \in \mathrm{A}$. Si $x = 0_{\mathrm{A}}$, alors pour tout $u \in \mathrm{A}$, $xux = x = 0_{\mathrm{A}}$. Sinon, x est inversible et, en posant $u = x^{-1}$, $xux = x$. Le cors A est donc un anneau régulier.

   c. Il est à peu près évident que si deux anneaux A et B sont isomorphes, A est régulier si et seulement si B est régulier. Comme l'anneau $\mathcal{L}(\mathrm{E})$ est isomorphe à l'anneau $\mathcal{M}_n(\mathbb{K})$ où $n = \dim \mathrm{E}$, il suffit donc de montrer que $\mathcal{M}_n(\mathbb{K})$ est régulier. Soit donc $\mathrm{X} \in \mathcal{M}_n(\mathbb{K})$. En notant $r = \operatorname{rg} \mathrm{X}$ et $\mathrm{J}_r = \left(\begin{array}{c|c} \mathrm{I}_r & 0 \\ \hline 0 & 0 \end{array}\right)$, on sait qu'il existe P et Q dans $\mathrm{GL}_n(\mathbb{K})$ telles que $\mathrm{X} = \mathrm{QJ}_r\mathrm{P}^{-1}$. En posant $\mathrm{U} = \mathrm{PQ}^{-1}$, on a bien $\mathrm{XUX} = \mathrm{X}$ puisque $\mathrm{J}_r^2 = \mathrm{J}_r$.

> **Remarque.** On peut raisonner de manière purement géométrique (notamment si E est de dimension infinie). Soit $f \in \mathcal{L}(\mathrm{E})$. En notant S un supplémentaire de $\mathrm{Ker}\, f$ dans E, on sait que f induit un isomorphisme de S sur $\mathrm{Im}\, f$. Notons T un supplémentaire de $\mathrm{Im}\, f$ dans E. On définit $g \in \mathcal{L}(\mathrm{E})$ en posant $g(x) = h^{-1}(x)$ pour $x \in \mathrm{Im}\, f$ et $g(x) = 0_{\mathrm{E}}$ pour $x \in \mathrm{T}$. On vérifie aisément que $(f \circ g \circ f)_{|\,\mathrm{Ker}\, f} = 0 = f_{|\,\mathrm{Ker}\, f}$ et $(f \circ g \circ f)_{|\mathrm{S}} = f_{|\mathrm{S}}$. Ainsi $f \circ g \circ f = f$ car $\mathrm{E} = \mathrm{Ker}\, f \oplus \mathrm{S}$.

2. En s'inspirant de la question précédente, on s'aperçoit que $\mathrm{U} = \mathrm{A}^{\mathsf{T}}$ convient.

> **Remarque.** On pourra consulter l'article suivant sur la pseudo-inverse de Penrose-Moore pour plus de précision.

3. Notons $n = \prod_{i=1}^{r} p_i^{\alpha_i}$. D'après le théorème des restes chinois, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à l'anneau produit $\prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$. D'après une remarque précédente, la régularité de $\mathbb{Z}/n\mathbb{Z}$ est équivalente à celle de l'anneau $\prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$. Mais on montre aisément qu'un produit d'anneau est régulier si et seulement si chaque facteur est régulier.
On est donc amené à étudier la régularité de $\mathbb{Z}/p^{\alpha}\mathbb{Z}$ avec p premier et $\alpha \in \mathbb{N}^*$. On va montrer que $\mathbb{Z}/p^{\alpha}\mathbb{Z}$ est régulier si et seulement si $\alpha = 1$. Si $\alpha = 1$, $\mathbb{Z}/p\mathbb{Z}$ est un corps donc un anneau régulier d'après une question précédente. Supposons que $\mathbb{Z}/p^{\alpha}\mathbb{Z}$ soit régulier. Notamment, il existe $\overline{u} \in \mathbb{Z}/p^{\alpha}\mathbb{Z}$ tel que $\overline{pup} = \overline{p}$. Notamment, p^{α} divise $up^2 - p = p(up-1)$. Comme p est clairement premier avec $up - 1$, p^{α} l'est également. Ainsi, p^{α} divise p d'après le lemme de Gauss de sorte que $\alpha = 1$.
Si on retourne au cas général, $\mathbb{Z}/n\mathbb{Z}$ est un anneau régulier si toutes ses valuations p-adiques valent 0 ou 1. On dit également que n est sans facteur carré.

Solution 3

---

1. Soit $x \in \mathrm{A}$. On a donc $x^3 = x$. Mais on a également $(x + 1_{\mathrm{A}})^3 = x + 1_{\mathrm{A}}$ ou encore $x^3 + 3x^2 + 3x + 1_{\mathrm{A}} = x + 1_{\mathrm{A}}$. Sachant que $x^3 = x$, on obtient donc $3(x^2 + x) = 0_{\mathrm{A}}$.

2. Soit à nouveau $x \in \mathrm{A}$. D'après la question précédente, $3(x^2 + x) = 0_{\mathrm{A}}$. Mais on a également $3\left[(x + 1_{\mathrm{A}})^2 + (x + 1_{\mathrm{A}})\right] = 0_{\mathrm{A}}$ ou encore $3(x^2 + x) + 3(1_{\mathrm{A}}^2 + 1_{\mathrm{A}}) + 6x = 0 - \mathrm{A}$. Sachant que $3(x^2 + x) = 0_{\mathrm{A}}$ de même que $3(1_{\mathrm{A}}^2 + 1_{\mathrm{A}}) = 0_{\mathrm{A}}$, on obtient donc $6x = 0_{\mathrm{A}}$.

3. Soit $(x, y) \in \mathrm{A}^2$. Alors $3(x + y)^2 + 3(x + y) = 0_{\mathrm{A}}$. En développant et en tenant compte du fait que $3x^2 + 3x = 3y^2 + 3y = 0_{\mathrm{A}}$, on obtient bien $3(xy + yx) = 0_{\mathrm{A}}$. Mais on sait également que $6yx = 0_{\mathrm{A}}$. En soustrayant, on obtient bien $3(xy - yx) = 0_{\mathrm{A}}$.

4. Soit $(x, y) \in \mathrm{A}^2$. D'une part,
$$(x + y)^3 = x^3 + y^3 + x^2y + xyx + yx^2 + y^2x + yxy + xy^2$$
et d'autre part,
$$(x - y)^3 = x^3 - y^3 - x^2y - xyx - yx^2 + y^2x + yxy + xy^2$$
Ainsi
$$(x + y)^3 + (x - y)^3 = 2x^3 + 2y^2x + 2yxy + 2xy^2 = 2x + 2y^2x + 2yxy + 2xy^2$$
Mais on sait également que $(x + y)^3 + (x - y)^3 = (x + y) + (x - y) = 2x$. On en déduit que
$$2(y^2x + yxy + xy^2) = 0_{\mathrm{A}}$$
En multipliant à gauche par y, on obtient sachant que $y^3 = y$,
$$2(yx + y^2xy + yxy^2) = 0_{\mathrm{A}}$$
et en multipliant à droite par y, on obtient
$$2(y^2xy + yxy^2 + xy) = 0_{\mathrm{A}}$$
En soustrayant membre à membre, on obtient comme convenu $2(xy - yx) = 0_{\mathrm{A}}$.

5. Soit $(x, y) \in \mathrm{A}$. On sait que $3(xy - yx) = 0_{\mathrm{A}}$ et $2(xy - yx) = 0_{\mathrm{A}}$. En soustrayant membre à membre, on obtient $xy - yx = 0_{\mathrm{A}}$. A est donc bien commutatif.

Solution 4

---

1. On vérifie que $\mathbb{Z}[i]$ est un sous anneau de $\mathbb{C}$.
    - $1 = 1 + 0i \in \mathbb{Z}[i]$
    - $\forall z, z' \in \mathbb{Z}, z - z' \in \mathbb{Z}[i]$,
    - $\forall z, z' \in \mathbb{Z}, zz' \in \mathbb{Z}[i]$.

2. Posons $\mathrm{N}(z) = z\overline{z}$. Pour $z = a + ib \in \mathbb{Z}[i]$, $\mathrm{N}(z) = a^2 + b^2 \in \mathbb{N}$. Pour $z, z' \in \mathbb{Z}[i]$, $\mathrm{N}(zz') = \mathrm{N}(z)\mathrm{N}(z')$. Soit $z \in (\mathbb{Z}[i])^*$. Il existe donc $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$. On a alors $\mathrm{N}(z)\mathrm{N}(z') = 1$ et $\mathrm{N}(z), \mathrm{N}(z') \in \mathbb{N}$. Ceci implique que $\mathrm{N}(z) = 1$. Si $z = a + ib$, on a donc $a^2 + b^2 = 1$. Les seuls couples d'entiers (a, b) possibles sont $(1, 0)$, $(-1, 0)$, $(0, 1)$ et $(0, -1)$, ce qui correspond à $z = \pm 1$ ou $z = \pm i$. Réciproquement on vérifie que ces éléments sont bien inversibles dans $\mathbb{Z}[i]$.

Solution 5

1. Supposons $x \times y$ nilpotent. Il existe donc $n \in \mathbb{N}$ tel que $(x \times y)^n = 0$. Alors

$$(y \times x)^{n+1} = y \times (x \times y)^n \times x = y \times 0_{\mathrm{A}} \times x = 0_{\mathrm{A}}$$

   de sorte que $y \times x$ est nilpotent.

2. Supposons que x et y commutent et que l'un d'entre eux est nilpotent. Puisque x et y commutent, on peut supposer x nilpotent. Il existe donc $n \in \mathbb{N}$ tels que $x^n = 0$. Comme x et y commutent,

$$(x \times y)^n = x^n \times y^n = 0_{\mathrm{A}} \times y^n = 0_{\mathrm{A}}$$

   de sorte que $x \times y$ est nilpotent.

3. Supposons x et y nilpotents. Il existe donc $(n, p) \in \mathbb{N}^2$ tel que $x^n = 0_{\mathrm{A}}$ et $y^p = 0_{\mathrm{A}}$. Posons $q = n + p$. Alors

$$(x + y)^q = \sum_{k=0}^{q} \binom{q}{k} x^k \times y^{q-k}$$

   Soit alors $k \in [\![0, q]\!]$.
    - Si $k \geq n$, alors $x^k = 0_{\mathrm{A}}$ puis $\binom{q}{k} x^k \times y^{q-k} = 0_{\mathrm{A}}$.
    - Si $k < n$, alors $q - k > q - n = p$ donc $y^k = 0_{\mathrm{A}}$ puis $\binom{q}{k} x^k \times y^{q-k} = 0_{\mathrm{A}}$.

   Ainsi $(x + y)^q = 0_{\mathrm{A}}$ de sorte que $x + y$ est bien nilpotent.

4. Supposons x nilpotent. Il existe donc $n \in \mathbb{N}$ tel que $x^n = 0_{\mathrm{A}}$. On écrit :

$$1_{\mathrm{A}} = 1_{\mathrm{A}}^n - x^n = (1_{\mathrm{A}} - x) \times \left(\sum_{k=0}^{n-1} x^k\right) = \left(\sum_{k=0}^{n-1} x^k\right) \times (1_{\mathrm{A}} - x)$$

   Ainsi $1_{\mathrm{A}} - x$ est inversible d'inverse $\sum_{k=0}^{n-1} x^k$.

Solution 6

1. Soit $x \in \mathrm{A}$. D'une part,

$$(x + 1)^2 = x^2 + 2x + 1 = 3x + 1$$

   D'autre part,

$$(x + 1)^2 = x + 1$$

   D'où $2x = 0$.

2. Soient $x, y \in \mathrm{A}$. D'une part,
$$(x+y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$$
D'autre part,
$$(x+y)^2 = x + y$$
D'où $xy + yx = 0$. Donc $2xy + yx = xy$. Or $2xy = 0$ d'après la question précédente donc $yx = xy$. Ceci étant valable pour tous $x, y \in \mathrm{A}$, l'anneau est commutatif.

Solution 7

---

1. Comme f est un morphisme de corps, on a $f(1) = 1$. De plus, pour $n \in \mathbb{Z}$,
$$f(n) = f(n1) = nf(1) = n1 = n$$
Soit $r = \dfrac{p}{q} \in \mathbb{Q}$. Alors $f(p) = f(qr) = qf(r)$. Or $p \in \mathbb{Z}$ donc $f(p) = p$. Par conséquent, $f(r) = \dfrac{p}{q} = r$.

2. Soit $x \geq 0$. Il existe $a \in \mathbb{R}$ tel que $x = a^2$. Alors $f(x) = f(a^2) = f(a)^2 \geq 0$.
Soit $x \leq y$. Alors $f(y) - f(x) = f(y - x) \geq 0$ car $y - x \geq 0$. Donc $f(x) \leq f(y)$. Ainsi f est croissant.

3. Soit $x \in \mathbb{R}$. Par densité de $\mathbb{Q}$ dans $\mathbb{R}$, il existe deux suites de rationnels (r_n) et $r'_n)$ convergeant respectivement vers x par valeurs inférieures et par valeurs supérieures. Ainsi, $\forall n \in \mathbb{N}$,
$$r_n \leq x \leq r'_n$$
Par croissance de f et en utilisant la première question,
$$r_n = f(r_n) \leq f(x) \leq f(r'_n) = r'_n$$
Par passage à la limite, on obtient $f(x) = x$. Ceci étant valable pour tout $x \in \mathbb{R}$, $f = \mathrm{Id}_{\mathbb{R}}$.

Solution 8

---

1. On peut par exemple utiliser les fonctions indicatrices pour montrer l'associativité de Δ. Soit $(\mathrm{A}, \mathrm{B}, \mathrm{C}) \in \mathcal{P}(\mathrm{E})^3$. On montre que :
$$\mathbb{1}_{(\mathrm{A}\Delta\mathrm{B})\Delta\mathrm{C}} = \mathbb{1}_\mathrm{A} + \mathbb{1}_\mathrm{B} + \mathbb{1}_\mathrm{C} - 2(\mathbb{1}_\mathrm{A}\mathbb{1}_\mathrm{B} + \mathbb{1}_\mathrm{A}\mathbb{1}_\mathrm{C} + \mathbb{1}_\mathrm{B}\mathbb{1}_\mathrm{C}) + 4\mathbb{1}_\mathrm{A}\mathbb{1}_\mathrm{B}\mathbb{1}_\mathrm{C}$$
La dernière expression est invariante par permutation de A, B et C. Par conséquent,
$$\mathbb{1}_{(\mathrm{A}\Delta\mathrm{B})\Delta\mathrm{C}} = \mathbb{1}_{(\mathrm{B}\Delta\mathrm{C})\Delta\mathrm{A}}$$
Finalement, $(\mathrm{A}\Delta\mathrm{B})\Delta\mathrm{C} = (\mathrm{B}\Delta\mathrm{C})\Delta\mathrm{A} = \mathrm{A}\Delta(\mathrm{B}\Delta\mathrm{C})$. La loi Δ possède un élément neutre en la personne de l'ensemble vide $\varnothing$. Tout élément $\mathrm{A} \in \mathcal{P}(\mathrm{E})$ possède un inverse pour Δ à savoir $\overline{\mathrm{A}}$. La loi Δ est clairement commutative. En conclusion, $(\mathcal{P}(\mathrm{E}), \Delta)$ est un groupe commutatif.
L'intersection $\cap$ est clairement associative. Elle possède un élément neutre, à savoir E. On peut à nouveau montrer la distributivité de $\cap$ sur Δ en utilisant les fonctions indicatrices. Enfin, $\cap$ est commutative donc $(\mathcal{P}(\mathrm{E}), \Delta, \cap)$ est un anneau commutatif.

2. Soit $\mathrm{A} \in \mathcal{P}(\mathrm{E})$. A est inversible pour $\cap$ si et seulement si il existe $\mathrm{B} \in \mathcal{P}(\mathrm{E})$ tel que $\mathrm{A} \cap \mathrm{B} = \mathrm{E}$. On a donc nécessairement $\mathrm{A} = \mathrm{E}$. Or E possède un inverse pour $\cap$, à savoir E lui-même. On en déduit que le seul élément inversible pour $\cap$ est E.

3. Pour tout $\mathrm{A} \in \mathcal{P}(\mathrm{E})$, $\mathrm{A} \cap \overline{\mathrm{A}} = \varnothing$. Comme E est non vide, $\mathcal{P}(\mathrm{E})$ possède des éléments A non nuls (i.e. des parties non vides de E). Donc l'anneau $(\mathcal{P}(\mathrm{E}), \Delta, \cap)$ n'est pas intègre.

Solution 9

On montre que $\mathbb{Q}[\sqrt{3}]$ est un sous-corps de $\mathbb{R}$.

- $1 = 1 + 0\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$.
- Soient $x = a + b\sqrt{3}$ et $x' = a' + b'\sqrt{3}$ des éléments de $\mathbb{Q}[\sqrt{3}]$. Alors $x - x' = (a - a') + (b - b')\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$.

- On a également $xx' = (aa' + 3bb') + (ab' + a'b)\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$.
- Supposons $x \neq 0$. On a alors

$$\frac{1}{x} = \frac{a - b\sqrt{3}}{a^2 - 3b^2} = \frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2}\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$$

  Mais il aurait fallu montrer auparavant que $a^2 - 3b^2 \neq 0$. Supposons $a^2 - 3b^2 = 0$. En notant $a = \frac{p}{q}$ et $b = \frac{r}{s}$ avec p, q, r, s entiers, on a donc $p^2s^2 - 3r^2q^2 = 0$. Il existe donc des entiers m et n tels que $m^2 = 3n^2$. Quitte à les diviser par leur pgcd, on peut les supposer premiers entre eux. On a alors toujours la relation $m^2 = 3n^2$. En particulier, 3 divise m^2. Mais 3 étant premier 3 divise m. Il existe donc $k \in \mathbb{Z}$ tel que $m = 3k$. On en déduit $9k^2 = 3n^2$ i.e. $3k^2 = n^2$ donc 3 divise n^2 et donc n. Ceci contredit le fait que m et n sont premiers entre eux. Finalement $a^2 - 3b^2 \neq 0$.

Solution 10

---

1. Soit $(x, y) \in \mathrm{A}^2$ tel que $\varphi(x) = \varphi(y)$. Alors $ax = ay$ i.e. $a(x - y) = 0$. Puisque A est intègre et que $a \neq 0$, $x - y = 0$ i.e. $x = y$. Ainsi φ est injective. Puisque A est de cardinal fini et que φ est une application de A dans A, φ est également bijective.

2. Soit a un élément non nul de A. Puisque l'application φ définie à la question précédente est bijective, elle est a fortiori surjective. Il existe donc $b \in \mathrm{A}$ tel que $\varphi(b) = 1$ i.e. $ab = 1$. Ceci prouve que a est inversible.
   Ainsi tout élément non nul de A est inversible : A est un corps.

Idéaux

Solution 11

---

1. Pour tout $x \in \mathrm{I}$, $x^1 = x \in \mathrm{I}$ donc $\mathrm{I} \subset \mathrm{R}(\mathrm{I})$. Montrons maintenant que R(I) est un idéal.

   - $0_{\mathrm{A}} \in \mathrm{I} \subset \mathrm{R}(\mathrm{I})$.
   - Soit $(a, x) \in \mathrm{A} \times \mathrm{I}$. Puisque $x \in \mathrm{I}$, il existe $n \in \mathbb{N}$ tel que $x^n \in \mathrm{I}$. Mais alors $(ax)^n = a^n x^n \in \mathrm{I}$ car I est un idéal. Ainsi $ax \in \mathrm{I}$.
   - Soit $(x, y) \in \mathrm{R}(\mathrm{I})^2$. Alors il existe $(m, n) \in \mathbb{N}^2$ tel que $x^m \in \mathrm{I}$ et $y^n \in \mathrm{I}$. Alors

$$\begin{aligned}
(x+y)^{m+n} &= \sum_{k=0}^{m+n} \binom{m+n}{k} x^k y^{m+n-k} \\
&= \sum_{k=0}^{m} \binom{m+n}{k} x^k y^{m+n-k} + \sum_{k=m+1}^{m+n} \binom{m+n}{k} x^k y^{m+n-k} \\
&= \sum_{k=0}^{m} \binom{m+n}{m-k} x^k y^{n+k} + \sum_{k=1}^{n} \binom{m+n}{m+k} x^{m+k} y^{n-k} \\
&= \left(\sum_{k=0}^{m} \binom{m+n}{m-k} x^k y^k \right) y^n + \left(\sum_{k=1}^{n} \binom{m+n}{m+k} x^k y^{n-k} \right) x^m
\end{aligned}$$

     Ainsi $(x + y)^{m+n} \in \mathrm{I}$ de sorte que $x + y \in \mathrm{R}(\mathrm{I})$.

   R(I) est donc bien un idéal.

2. Soit $x \in \mathrm{R}(\mathrm{I} \cap \mathrm{J})$. Il existe donc $n \in \mathbb{N}$ tel que $x^n \in \mathrm{I} \cap \mathrm{J}$. On en déduit que $x \in \mathrm{R}(\mathrm{I}) \cap \mathrm{R}(\mathrm{J})$.
   Soit $x \in \mathrm{R}(\mathrm{I}) \cap \mathrm{R}(\mathrm{J})$. Il existe donc $(m, n) \in \mathbb{N}^2$ tel que $x^m \in \mathrm{I}$ et $x^n \in \mathrm{J}$. Alors $x^{m+n} \in \mathrm{I} \cap \mathrm{J}$ de sorte que $x \in \mathrm{R}(\mathrm{I} \cap \mathrm{J})$.
   Par double inclusion, $\mathrm{R}(\mathrm{I} \cap \mathrm{J}) = \mathrm{R}(\mathrm{I}) \cap \mathrm{R}(\mathrm{J})$.

> **Remarque.** Le radical de l'idéal nul s'appelle le *nilradical* de l'anneau A. C'est l'idéal des éléments nilpotents de A.

Solution 12

Si $a \in \mathbb{Z}$, $a\mathbb{Q}$ est clairement un idéal de $\mathbb{Q}$.
Soit I un idéal de $\mathbb{Q}$. On vérifie aisément que $\mathrm{I} \cap \mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$. Il existe donc $a \in \mathbb{Z}$ tel que $\mathrm{I} \cap \mathbb{Z} = a\mathbb{Z}$.
En particulier, $a \in \mathrm{I}$ et donc $a\mathbb{Q} \subset \mathrm{I}$ car I est un idéal de $\mathbb{Q}$.
Réciproquement, soit $x \in \mathrm{I}$. Comme $x \in \mathbb{Q}$, il existe $q \in \mathbb{N}^*$ tel que $qx \in \mathbb{Z}$. Mais comme $x \in \mathrm{I}$, $qx \in \mathrm{I}$ car I est un idéal de $\mathbb{Q}$. Ainsi $qx \in \mathrm{I} \cap \mathbb{Z} = a\mathbb{Z}$. Il existe donc $p \in \mathbb{Z}$ tel que $qx = ap$ i.e. $x = a\dfrac{p}{q} \in a\mathbb{Q}$. Ainsi $\mathrm{I} \subset a\mathbb{Q}$.
Par double inclusion, $\mathrm{I} = a\mathbb{Q}$.

Solution 13

On vérifie déjà que $\mathbb{D}$ est un sous-anneau de $(\mathbb{Q}, +, \times)$ (facile).
Si $a \in \mathbb{Z}$, $a\mathbb{D}$ est clairement un idéal de $\mathbb{D}$.
Soit I un idéal de $\mathbb{D}$. On vérifie aisément que $\mathrm{I} \cap \mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$. Il existe donc $a \in \mathbb{Z}$ tel que $\mathrm{I} \cap \mathbb{Z} = a\mathbb{Z}$.
En particulier, $a \in \mathrm{I}$ et donc $a\mathbb{D} \subset \mathrm{I}$ car I est un idéal de $\mathbb{D}$.
Réciproquement, soit $x \in \mathrm{I}$. Comme $x \in \mathbb{D}$, il existe $n \in \mathbb{N}$ tel que $10^n x \in \mathbb{Z}$. Mais comme $x \in \mathrm{I}$, $10^n x \in \mathrm{I}$ car I est un idéal de $\mathbb{D}$. Ainsi $10^n x \in \mathrm{I} \cap \mathbb{Z} = a\mathbb{Z}$. Il existe donc $p \in \mathbb{Z}$ tel que $10^n x = ap$ i.e. $x = a\dfrac{p}{10^n} \in a\mathbb{D}$. Ainsi $\mathrm{I} \subset a\mathbb{D}$.
Par double inclusion, $\mathrm{I} = a\mathbb{D}$.

Solution 14

1. Cf. cours.

2. On a clairement $\mathrm{I} \subset \mathrm{A}$. Supposons que $1_\mathrm{A} \in \mathrm{I}$. Par définition d'un idéal, pour tout $a \in \mathrm{A}$, $1_\mathrm{A} \times a \in \mathrm{I}$ i.e. $\mathrm{A} \subset \mathrm{I}$. Ainsi $\mathrm{I} = \mathrm{A}$.

3.
   - $0_\mathrm{A} = a0_\mathrm{A} \in \mathrm{I}_a$.
   - Soit $(x, y) \in \mathrm{A}^2$. Alors $ax + ay = a(x + y) \in \mathrm{I}_a$.
   - Soit $x \in \mathrm{A}$. Alors pour tout $y \in \mathrm{A}$, $(ax)y = a(xy) \in \mathrm{I}_a$.

   On en déduit que I_a est bien un idéal de A.

4. Supposons que A est un corps. Soit I un idéal non nul de A. Alors il existe $a \in \mathrm{I}$ tel que $a \neq 0_\mathrm{A}$. Mais comme A est un corps, a est inversible. Par conséquent, $1_\mathrm{A} = aa^{-1} \in \mathrm{I}$ car I est un idéal de A. D'après une question précédente, $\mathrm{I} = \mathrm{A}$.
   Réciproquement supposons que les seuls idéaux de A soient $\{0_\mathrm{A}\}$ et A. Soit a un élément non nul de A. On sait que I_a est un idéal de A. On ne peut avoir $\mathrm{I}_a = \{0_\mathrm{A}\}$ sinon on aurait $a = 0_\mathrm{A}$. Ainsi $\mathrm{I}_a = \mathrm{A}$. Notamment $1_\mathrm{A} \in \mathrm{I}_a$. Il existe donc $x \in \mathrm{A}$ tel que $ax = 1_\mathrm{A}$. Ainsin a est inversible et A est un corps.

Solution 15

Soit $(x, y) \in \mathrm{A}^2$ tel que $xy = 0$. Comme $\{0\}$ est un idéal premier par hypothèse, $x = 0$ ou $y = 0$, ce qui prouve que A est intègre.
Pour $x \in \mathrm{A}$, on notera $\langle x \rangle$ l'idéal engendré par x. Soit $x \in \mathrm{A}$. L'idéal $\langle x^2 \rangle$ est premier et $x^2 \in \langle x^2 \rangle$ donc $x \in \langle x^2 \rangle$. Il existe donc $y \in \mathrm{A}$ tel que $x = x^2 y$ ou encore $x(1 - xy) = 0$. Notamment, si $x \neq 0$, on a $xy = 1$ par intégrité de A et donc x est inversible.

Arithmétique de $\mathbb{Z}$

Solution 16

1. Notons q ce quotient. Alors $a - bq$ est le reste de cette même division euclidienne donc $0 \leq a - bq < b$ puis $q \leq \dfrac{a}{b} < q + 1$. Puisque q est entier, $q = \left\lfloor \dfrac{a}{b} \right\rfloor$.

2. Puisque $a \wedge b = 1$, $\overline{a}$ est inversible dans $\mathbb{Z}/b\mathbb{Z}$. L'application de l'énoncé est donc clairement bijective d'inverse $\left\{ \begin{array}{ccc} \mathbb{Z}/b\mathbb{Z} & \longrightarrow & \mathbb{Z}/b\mathbb{Z} \\ \overline{k} & \longmapsto & (\overline{a})^{-1}\overline{k} \end{array} \right.$.

3. Notons r_n le reste de la division euclidienne de n par b. D'après la première question, $r_n = n - b\left\lfloor \frac{n}{b} \right\rfloor$. On en déduit que

$$\sum_{k=1}^{b-1} \left\lfloor \frac{ka}{b} \right\rfloor = \sum_{k=1}^{b-1} \frac{ka}{b} - \sum_{k=1}^{b-1} \frac{r_{ka}}{b}$$

Mais d'après la question précédente, $\sum_{k=1}^{b-1} \frac{r_{ka}}{b} = \sum_{k=1}^{b-1} \frac{k}{b}$ (l'image de 0 par l'application de la question précédente étant 0). Finalement

$$\sum_{k=1}^{b-1} \left\lfloor \frac{ka}{b} \right\rfloor = \sum_{k=1}^{b-1} \frac{ka}{b} - \sum_{k=1}^{b-1} \frac{k}{b} = \frac{a-1}{b} \sum_{k=1}^{b-1} k = \frac{(a-1)(b-1)}{2}$$

Solution 17

Si $a = 1$, la suite (u_n) est constante égale à 1 de sorte que le résultat est clair. Dans la suite, on suppose $a \geq 2$. On peut alors prouver sans peine que la suite (u_n) est croissante et tend vers $+\infty$.

On raisonne alors par récurrence forte sur N.

Tout d'abord, la suite $(u_n \mod 1)$ est constamment nulle donc stationnaire.

Soit N un entier supérieur à 2. Supposons que pour tout $\mathrm{M} \in [\![1, \mathrm{N}-1]\!]$, la suite $(u_n \mod \mathrm{M})$ soit stationnaire.

- Si la suite $(a^n \mod \mathrm{N})$ s'annule, elle est constamment nulle à partir d'un certain rang.
- Sinon, elle ne prend que des valeurs dans $[\![1, \mathrm{N}-1]\!]$. D'après le principe de Dirichlet, les entiers $a^0 \mod \mathrm{N}, \dots, a^{\mathrm{N}-1} \mod \mathrm{N}$ ne peuvent être tous distincts. Il existe donc des entiers p et q tels que $0 \leq p < q \leq \mathrm{N}-1$ et $a^p \mod \mathrm{N} = a^q \mod \mathrm{N}$. En posant $\mathrm{M} = q - p$, la suite $(a^n \mod \mathrm{N})$ est alors M-périodique à partir du rang p.

Dans les deux cas, la suite $(a^n \mod \mathrm{N})$ est M-périodique à partir d'un certain rang p avec $1 \leq \mathrm{M} \leq \mathrm{N}-1$.
D'après l'hypothèse de récurrence, la suite $(u_n \mod \mathrm{M})$ est stationnaire. Il existe donc $q \in \mathbb{N}$ tel que pour tout entier $n \geq q$, $u_{n+1} \mod \mathrm{M} = u_n \mod \mathrm{M}$. La suite (u_n) tend vers $+\infty$ donc il existe un rang r tel que $u_n \geq p$ pour tout entier $n \geq r$. Soit un entier $n \geq \max(q, r)$. Il existe $k \in \mathbb{Z}$ tel que $u_{n+1} = u_n + k\mathrm{M}$ car $u_{n+1} \mod \mathrm{M} = u_n \mod \mathrm{M}$. En fait, $k \in \mathbb{N}$ car la suite (u_n) est croissante. Alors

$$a^{u_{n+1}} \mod \mathrm{N} = a^{u_n + k\mathrm{M}} \mod \mathrm{N} = a^{u_n} \mod \mathrm{N}$$

car la suite $(a^n \mod \mathrm{N})$ est M-périodique à partir du rang p. Ainsi $u_{n+2} \mod \mathrm{N} = u_{n+1} \mod \mathrm{N}$. La suite $(u_n \mod \mathrm{N})$ est donc constante à partir du rang $\max(q, r) + 1$.
Par récurrence forte, la suite $(u_n \mod \mathrm{N})$ est stationnaire pour tout $\mathrm{N} \in \mathbb{N}^*$.

Solution 18

1. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps

$$x^2 = x \iff x(x-1) = 0 \iff (x = 0 \text{ ou } x = 1)$$

2. Comme $34 = 2 \times 17$ et $2 \wedge 17 = 1$, on peut considérer l'isomorphisme d'anneaux naturel φ de $\mathbb{Z}/34\mathbb{Z}$ sur $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$. Alors

$$x^2 = x \iff \varphi(x^2) = \varphi(x) \iff \varphi(x)^2 = \varphi(x)$$

En posant $\varphi(x) = (y, z)$, ceci équivaut à $y^2 = y$ et $z^2 = z$. D'après la question précédente, on a donc

$$x^2 = x \iff (y, z) \in \{(0,0), (0,1), (1,0), (1,1)\}$$

Il s'agit donc maintenant de trouver les antécédents de $(0,0)$, $(0,1)$, $(1,0)$ et $(1,1)$ par φ. Les solutions de $x^2 = x$ sont par conséquent 0, 18, 17 et 1.

> **Remarque.** On confond ici les entiers avec leurs classes modulo 34, ce qui est très mal.

Remarque. Si on n'est pas à l'aise avec les anneaux $\mathbb{Z}/n\mathbb{Z}$, on peut raisonner en termes de congruence. Il s'agit en fait de résoudre $k^2 \equiv k[34]$ dans $\mathbb{Z}$. Cette équation équivaut à $34 \mid k^2 - k$ ou encore $2 \times 17 \mid k(k-1)$. Comme $2 \wedge 17 = 1$, ceci équivaut au système $\begin{cases} 2 \mid k(k-1) \\ 17 \mid k(k-1) \end{cases}$. Mais comme 2 et 17 sont premiers, ceci équivaut à

$$\begin{cases} 2 \mid k \text{ ou } 2 \mid k-1 \\ 17 \mid k \text{ ou } 17 \mid k-1 \end{cases}$$

ou encore à

$$\begin{cases} 2 \mid k \\ 17 \mid k \end{cases} \text{ou} \begin{cases} 2 \mid k-1 \\ 17 \mid k \end{cases} \text{ou} \begin{cases} 2 \mid k \\ 17 \mid k-1 \end{cases} \text{ou} \begin{cases} 2 \mid k-1 \\ 17 \mid k-1 \end{cases}$$

et finalement à

$$\begin{cases} k \equiv 0[2] \\ k \equiv 0[17] \end{cases} \text{ou} \begin{cases} k \equiv 1[2] \\ k \equiv 0[17] \end{cases} \text{ou} \begin{cases} k \equiv 0[2] \\ k \equiv 1[17] \end{cases} \text{ou} \begin{cases} k \equiv 1[2] \\ k \equiv 1[17] \end{cases}$$

Des solutions particulières de chacun de ces systèmes sont respectivement 0, 17, 18 et 1 donc, comme $2 \wedge 17 = 1$, on prouve classiquement que l'ensemble des solutions recherchées est $\{0, 1, 17, 18\} + 34\mathbb{Z}$.

Solution 19

1. **a.** Il existe donc $b \in \mathbb{N}^*$ tel que $n = ab$. Or $2^a \equiv 1[2^a - 1]$ donc $2^{ab} \equiv 1[2^a - 1]$. Ainsi $2^a - 1$ divise M_n.
   b. On suppose M_n premier. Soit a un diviseur positif de n. La question précédente montre que $2^a - 1$ divise M_n. M_n étant premier, on a donc $2^a - 1 = 1$ i.e. $a = 1$ ou $2^a - 1 = 2^n - 1$ i.e. $a = n$. Les seuls diviseurs positifs de n sont donc 1 et n, ce qui prouve que n est premier.
2. **a.** Comme $p \geq 1$, M_p est impair. Donc q est impair. Ainsi $2 \wedge q = 1$. En appliquant le petit théorème de Fermat, on a donc $2^{q-1} \equiv 1[q]$.
   b. Notons m l'ordre de $\overline{2}$ dans le groupe multiplicatif $(\mathbb{Z}/q\mathbb{Z})^*$. Comme q divise M_p, $\overline{2}^p = \overline{1}$ donc m divise p. Or p est premier donc $m = 1$ et $m = p$. Mais $\overline{2} \neq \overline{1}$ (sinon $q = 1$) donc $m = p$.
   c. On a vu que $\overline{2}^{q-1} = \overline{1}$ donc $m = p$ divise $q - 1$ i.e. $q \equiv 1[p]$. Mais comme q est impair, 2 divise $q - 1$. Or p est impair donc $2 \wedge p = 1$. On peut alors affirmer que $2p$ divise $q - 1$ i.e. $q \equiv 1[p]$.
3. Si $n = 1$, on a évidemment $n \equiv 1[2p]$. Sinon n peut s'écrire sous la forme $n = \prod_{i=1}^{r} q_i$ où les q_i sont des nombres premiers. Soit $i \in [\![1, r]\!]$. q_i divise n et donc M_p. La question précédente montre que $q_i \equiv 1[2p]$. En multipliant membre à membre ces congruences, on obtient $n \equiv 1[2p]$.

Solution 20

1. On sait que $(\mathbb{F}_p, +, \times)$ est un corps et que $(\mathbb{F}_p^*, \times)$ est un groupe. Ainsi $(\mathcal{C}, \times)$ est également un groupe puisque c'est l'image de $\mathbb{F}_p^*$ par l'endomorphisme de groupe $x \mapsto x^2$.
2. On trouve $\mathcal{C} = \left\{\overline{1}, \overline{4}, \overline{9}, \overline{5}, \overline{3}\right\}$.
3. D'après un résultat sur les polynômes interpolateurs de Lagrange :

$$\mathrm{P} = \sum_{i=1}^{d} \mathrm{P}(a_i) \prod_{j \neq i} \frac{\mathrm{X} - a_j}{a_i - a_j}$$

   Il existe donc des entiers $m_1, \dots, m_d$ tels que

$$\left(\prod_{1 \leq i < j \leq n} a_j - a_i\right) \mathrm{P} = \sum_{i=1}^{n} m_i \mathrm{P}(a_i) \prod_{j \neq i} (\mathrm{X} - a_j)$$

Soit $n \in \mathbb{Z}$. Alors
$$\left(\prod_{1\leq i<j\leq n} a_j - a_i\right) \mathrm{P}(n) = \sum_{i=1}^n m_i \mathrm{P}(a_i) \prod_{j\neq i}(n-a_j)$$
Puisque p divise les $\mathrm{P}(a_i)$, p divise le membre de droite. Les a_i étant distincts modulo p, aucun des facteurs $a_j - a_i$ n'est divisible par p. Comme p est premier, le lemme d'Euclide permet d'affirmer que p divise $\mathrm{P}(n)$.

4. Soit $y \in \mathcal{C}$. Il existe donc $x \in \mathbb{F}_p^*$ tel que $y = x^2$. Alors $y^{\frac{p-1}{2}} = x^{p-1} = \overline{1}$ car $\mathbb{F}_p^*$ est un groupe multiplicatif d'ordre $p-1$.
Montrons ensuite que $\operatorname{card} \mathcal{C} = \frac{p-1}{2}$. Soit $(x, y) \in \left(\mathbb{F}_p^*\right)^2$. Alors $x^2 = y^2 \iff (x-y)(x+y) = 0 \iff x = \pm y$. De plus, y et $-y$ sont distincts car $p \neq 2$. Ainsi tout élément de $\mathbb{C}$ admet exactement deux antécédents par l'application $x \in \mathbb{F}_p^* \mapsto x^2$. Comme cette application est d'image $\mathcal{C}$ par définition, le lemme des bergers permet de conclure que $\operatorname{card} \mathbb{F}_p^* = 2 \operatorname{card} \mathcal{C}$ i.e. $\operatorname{card} \mathcal{C} = \frac{p-1}{2}$.
Soit $\mathrm{P} = \mathrm{X}^{\frac{p-1}{2}} - 1$. Supposons qu'il existe $a \in \mathbb{F}_p \setminus \mathcal{C}$ tel que $a^{\frac{p-1}{2}} = \overline{1}$. Comme $\deg \mathrm{P} = \operatorname{card} \mathcal{C} = \frac{p-1}{2}$, la question précédente montrerait que $\mathrm{P}(n)$ est divisible par p pour tout $n \in \mathbb{Z}$, ce qui est évidemment absurde (prendre $n = 0$ par exemple).

> **Remarque.** L'énoncé essaie de rester dans le cadre du programme et évite de parler de l'anneau des polynômes $\mathbb{F}_p[\mathrm{X}]$. Si l'on s'autorise ce petit écart du programme, les choses sont plus simples. On peut encore affirmer qu'un polynôme non nul de $\mathbb{F}_p[\mathrm{X}]$ possède au plus autant de racines que son degré. Le polynôme $\mathrm{X}^{\frac{p-1}{2}} - 1$ possède donc au plus $\frac{p-1}{2}$ racines dans $\mathbb{F}_p$. Tous les éléments de $\mathcal{C}$ sont des racines de $\mathrm{X}^{\frac{p-1}{2}} - 1$ et $\operatorname{card} \mathcal{C} = \frac{p-1}{2}$ donc $\mathcal{C}$ est exactement l'ensemble des racines de $\mathrm{X}^{\frac{p-1}{2}}$.

Solution 21

Comme $65 = 5 \times 13$ et $5 \wedge 13 = 1$, on va résoudre cette équation dans $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/13\mathbb{Z}$ puis utiliser l'isomophisme d'anneaux naturel entre $\mathbb{Z}/65\mathbb{Z}$ et $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$. Pour simplifier, on confondra les entiers avec leurs classes d'équivalence dans un anneau $\mathbb{Z}/n\mathbb{Z}$.
Résolution dans $\mathbb{Z}/5\mathbb{Z}$. On s'inspire de la résolution d'une équation du degré 2. Le «discriminant» est -4. Mais dans $\mathbb{Z}/5\mathbb{Z}$, $-4 = 1 = 1^2$. On pressent donc que les solutions sont $\frac{2\pm1}{2}$. Mais on ne peut pas «diviser» par 2 donc on multiplie par l'inverse de 2 dans $\mathbb{Z}/5\mathbb{Z}$, c'est-à-dire 3. Les solutions «raisonnables» sont donc $3(2\pm1)$, c'est-à-dire 3 et $9 = 4$. On peut raisonner maintenant plus rigoureusement :
$$(x-3)(x-4) = x^2 - 7x + 12 = x^2 - 2x + 2$$
Comme 5 est premier, $\mathbb{Z}/5\mathbb{Z}$ est intègre de sorte que $x^2 - 2x + 2 = 0$ équivaut à $x = 3$ ou $x = 4$.
Résolution dans $\mathbb{Z}/13\mathbb{Z}$. Le «discriminant» est toujours -4. Mais dans $\mathbb{Z}/13\mathbb{Z}$, $-4 = 9 = 3^2$. On pressent donc que les solutions sont $\frac{2\pm3}{2}$. Comme l'inverse de 2 dans $\mathbb{Z}/13\mathbb{Z}$ est 7, les solutions $7(2\pm3)$, c'est-à-dire $-7 = 6$ et $35 = 9$. On vérifie à nouveau :
$$(x-6)(x-9) = x^2 - 15x + 54 = x^2 - 2x + 2$$
A nouveau, par intégrité de $\mathbb{Z}/13\mathbb{Z}$, $x^2 - 2x + 2 = 0$ équivaut à $x = 6$ ou $x = 9$.
Pour résoudre dans $\mathbb{Z}/65\mathbb{Z}$, on recherche donc les antécédents dans $\mathbb{Z}/65\mathbb{Z}$ des couples $(3,6)$, $(3,9)$, $(4,6)$, $(4,9)$ de $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$ par l'isomorphisme d'anneaux mentionné au début. On trouve 58, 48, 19, 9.
On peut vérifier avec Python.

```
>>> [x for x in range(65) if (x**2-2*x+2)%65==0]
[9, 19, 48, 58]
```

Solution 22

1. Soit $(x, y) \in \left(\mathbb{F}_p^*\right)^2$. Alors, par intégrité de $\mathbb{F}_p$.
$$x^2 = y^2 \iff (x+y)(x-y) = 0 \iff (x = y \text{ ou } x = -y)$$
Comme $p \neq$, $y \neq -y$. Ainsi tout élément de $\mathbb{C}$ admet exactement deux antécédents par l'application $x \in \mathbb{F}_p^* \mapsto x^2$. Comme cette application est d'image $\mathcal{C}$ par définition, le lemme des bergers permet de conclure que $\operatorname{card} \mathbb{F}_p^* = 2 \operatorname{card} \mathcal{C}$ i.e. $\operatorname{card} \mathcal{C} = \frac{p-1}{2}$.

> **Remarque.** En fait, $\varphi : x \mapsto x^2$ est un endomorphisme du groupe $(\mathbb{F}_p^*, \times)$ de noyau $\{-1, 1\}$. De manière générale, si f est un morphisme d'un groupe G dans un groupe H, alors $\operatorname{card} G = \operatorname{card} \operatorname{Ker} f \times \operatorname{card} \operatorname{Im} f$.

2. Posons $b = a^{\frac{p-1}{2}}$. Comme $\mathbb{F}_p^*$ est un groupe multiplicatif d'ordre $p-1$, $b^2 = a^{p-1} = 1$ i.e. $(b-1)(b+1) = 0$. Par intégrité du corps $\mathbb{F}_p$, $b = \pm 1$.

3. Si $a \in \mathcal{C}$, il existe $x \in \mathbb{F}_p^*$ tel que $a = x^2$. Toujours en vertu du petit théorème de Fermat, $a^{\frac{p-1}{2}} = x^{p-1} = 1$. Comme $X^{\frac{p-1}{2}} - 1$ possède au plus $\frac{p-1}{2}$ racines dans $\mathbb{F}_p$ et que $\operatorname{card} \mathcal{C} = \frac{p-1}{2}$, $\mathcal{C}$ est exactement l'ensemble des racines de $X^{\frac{p-1}{2}} - 1$. Notamment, si $a \notin \mathcal{C}$, $a^{\frac{p-1}{2}} \neq 1$ et donc $a^{\frac{p-1}{2}} = -1$ d'après la question précédente.

Solution 23

---

1. Soit $k \in \mathbb{Z}$ et notons p l'ordre de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$.
Alors $p\overline{k} = \overline{0}$ donc n divise kp. Il existe donc $q \in \mathbb{Z}$ tel que $pk = nq$ puis $p\frac{k}{n \wedge k} = \frac{n}{n \wedge k}q$. Comme $\frac{k}{n \wedge k}$ et $\frac{n}{n \wedge k}$ sont des entiers premiers entre eux, $\frac{n}{n \wedge k}$ divise p.
Inversement $\frac{nk}{n \wedge k} = n \vee k$ est un multiple de n donc $\frac{n}{n \wedge k}\overline{k} = \overline{0}$ de sorte que p divise $\frac{n}{n \wedge k}$.
Finalement, $p = \frac{n}{n \wedge k}$.
Soit $k \in [\![0, n-1]\!]$. Alors $\overline{k}$ est d'ordre d si et seulement si $n \wedge k = n/d$. Supposons que $n \wedge k = n/d$. Alors n/d divise k. Il existe donc $q \in [\![0, d-1]\!]$ tel que $k = nq/d$. Mais comme $n \wedge k = n/d$, on a $d \wedge q = 1$. Réciproquement, si $k = nq/d$ avec $q \in [\![0, d-1]\!]$ tel que $d \wedge q = 1$, on a bien $n \wedge k = n/d$.
Finalement, les $k \in [\![0, n-1]\!]$ tels que $\overline{k}$ est d'ordre d sont les nq/d avec $q \in [\![0, d-1]\!]$ tels que $q \wedge d = 1$. Il y a exactement $\varphi(d)$ tels éléments.

2. Remarquons que l'ordre d'un élément de $\mathbb{Z}/n\mathbb{Z}$ divise l'ordre de $\mathbb{Z}/n\mathbb{Z}$, à savoir n. En notant A_d l'ensemble des éléments d'ordre d de $\mathbb{Z}/n\mathbb{Z}$, on a donc

$$\mathbb{Z}/n\mathbb{Z} = \bigsqcup_{d \mid n} A_d$$

puis en passant aux cardinaux

$$n = \sum_{d \mid n} \varphi(d)$$

3.
```
>>> def indicatrice(n):
...     if n==1:
...         return 1
...     s=0
...     for d in range(1,n):
...         if n%d==0:
...             s+=indicatrice(d)
...     return n-s
...
>>> [indicatrice(n) for n in range(1,11)]
[1, 1, 2, 2, 4, 2, 6, 4, 6, 4]
```

Solution 24

---

1. Le produit sur $\mathbb{R}$ étant commutatif, on peut supposer que $2 \leq n_1 < n_2 < \cdots < n_k$. Les n_j étant entiers, $n_{j+1} - n_j \geq 1$ pour tout $j \in [\![1, k-1]\!]$. Ainsi pour tout $i \in [\![1, k]\!]$,

$$n_i - n_1 = \sum_{j=1}^{i-1} n_{j+1} - n_j \geq \sum_{j=1}^{i-1} 1 = i - 1$$

Ainsi $n_i \geq i - 1 + n_1 \geq i + 1$ puis

$$1 - \frac{1}{n_i} \geq 1 - \frac{1}{i+1} = \frac{i}{i+1}$$

Par télescopage,

$$\prod_{i=1}^{k}\left(1 - \frac{1}{n_i}\right) \geq \prod_{i=1}^{k} \frac{i}{i+1} = \frac{1}{k+1}$$

2. Soit $n \in \mathbb{N}^*$. Notons $p_1, \dots, p_k$ les diviseurs premiers de n ($k = 0$ si $n = 1$). D'après ce qui précède,

$$\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right) \geq \frac{1}{k+1}$$

Donc

$$\varphi(n) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right) \geq \frac{n}{k+1}$$

De plus, tous les p_i étant supérieurs ou égaux à 2, $n \geq \prod_{i=1}^{k} p_i \geq 2^k$, puis $2n \geq 2^{k+1}$ et enfin, $\frac{1}{k+1} \geq \frac{\ln(2)}{\ln(2n)}$. Finalement,

$$\varphi(n) \geq \frac{n}{k+1} \geq \frac{n\ln(2)}{\ln(2n)} = \frac{n\ln(2)}{\ln(n) + \ln(2)}$$

Solution 25

Première méthode.
Notons $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ la décomposition en facteurs premiers de n ($r = 0$ si $n = 1$). Les diviseurs de d sont les entiers de la forme $\prod_{i=1}^{r} p_i^{\beta_i}$ où $0 \leq \beta_i \leq \alpha_i$. Ainsi

$$\sum_{d|n} \frac{n}{d}\mu(d) = n \sum_{(\beta_1,\dots,\beta_r)\in\prod_{i=1}^{r}[\![0,\alpha_i]\!]} \prod_{i=1}^{r} \frac{1}{p_i^{\beta_i}}\mu\left(\prod_{i=1}^{r} p_i^{\beta_i}\right)$$

Mais dès qu'il existe $i \in [\![1,r]\!]$ tel que $\beta_i \geq 2$, $\mu\left(\prod_{i=1}^{r} p_i^{\beta_i}\right) = 0$ donc

$$\begin{aligned}
\sum_{d|n} \frac{n}{d}\mu(d) &= n \sum_{(\beta_1,\dots,\beta_r)\in\{0,1\}^r} \prod_{i=1}^{r} \frac{1}{p_i^{\beta_i}}\mu\left(\prod_{i=1}^{r} p_i^{\beta_i}\right) \\
&= n \sum_{\mathrm{I}\subset[\![0,r]\!]} \prod_{i\in\mathrm{I}} \frac{1}{p_i}\mu\left(\prod_{i\in\mathrm{I}} p_i\right) \\
&= n \sum_{\mathrm{I}\subset[\![0,r]\!]} \prod_{i\in\mathrm{I}} \frac{1}{p_i}(-1)^{|\mathrm{I}|} \\
&= n \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right) = \varphi(n)
\end{aligned}$$

Deuxième méthode.
D'après le théorème des restes chinois, on sait que pour m et n deux entiers naturels non nuls premiers entre eux, $\varphi(mn) = \varphi(m)\varphi(n)$. On sait également que pour p premier et $\alpha \in \mathbb{N}^*$, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
On va montrer que $\psi : n \in \mathbb{N}^* \mapsto \sum_{d|n} \frac{n}{d}\mu(d)$ vérifie les mêmes propriétés. Soit donc $(m,n) \in (\mathbb{N}^*)^2$ tel que $m \wedge n = 1$. On vérifie aisément que l'application $\left\{\begin{array}{ccc} \mathrm{D}_m \times \mathrm{D}_n & \longrightarrow & \mathrm{D}_{mn} \\ (d_1,d_2) & \longmapsto & d_1 d_2 \end{array}\right.$ est bijective (on note D_n l'ensemble des diviseurs positifs de n). Ainsi

$$\psi(mn) = \sum_{d_1|m}\sum_{d_2|n} \frac{mn}{d_1 d_2}\mu(d_1 d_2)$$

Mais si d_1 et d_2 sont des diviseurs respectifs de m et n, ils sont également premiers entre eux de sorte que $\mu(d_1d_2) = \mu(d_1)\mu(d_2)$ puisque d_1 et d_2 n'ont pas de facteur premier commun. On en déduit que

$$\psi(mn) = \left(\sum_{d_1|m} \frac{m}{d_1}\mu(d_1)\right)\left(\sum_{d_2|n} \frac{n}{d_2}\mu(d_2)\right) = \psi(m)\psi(n)$$

Soit alors p un nombre premier et $\alpha \in \mathbb{N}^*$. Les diviseurs de p^α sont les p^β avec $0 \leq \beta \leq \alpha$. Ainsi

$$\psi(p^\alpha) = \sum_{\beta=0}^{\alpha} p^{\alpha-\beta}\mu(p^\beta)$$

Mais dès que $\beta \geq 2$, $\mu(p^\beta) = 0$ donc

$$\psi(p^\alpha) = p^\alpha\mu(p^0) + p^{\alpha-1}\mu(p^1) = p^\alpha - p^{\alpha-1}$$

Notons alors $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ la décomposition en facteurs premiers de $n \in \mathbb{N}^*$. Les $p_i^{\alpha_i}$ étant premiers entre eux deux à deux,

$$\psi(n) = \prod_{i=1}^{r} \psi\left(p_i^{\alpha_i}\right) = \prod_{i=1}^{r}\left(p_i^{\alpha_i} - p_i^{\alpha_i-1}\right) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) = \varphi(n)$$

Solution 26

1. La matrice A est clairement triangulaire inférieure avec des 1 sur la diagonale donc $\det A = 1$.
2. Remarquons que
$$d_{i,j} = \sum_{\substack{k|i\\k|j}} 1 = \sum_{k=1}^{n} a_{i,k}a_{j,k}$$
Ainsi $D = AA^\top$. Par conséquent, $\det D = (\det A)^2 = 1$.
3. Remarquons que $k \mid i \wedge j \iff (k \mid i \text{ ET } k \mid j)$. D'après la formule admise
$$i \wedge j = \sum_{k|i\wedge j} \varphi(k) = \sum_{\substack{k|i\\k|j}} \varphi(k)$$
Posons $p_{i,j} = \varphi(j)$ si j divise i et $p_{i,j} = 0$ sinon ainsi que $P = (p_{i,j})_{1\leq i,j\leq n}$. Alors
$$i \wedge j = \sum_{k=1}^{n} p_{i,k}a_{j,k}$$
Ainsi $S = PA^\top$ puis $\det S = \det P \det A = \det P$. A nouveau, P est triangulaire inférieure et ses coefficients diagonaux sont $\varphi(1), \dots, \varphi(n)$. Ainsi $\det S = \prod_{k=1}^{n} \varphi(k)$.

Solution 27

Puisque a est impair, a est premier avec 2^n. D'après le théorème d'Euler, $a^{\varphi(2^n)} \equiv 1[2^n]$. Or 2 est premier donc $\varphi(2^n) = 2^n - 2^{n-1} = 2^{n-1}$.

Arithmétique de $\mathbb{K}[X]$

Solution 28

Les racines de Q sont j et j^2. Ce sont des racines simples et conjuguées. Pour prouver que Q divise P_m, il est nécessaire et suffisant de prouver que j et j^2 sont des racines d'ordre au moins 1 de P_m. Comme P_m est un polynôme à coefficients réels, ses racines sont conjuguées donc si j

est une racine de P_m, j^2 en est aussi une. Donc Q divise P_m si et seulement si j est une racine de P_m.
On a $P_m(j) = (j+1)^m - j^m - 1$ mais on sait que $j^2 + j + 1 = 0$ donc $P_m(j) = (-j^2)^m - j^m - 1$. En utilisant le fait que

$$j^2 + j + 1 = 0 \quad \text{et} \quad j^3 = 1,$$

un rapide calcul nous donne :

$$\begin{array}{lll} P_0(j) = -3 & P_1(j) = 0 & P_2(j) = 2j \\ P_3(j) = -3 & P_4(j) = 2j^2 & P_5(j) = 0 \end{array}$$

Si on poursuit le calcul pour des plus grandes valeurs de m, on constate que l'on retombe sur les mêmes valeurs. Prouvons que la suite $(P_m(j))_{m\in\mathbb{N}}$ est périodique de période 6. En effet,

$$\begin{aligned} P_{m+6}(j) &= (-j^2)^{m+6} - j^{m+6} - 1 \\ &= (-j^2)^m j^{12} - j^m j^6 - 1 \\ &= (-j^2)^m - j^m - 1 = P_m(j) \end{aligned}$$

Les seuls entiers m tels que $P_m(j) = 0$ sont les entiers de la forme $1 + 6k$ ou $5 + 6k$, où $k \in \mathbb{N}$. D'après ce qui précède, ce sont les seuls entiers tels que Q divise P_m.

Solution 29

1. On sait que j est une racine de $X^2 + X + 1$. On en déduit que $j + 1 = -j^2$. De plus, $2009 \equiv 2[3]$ (2007 est divisible par 3 car la somme de ses chiffres vaut 9). Or on sait également que $j^3 = 1$. Donc
$$j^{2009} = j^2 \quad \text{et} \quad (j+1)^{2009} = (-1)^{2009} j^4 = -j.$$
Posons $P = (X+1)^{2009} + X^{2009} + 1$. On a
$$P(j) = j^2 - j + 1 = -2j \neq 0.$$
Par conséquent, j n'est pas une racine de P et $X^2 + X + 1$ ne divise pas P.

2. D'après la question précédente, la valeur j^n dépend de la congruence de n modulo 3 et $(j+1)^n$ dépend des congruences de n modulo 2 et modulo 3. Si on pose $P_n = (X+1)^n + X^n + 1$, $P_n(j)$ devrait dépendre de la congruence de n modulo 6. On a :
$$P_n(j) = (-1)^n j^{2n} + j^n + 1$$
   - Si $n \equiv 0[6]$, alors $P_n(j) = 3 \neq 0$.
   - Si $n \equiv 1[6]$, alors $P_n(j) = -j^2 + j + 1 = -2j^2 \neq 0$.
   - Si $n \equiv 2[6]$, alors $P_n(j) = j + j^2 + 1 = 0$.
   - Si $n \equiv 3[6]$, alors $P_n(j) = 1 \neq 0$.
   - Si $n \equiv 4[6]$, alors $P_n(j) = j^2 + j + 1 = 0$.
   - Si $n \equiv 5[6]$, alors $P_n(j) = -j + j^2 + 1 = -2j$.

   Comme P_n est à coefficients réels, j^2 est une racine de P_n si et seulement si j est une racine de P_n. Donc j et j^2 sont des racines de P_n si et seulement si $n \equiv 2[6]$ ou $n \equiv 4[6]$. Par conséquent, $X^2 + X + 1$ divise P_n pour ces valeurs de n.

Solution 30

1. On vérifie que $P(1) = P(2) = Q(1) = Q(2) = 0$. On peut donc factoriser P et Q par $(X-1)(X-2)$. On trouve
$$\begin{aligned} P &= (X-1)(X-2)(3X^2+1) \\ Q &= (X-1)(X-2)(X^2+1) \end{aligned}$$
Ce sont bien des décompositions en facteurs irréductibles de P et Q sur $\mathbb{R}[X]$ puisque $3X^2 + 1$ et $X^2 + 1$ sont des polynômes de degré 2 de discriminant strictement négatif. On en déduit
$$\begin{aligned} P &= (X-1)(X-2)(3X+i)(3X-i) \\ Q &= (X-1)(X-2)(X+i)(X-i) \end{aligned}$$
qui sont des décompositions de P et Q en facteurs irréductibles dans $\mathbb{C}[X]$.

2. On a clairement

$$\begin{aligned}
\mathrm{P} \wedge \mathrm{Q} &= (\mathrm{X}-1)(\mathrm{X}-2) \\
\mathrm{P} \vee \mathrm{Q} &= (\mathrm{X}-1)(\mathrm{X}-2)(\mathrm{X}^2+1)\left(\mathrm{X}^2+\frac{1}{3}\right)
\end{aligned}$$

Attention, le PPCM doit être unitaire.

Solution 31

S'il existe $m \in \mathbb{Z}$ tel que $\theta = \dfrac{m\pi}{n}$, alors $\mathrm{P} = \mathrm{X}^{2n} - 2(-1)^m\mathrm{X}^n + 1$.

- Si m est pair,

$$\mathrm{P} = (\mathrm{X}^n - 1)^2 = \prod_{k=0}^{n-1}\left(\mathrm{X} - e^{\frac{2ik\pi}{n}}\right)^2$$

qui est la décomposition en facteurs irréductibles de P dans $\mathbb{C}[\mathrm{X}]$. Il faut alors distinguer suivant la parité de n.
Si n est pair, alors

$$\mathrm{P} = (\mathrm{X}-1)^2(\mathrm{X}+1)^2\prod_{k=1}^{\frac{n}{2}-1}\left(\mathrm{X}^2 - 2\cos\frac{2k\pi}{n} + 1\right)^2$$

qui est la décomposition en facteurs irréductibles de P dans $\mathbb{R}[\mathrm{X}]$.
Si n est impair, alors

$$\mathrm{P} = (\mathrm{X}-1)^2\prod_{k=1}^{\frac{n-1}{2}}\left(\mathrm{X}^2 - 2\cos\frac{2k\pi}{n} + 1\right)^2$$

qui est la décomposition en facteurs irréductibles de P dans $\mathbb{R}[\mathrm{X}]$.

- Si m est impair,

$$\mathrm{P} = (\mathrm{X}^n + 1)^2 = \prod_{k=0}^{n-1}\left(\mathrm{X} - e^{\frac{(2k+1)i\pi}{n}}\right)^2$$

qui est la décomposition en facteurs irréductibles de P dans $\mathbb{C}[\mathrm{X}]$. Il faut alors distinguer suivant la parité de n.
Si n est pair, alors

$$\mathrm{P} = \prod_{k=0}^{\frac{n}{2}-1}\left(\mathrm{X}^2 - 2\cos\frac{(2k+1)\pi}{n} + 1\right)^2$$

qui est la décomposition en facteurs irréductibles de P dans $\mathbb{R}[\mathrm{X}]$.
Si n est impair, alors

$$\mathrm{P} = (\mathrm{X}+1)^2\prod_{k=0}^{\frac{n-1}{2}-1}\left(\mathrm{X}^2 - 2\cos\frac{(2k+1)\pi}{n} + 1\right)^2$$

qui est la décomposition en facteurs irréductibles de P dans $\mathbb{R}[\mathrm{X}]$.

Dans toutes les expressions précédentes, on convient qu'un produit indexé sur le vide vaut 1 et les facteurs sont bien irréductibles car les cosinus ne valent ni 1 ni -1.
On suppose maintenant qu'il n'existe pas d'entier $m \in \mathbb{Z}$ tel que $\theta = \dfrac{m\pi}{n}$. Remarquons que

$$\mathrm{P} = \left(\mathrm{X}^n - e^{ni\theta}\right)\left(\mathrm{X}^n - e^{-ni\theta}\right)$$

On a

$$\mathrm{X}^n - e^{ni\theta} = \prod_{k=0}^{n-1}\left(\mathrm{X} - e^{i\left(\theta + \frac{2k\pi}{n}\right)}\right)$$

et par conjugaison

$$\mathrm{X}^n - e^{-ni\theta} = \prod_{k=0}^{n-1}\left(\mathrm{X} - e^{-i\left(\theta + \frac{2k\pi}{n}\right)}\right)$$

La décomposition de P en facteurs irréductibles dans $\mathbb{C}[X]$ est donc

$$P = \prod_{k=0}^{n-1} \left(X - e^{i\left(\theta + \frac{2k\pi}{n}\right)}\right) \prod_{k=0}^{n-1} \left(X - e^{-i\left(\theta + \frac{2k\pi}{n}\right)}\right)$$

On en déduit que la décomposition de P en facteurs irréductibles dans $\mathbb{R}[X]$ est

$$P = \prod_{k=0}^{n-1} \left(X^2 - 2X\cos\left(\theta + \frac{2k\pi}{n}\right) + 1\right)$$

Les facteurs sont bien irréductibles car la condition $\theta \notin \frac{\pi}{n}\mathbb{Z}$ assure qu'aucun des cosinus ne vaut 1 ou -1.

Solution 32

Les nombres 0 et -1 sont des racines évidentes de P (donc de multiplicté au moins 1). De plus,

$$\begin{aligned} P(j) &= (1+j)^7 - j^7 - 1 = (-j^2)^7 - j - 1 \\ &= -j^{14} - j - 1 = -(1 + j + j^2) = 0 \end{aligned}$$

De même,

$$\begin{aligned} P'(j) &= 7(1+j)^6 - 7j^6 = 7(-j^2)^6 - 7 \\ &= 7j^{12} - 7 = 7 - 7 = 0 \end{aligned}$$

Donc j est racine de multiplicité au moins égale à 2. Comme P est à coefficients réels, $\overline{j}$ est également racine de multiplicité au moins 2. On remarque que $\deg P = 6$. On en déduit que 0 et -1 sont des racines simples, que j et $\overline{j}$ sont des racines doubles et que ce sont les seules racines de P. Enfin, le coefficient domiant de P est $\binom{7}{1} = 7$ donc

$$P = 7X(X+1)(X-j)^2(X-\overline{j})^2 = 7X(X+1)(X^2+X+1)^2$$

Solution 33

1. On trouve $P_0 = 1$, $P_1 = X$, $P_2 = \frac{3}{2}X^2 - \frac{1}{2}$ et $P_3 = \frac{5}{2}X^3 - \frac{3}{2}X$.

2. On a $\deg Q_n = n\deg(X^2-1) = 2n$. Ainsi $\deg P_n = \deg Q_n - n = n$.

3. Comme Q_n est pair, sa dérivée $n^{\text{ème}}$ P_n est paire si n est pair et impaire si n est impair.
   Si n est impair, P_n est impair : on a donc $P_n(0) = 0$.
   Si n est pair, P_n est pair donc P_n' est impair : on a donc $P_n'(0) = 0$.

4. Via la formule du binôme

$$Q_n = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} X^{2k}$$

   La formule de Taylor en 0 donne également

$$Q_n = \sum_{l=0}^{2n} \frac{Q_n^{(l)}(0)}{l!} X^l$$

   Supposons n pair. Il existe donc $p \in \mathbb{N}$ tel que $n = 2p$. En identifiant les coefficients de X^n dans ces deux expressions, on obtient

$$\frac{Q^{(n)}(0)}{n!} = \binom{2p}{p}(-1)^p$$

   puis

$$P_n(0) = \frac{(-1)^p\binom{2p}{p}}{2^{2p}} = \frac{(-1)^p(2p)!}{2^{2p}(p!)^2}$$

Supposons n impair. Il existe donc $p \in \mathbb{N}$ tel que $n = 2p+1$. En identifiant les coefficients de X^{n+1} dans les deux expressions précédentes, on obtient

$$\frac{Q^{(n+1)}(0)}{(n+1)!} = \binom{2p+1}{p+1}(-1)^p$$

puis

$$P_n'(0) = \frac{(2p+2)(-1)^p\binom{2p+1}{p+1}}{2^{2p+1}} = \frac{(-1)^p(2p+1)!}{2^{2p}(p!)^2}$$

5. **a.** Pour $n \geq 1$, on a $Q_n' = 2nX(X^2-1)^{n-1}$ et donc $(X^2-1)Q_n' = 2nX(X^2-1)^n = 2nXQ_n$. On vérifie que cette égalité est encore valable pour $n=0$ puisque $Q_0 = 1$.

b. On utilise la formule de Leibniz. Comme les dérivées de X^2-1 sont nulles à partir de l'ordre 3 et que celles de X sont nulles à partir de l'ordre 2, on a

$$\binom{n+1}{0}(X^2-1)Q_n^{(n+2)} + 2\binom{n+1}{1}XQ_n^{(n+1)} + 2\binom{n+1}{2}Q_n^{(n)} = 2n\binom{n+1}{0}XQ_n^{(n+1)} + 2n\binom{n+1}{1}Q_n^{(n)}$$

Autrement dit

$$(X^2-1)Q_n^{(n+2)} + 2(n+1)XQ_n^{(n+1)} + n(n+1)Q_n^{(n)} = 2nXQ_n^{(n+1)} + 2n(n+1)Q_n^{(n)}$$

ou encore

$$(X^2-1)Q_n^{(n+2)} + 2XQ_n^{(n+1)} = n(n+1)Q_n^{(n)}$$

Par définition de P_n, on a donc

$$(X^2-1)P_n'' + 2XP_n' = n(n+1)P_n$$

6. **a.** $Q_n = (X-1)^n(X+1)^n$ ce qui prouve que 1 et -1 sont des racines de Q_n de multiplicité n. On a donc $Q_n^{(k)}(\pm 1) = 0$ pour $k \in [\![0, n-1]\!]$.

b. On fait l'hypothèse de récurrence HR(k) suivante :

$Q_n^{(k)}$ possède au moins k racines distinctes dans l'intervalle $]-1,1[$

HR(0) est vraie puisque les seules racines de Q_n sont -1 et 1 (pas de racine du tout si $n=0$).
Supposons que HR(k) soit vraie pour un certain $k \in [\![0, n-1]\!]$. Posons $\alpha_0 = -1$, $\alpha_{k+1} = 1$ et α_i pour $1 \leq i \leq k$ k racines distinctes de $Q_n^{(k)}$ dans l'intervalle $]-1,1[$ rangées dans l'ordre croissant. D'après la question précédente, $Q_n^{(k)}$ s'annule en α_0 et α_{k+1}. De plus, $Q_n^{(k)}$ s'annule en les α_i pour $1 \leq i \leq k$. Comme Q_n est dérivable et continue sur $\mathbb{R}$, on peut appliquer le théorème de Rolle entre α_i et α_{i+1} pour $0 \leq i \leq k$. Ceci prouve que la dérivée de $Q_n^{(k)}$, à savoir $Q_n^{(k+1)}$ s'annule $k+1$ fois.
Par récurrence finie, $Q_n^{(n)}$ et donc P_n possède au moins n racines dans l'intervalle $]-1,1[$. Comme $\deg P_n = n$, P_n possède au plus n racines réelles. On en déduit que P_n possède exactement n racines réelles toutes situées dans l'intervalle $]-1,1[$.

Solution 34

Première méthode :
Notons $D = (X^n-1) \wedge (X^p-1)$. On a

$$X^n - 1 = \prod_{\omega \in \mathbb{U}_n}(X-\omega)$$

et

$$X^p - 1 = \prod_{\omega \in \mathbb{U}_p}(X-\omega)$$

Donc

$$D = \prod_{\omega \in \mathbb{U}_n \cap \mathbb{U}_p}(X-\omega)$$

Montrons que $\mathbb{U}_n \cap \mathbb{U}_p = \mathbb{U}_{n \wedge p}$.

- Soit $z \in \mathbb{U}_n \cap \mathbb{U}_p$. Notons $d = n \wedge p$. D'après le théorème de Bézout, il existe $(u,v) \in \mathbb{Z}^2$ tel que $un + vp = d$. Par conséquent

$$z^d = (z^n)^u(z^p)^v = 1$$

Donc $z \in \mathbb{U}_d$.
On peut aussi remarquer que z est d'ordre fini dans $(\mathbb{C}^*, \times)$. Notons k son ordre. Puisque $z^n = z^p = 1$, k divise n et p donc k divise d puis $z^d = 1$.

- Soit $z \in \mathbb{U}_d$. On a donc $z^d = 1$. Comme $d|n$, on a également $z^n = 1$ donc $z \in \mathbb{U}_n$. De même, $z \in \mathbb{U}_p$. Ainsi $z \in \mathbb{U}_n \cap \mathbb{U}_p$.

On a donc par double inclusion $\mathbb{U}_n \cap \mathbb{U}_p = \mathbb{U}_{n \wedge p}$. Ainsi

$$\mathrm{D} = \prod_{\omega \in \mathbb{U}_d} (\mathrm{X} - \omega) = \mathrm{X}^d - 1$$

Seconde méthode :
Posons $r_0 = n$ et $r_1 = p$ et notons $(r_k)_{0 \leq k \leq \mathrm{N}}$ la suite des restes dans l'algorithme d'Euclide appliqué à n et p. En particulier, $r_{\mathrm{N}-1} = n \wedge p$ et $r_{\mathrm{N}} = 0$.
Soit $k \in [\![0, \mathrm{N}-2]\!]$. Alors il existe $q \in \mathbb{N}$ tel que $r_k = qr_{k+1} + r_{k+2}$.

$$\mathrm{X}^{r_k - r_{k+2}} - 1 = \mathrm{X}^{qr_{k+1}} - 1 = (\mathrm{X}^{r_{k+1}} - 1)\mathrm{Q}$$

en posant $\mathrm{Q} = \sum_{j=0}^{q-1} \mathrm{X}^{jr_{k+1}}$. Il s'ensuit que

$$\mathrm{X}^{r_k} - \mathrm{X}^{r_{k+2}} = (\mathrm{X}^{r_{k+1}} - 1)\mathrm{X}^{r_{k+2}}\mathrm{Q}$$

ou encore

$$\mathrm{X}^{r_k} - 1 = \mathrm{X}^{r_{k+2}} - 1 + (\mathrm{X}^{r_{k+1}} - 1)\tilde{\mathrm{Q}}$$

en posant $\tilde{\mathrm{Q}} = \mathrm{X}^{r_{k+2}}\mathrm{Q}$. On en déduit classiquement que $(\mathrm{X}^{r_k} - 1) \wedge (\mathrm{X}^{r_{k+1}} - 1) = (\mathrm{X}^{r_{k+1}} - 1) \wedge (\mathrm{X}^{r_{k+2}} - 1)$.

> **Remarque.** On peut simplifier les choses en utilisant des congruences de polynômes.
>
> $$\mathrm{X}^{r_{k+1}} \equiv 1\,[\mathrm{X}^{r_{k+1}} - 1]$$
>
> donc
>
> $$\mathrm{X}^{qr_{k+1}} \equiv 1\,[\mathrm{X}^{r_{k+1}} - 1]$$
>
> puis
>
> $$\mathrm{X}^{qr_{k+1}+r_{k+2}} \equiv \mathrm{X}^{r_{k+2}}\,[\mathrm{X}^{r_{k+1}} - 1]$$
>
> et enfin
>
> $$\mathrm{X}^{r_k} - 1 \equiv \mathrm{X}^{r_{k+2}} - 1\,[\mathrm{X}^{r_{k+1}} - 1]$$
>
> ce qui permet d'aboutir également à $(\mathrm{X}^{r_k} - 1) \wedge (\mathrm{X}^{r_{k+1}} - 1) = (\mathrm{X}^{r_{k+1}} - 1) \wedge (\mathrm{X}^{r_{k+2}} - 1)$.

Finalement, $(\mathrm{X}^n - 1) \wedge (\mathrm{X}^p - 1) = (\mathrm{X}^{r_{\mathrm{N}-1}} - 1) \wedge (\mathrm{X}^{r_{\mathrm{N}}} - 1) = (\mathrm{X}^{n \wedge p} - 1) \wedge 0 = (\mathrm{X}^{n \wedge p} - 1)$.

Solution 35

Puisque P et Q sont à coefficients dans $\mathbb{Z}$ et, a fortiori, à coefficients dans le corps $\mathbb{Q}$, le théorème de Bézout assure l'existence de deux polynômes U et V de $\mathbb{Q}[\mathrm{X}]$ tels que $\mathrm{UP} + \mathrm{VQ} = 1$. En notant d le ppcm des dénominateurs des coefficients de U et V écrits sous forme fractionnaire et en posant $\mathrm{A} = d\mathrm{U}$ et $\mathrm{B} = d\mathrm{V}$, on a $\mathrm{AP} + \mathrm{BQ} = d$ avec A et B dans $\mathbb{Z}[\mathrm{X}]$. Pour tout $n \in \mathbb{N}$, $\mathrm{A}(n)\mathrm{P}(n) + \mathrm{B}(n)\mathrm{Q}(n) = d$ de sorte que u_n divise d.
Montrons alors que (u_n) est d-périodique. Soit $n \in \mathbb{N}$. Pour tout $k \in \mathbb{N}$

$$(n+d)^k = n^k + \sum_{j=1}^{k} \binom{k}{j} n^{k-j} d^j = n^k + cd$$

avec $c \in \mathbb{N}$. On en déduit que $\mathrm{P}(n+d) = \mathrm{P}(n) + ad$ et $\mathrm{Q}(n+d) = \mathrm{Q}(n) + bd$ avec $(a, b) \in \mathbb{Z}^2$. Puisque u_n divise $\mathrm{P}(n)$, $\mathrm{Q}(n)$ et d, u_n divise $\mathrm{P}(n+d)$ et $\mathrm{Q}(n+d)$ donc u_n divise u_{n+d}. De même, u_{n+d} divise $\mathrm{P}(n+d)$, $\mathrm{Q}(n+d)$ et d de sorte que u_{n+d} divise $\mathrm{P}(n)$ et $\mathrm{Q}(n)$ et donc u_n. On en déduit que $u_{n+d} = u_n$, ce qui prouve que la suite (u_n) est d-périodique.

Solution 36

Il n'y a aucune restriction à supposer P unitaire. Puisque P est scindé, il existe $(\alpha_1, \dots, \alpha_n) \in \mathbb{K}^n$ et $(\mu_1, \dots, \mu_n) \in (\mathbb{N}^*)^n$ tels que $\mathrm{P} = \prod_{i=1}^{n} (\mathrm{X} - \alpha_i)^{\mu_i}$. Puisque $\mathrm{P} \wedge \mathrm{P}'$ divise P, il existe $(\nu_1, \dots, \nu_n) \in \mathbb{N}^n$ tel que $\mathrm{P} \wedge \mathrm{P}' = \prod_{i=1}^{n} (\mathrm{X} - \alpha_i)^{\nu_i}$.
Soit $i \in [\![1, n]\!]$. Puisque α_i est une racine de P de multiplicité μ_i, la caractérisation de la multiplicité à l'aide des dérivées successives montre

que α_i est une racine de P' de multiplicité $\mu_i - 1$. Puisque $P \wedge P'$ divise P', $\nu_i \leq \mu_i - 1$. Finalement, $P \wedge P'$ divise $\prod_{i=1}^{n}(X-\alpha_i)^{\mu_i - 1}$.
Réciproquement, $\prod_{i=1}^{n}(X-\alpha_i)^{\mu_i-1}$ divise bien P et P' donc divise également $P \wedge P'$. On en déduit que $P \wedge P' = \prod_{i=1}^{n}(X-\alpha_i)^{\mu_i-1}$.

Solution 37

---

1. Le nombre i n'étant pas racine de P_n. Soit donc $z \in \mathbb{C} \setminus \{i\}$. Alors

$$(z+i)^n = (z-i)^n \iff \left(\frac{z+i}{z-i}\right)^n = 1$$

Ainsi,

$$\begin{aligned}
P_n(z) = 0 &\iff \exists k \in [\![0, n-1]\!],\ \frac{z+i}{z-i} = e^{\frac{2ik\pi}{n}} \\
&\iff \exists k \in [\![0, n-1]\!],\ z\left(e^{\frac{2ik\pi}{n}} - 1\right) = i\left(e^{\frac{2ik\pi}{n}} + 1\right) \\
&\iff \exists k \in [\![1, n-1]\!],\ z = i\frac{e^{\frac{2ik\pi}{n}}+1}{e^{\frac{2ik\pi}{n}}-1} \qquad \text{car l'équation précédente n'admet pas de solution lorsque } k = 0 \\
&\iff \exists k \in [\![1, n-1]\!],\ z = \operatorname{cotan}\left(\frac{k\pi}{n}\right) \qquad \text{en utilisant la méthode de l'arc-moitié}
\end{aligned}$$

Remarquons que cotan étant strictement décroissante sur $]0, \pi[$, on trouve bien $n-1$ racines distinctes.

2. En utilisant la formule du binôme, on voit que

- P_n est de degré $n-1$;
- son coefficient dominant est $2in$;
- son coefficient constant est $i^n - (-i)^n$;
- son coefficient du monôme de degré $n-2$ est nul.

D'après les liens coefficients/racines, la somme des racines de P_n vaut

$$A_n = \sum_{k=1}^{n-1} \operatorname{cotan}\left(\frac{k\pi}{n}\right) = -\frac{0}{2in} = 0$$

et le produit des racines de P_n vaut

$$B_n = \prod_{k=1}^{n-1} \operatorname{cotan}\left(\frac{k\pi}{n}\right) = \frac{(-1)^{n-1}(i^n - (-i)^n)}{2in} = \frac{(-1)^{n-1}}{n} \cdot \frac{e^{\frac{ni\pi}{2}} - e^{-\frac{ni\pi}{2}}}{2i} = \frac{(-1)^{n-1}\sin\left(\frac{n\pi}{2}\right)}{n}$$

> **Remarque.** Le calcul de A_n peut se faire dirrectement. En effet, par le changement d'indice $k \mapsto n-k$,
>
> $$A_n = \sum_{k=1}^{n-1} \operatorname{cotan}\left(\frac{(n-k)\pi}{n}\right) = \sum_{k=1}^{n-1} \operatorname{cotan}\left(\pi - \frac{k\pi}{n}\right) = -\sum_{k=1}^{n-1} \operatorname{cotan}\left(\frac{k\pi}{n}\right) = -A_n$$
>
> de sorte que $A_n = 0$.
> On peut également remarquer directement que $B_n = 0$ si n est pair. En effet, le facteur d'indice $k = \frac{n}{2}$ est nul dans ce cas puisque $\operatorname{cotan}\left(\frac{\pi}{2}\right) = 0$.

Algèbres

Solution 38

1. f est clairement un endomorphisme. Comme $\mathbb{K}$ est intègre et $a \neq 0$, le noyau de f est nul. Comme K est de dimension finie, f est un automorphisme. Notamment, f est surjectif et 1 admet un antécédent i.e. a est inversible. Autrement dit $\mathbb{K}$ est un corps.

2. Si $(1, a)$ était liée, il existerait $\lambda \in \mathbb{R}$ tel que $a = \lambda \cdot 1 = \lambda$, ce qui est exclu car $a \notin \mathbb{R}$.
Comme K est de dimension finie, on peut considérer le polynôme minimal $\mathrm{P} \in \mathbb{R}[\mathrm{X}]$ de l'endomorphisme $f : x \mapsto ax$. Clairement $\mathrm{P}(f) = \mathrm{P}(a)\,\mathrm{Id}_{\mathrm{K}}$ donc $\mathrm{P}(a) = 0$. Par intégrité de K, P est nécessairement irréductible (dans $\mathbb{R}[\mathrm{X}]$). Ainsi $\deg \mathrm{P} = 1$ ou $\deg \mathrm{P} = 2$ (et P est de discriminant strictement négatif). Le premier cas est exclu car $(1, a)$ est libre. Ainsi $\deg \mathrm{P} = 2$ et donc $(1, a, a^2)$ est liée.

> **Remarque.** On aurait aussi pu prouver que l'ensemble des polynômes de $\mathbb{R}[\mathrm{X}]$ annulant a était un idéal de $\mathbb{R}[\mathrm{X}]$ et noter P son générateur unitaire.

3. Comme $n > 1$, $\mathbb{R} \subsetneq \mathbb{K}$. On peut donc considérer $a \in \mathbb{K} \setminus \mathbb{R}$. D'après la question précédente, il existe un polynôme $\mathrm{P} \in \mathbb{R}[\mathrm{X}]$ de degré 2 irréductible annulant a. Posons $\mathrm{P} = \mathrm{X}^2 + \alpha\mathrm{X} + \beta$. On a donc $a^2 + \alpha a + \beta = 0$ avec $\alpha^2 - 4\beta < 0$. Ceci peut se réécrire
$$\left(a + \frac{\alpha}{2}\right)^2 = \frac{\alpha^2 - 4\beta}{4}$$
On peut donc poser
$$i = \frac{2a + \alpha}{\sqrt{4\beta - \alpha}}$$
pour avoir $i^2 = -1$.
On va maintenant montrer que $\mathbb{K} = \operatorname{vect}(1, i)$.On a clairement $\mathbb{R} \subset \operatorname{vect}(1, i)$. Soit alors $a \in \mathbb{K} \setminus \mathbb{R}$. En reprenant les notations précédentes
$$\left(a + \frac{\alpha}{2}\right)^2 = \frac{\alpha^2 - 4\beta}{4} = \left(\frac{i\sqrt{4\beta - \alpha}}{2}\right)^2$$
Par intégrité de $\mathbb{K}$,
$$a = \frac{-\alpha \pm i\sqrt{4\beta - \alpha}}{2} \in \operatorname{vect}(1, i)$$
Ainsi $\mathbb{K} = \operatorname{vect}(1, i)$ et $(1, i)$ est une base du $\mathbb{R}$-espace vectoriel $\mathbb{K}$.
Rappelons que $(1, \imath)$ est une base du $\mathbb{R}$-espace vectoriel $\mathbb{C}$. Notons alors φ l'unique application $\mathbb{R}$-linéaire de $\mathbb{K}$ dans $\mathbb{C}$ telle que $\varphi(1) = 1$ et $\varphi(i) = \imath$. C'est clairement un isomorphisme linéaire car $(1, i)$ et $(1, \imath)$ sont des bases respectives de $\mathbb{K}$ et $\mathbb{C}$. Enfin, pour $(a, b) \in \mathbb{K}^2$, il existe $(\alpha, \beta, \gamma, \delta) \in \mathbb{R}^4$ tel que $a = \alpha + \beta i$ et $b = \gamma + \delta i$. Alors
$$\begin{aligned}
\varphi(ab) &= \varphi\left((\alpha + \beta i)(\gamma + \delta i)\right) \\
&= \varphi(\alpha\gamma - \beta\delta + (\alpha\delta + \beta\gamma)i) \\
&= \alpha\gamma - \beta\delta + (\alpha\delta + \beta\gamma)\imath \\
&= (\alpha + \beta\imath)(\gamma + \delta\imath) \\
&= \varphi(a)\varphi(b)
\end{aligned}$$
On en déduit que φ est un isomorphisme de $\mathbb{R}$-algèbres de $\mathbb{K}$ sur $\mathbb{C}$.

> **Remarque.** On a tenté de différencier $i \in \mathbb{K}$ et $\imath \in \mathbb{C}$.

Solution 39

Il est claire que M est linéaire car Re et Im sont des formes linéaires sur le $\mathbb{R}$-espace vectoriel $\mathbb{C}$. On a également $\mathrm{M}(1) = \mathrm{I}_2$. Enfin, on vérifie aisément que $\mathrm{M}(z_1 z_2) = \mathrm{M}(z_1)\mathrm{M}(z_2)$ pour tout $(z_1, z_2) \in \mathbb{C}$. Ainsi M est bien un morphisme de $\mathbb{R}$-algèbres.
Enfin $z \in \operatorname{Ker} \mathrm{M} \iff \operatorname{Re}(z) = \operatorname{Im}(z) = 0 \iff z = 0$ donc $\operatorname{Ker} \mathrm{M} = \{0\}$ de sorte que M est injectif.

Solution 40

Soit θ un morphisme d'algèbres de $\mathbb{K}[X]$ dans $\mathbb{K}$. Posons $a = \theta(X)$. Alors pour tout $P \in \mathbb{K}[X]$, $\theta(P) = P(\theta(X)) = P(a)$.
Réciproquement, pour tout $a \in \mathbb{K}$, $P \mapsto P(a)$ est bien un morphisme d'algèbres de $\mathbb{K}[X]$ dans $\mathbb{K}$.
Les morphismes d'algèbres de $\mathbb{K}[X]$ dans $\mathbb{K}$ sont donc les morphismes d'évaluation $P \in \mathbb{K}[X] \mapsto P(a)$ avec $a \in \mathbb{K}$.

Solution 41

L'énoncé considère implicite $\mathbb{C}$ comme une $\mathbb{R}$-alèbre puisque $\mathcal{M}_2(\mathbb{R})$ en est une. On vérifie sans peine que

- Φ est linéaire ;
- $\Phi(1) = I_2$;
- $\forall (z_1, z_2) \in \mathbb{C}^2,\ \Phi(z_1 z_2) = \Phi(z_1)\Phi(z_2)$.

Ainsi Φ est un morphisme d'algèbres. De plus, il est clair que $\operatorname{Ker} \Phi = \{0\}$ donc Φ est injectif.

Remarquons que $A_\theta = \Phi(i\theta)$. En posant $P_n = \sum_{k=0}^{n} \frac{X^k}{k!}$, on a par propriété de morphisme $P_n(A_\theta) = \Phi(P_n(i\theta))$. D'une part, $(P_n(A_\theta))_{n\in\mathbb{N}}$ converge vers $\exp(A_\theta)$. D'autre part, $(P_n(i\theta))$ converge vers $\exp(i\theta)$ et Φ est continue comme application linéaire sur un espace de dimension finie de sorte que $(\Phi(P_n(i\theta)))_{n\in\mathbb{N}}$ converge vers $\Phi(e^{i\theta})$. Par unicité de la limite,

$$\exp(A_\theta) = \Phi(e^{i\theta}) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$