1. Exercices traités en cours

2. Anneaux et idéaux, corps, algèbres

Solution de 5 : Idéaux premiers

1. Les idéaux engendrés par 0, 1 ou un nombre premier.
2.
3.
4. Montrer que A est intègre puis considérer l'idéal engendré par le carré d'un élément non nul.

Solution de 11 :

Par analyse synthèse.

- Si φ est un endomorphisme de l'anneau $\mathbb{Z}$, on a par récurrence que pour tout $n \in \mathbb{N}$, $\varphi(n) = n$ (car $\varphi(0) = 0$ et si pour un $n \in \mathbb{N}$, $\varphi(n) = n$, alors $\varphi(n+1) = \varphi(n) + 1 = n + 1$).
  Puis pour tout $n \in \mathbb{N}$, $\varphi(-n) = -\varphi(n) = -n$ donc pour tout $k \in \mathbb{Z}$, $\varphi(k) = k$.
  On en déduit $\boxed{\varphi = \mathrm{id}_{\mathbb{Z}}}$ et la réciproque est facile.
- Si φ est un endomorphisme de l'anneau $\mathbb{Q}$, c'est aussi un endomorphisme de l'anneau $\mathbb{Z}$, donc $\varphi_{\mathbb{Z}} = \mathrm{id}_{\mathbb{Z}}$.
  Puis, si $r = \dfrac{p}{q} \in \mathbb{Q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$, alors $\varphi(r) = \varphi\left(\dfrac{p}{q}\right) = \dfrac{\varphi(p)}{\varphi(q)} = \dfrac{p}{q} = r$.
  On en déduit $\boxed{\varphi = \mathrm{id}_{\mathbb{Q}}}$ et la réciproque est facile.
- Si φ est un endomorphisme de l'anneau $\mathbb{R}$, c'est aussi un endomorphisme de l'anneau $\mathbb{Q}$, donc $\varphi_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$.
  Puis, pour utiliser la densité de $\mathbb{Q}$ dans $\mathbb{R}$ sans caractérisation séquentielle car nous n'avons pas d'hypothèse de continuité, nous allons montrer que φ est croissante.
  Commençons par remarquer que si $x \geqslant 0$,

$$\varphi(x) = \left(\varphi\left(\sqrt{x}\right)\right)^2 \geqslant 0.$$

  Ainsi, si $x \leqslant y$,

$$\varphi(y) - \varphi(x) = \varphi(y - x) \geqslant 0$$

  donne la croissante de φ.
  Alors, si $x \in \mathbb{R}$ et $n \in \mathbb{N}^*$, par densité, on a $r_n \in \mathbb{Q}$ tel que

$$x \leqslant r_n \leqslant x + \frac{1}{n}.$$

  Par croissance et ce qui précède,

$$\varphi(x) \leqslant r_n \leqslant \varphi(x) + \frac{1}{n}.$$

  Or, par encadrement, $r_n \to x$, donc en faisant $n \to +\infty$ dans ce dernier encadrement, $\varphi(x) = x$.
  On en déduit $\boxed{\varphi = \mathrm{id}_{\mathbb{R}}}$ et la réciproque est facile.

Solution de 14 : Entiers de Gauß

1. On montre que c'est un sous-anneau de $(\mathbb{C},+,\times)$.
   - $\mathbb{Z}[i]\subset\mathbb{C}$
   - $1=1+0\cdot\mathrm{i}\in\mathbb{Z}[i]\neq\varnothing$
   - Si $a,b,a',b'\in\mathbb{Z}$,
   $$(a+\mathrm{i}b)-(a'+\mathrm{i}b')=(a-a')+\mathrm{i}(b-b')\in\mathbb{Z}[i]$$
   $$(a+\mathrm{i}b)\cdot(a'+\mathrm{i}b')=(ab'-bb'')+\mathrm{i}(ab'+ba')\in\mathbb{Z}[i]$$

   Donc $(\mathbb{Z}[i],+,\times)$ est un anneau.

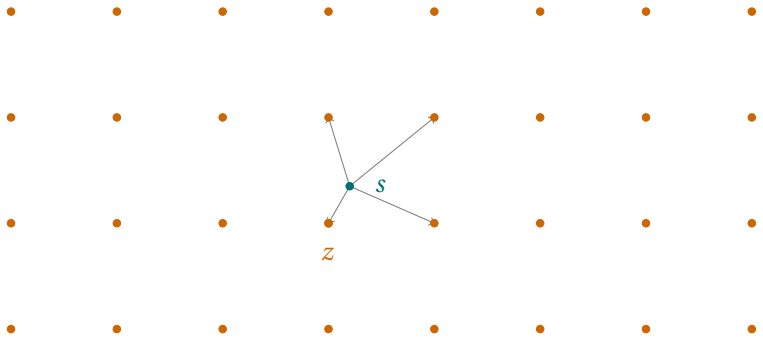
2. Si $z\in\mathbb{Z}[i]$, $a,b\in\mathbb{Z}$ tel que $z=a+\mathrm{i}b$ est inversible, on a $z'\in\mathbb{Z}[i]$ tel que $zz'=1$.
   Alors $N(1)=1=N(zz')=|zz'|^2=|z|^2|z'|^2=\underbrace{N(z)}_{\in\mathbb{N}}\underbrace{N(z')}_{\in\mathbb{N}}$ donc $N(z)=1=\underbrace{a^2}_{\in\mathbb{N}}+\underbrace{b^2}_{\in\mathbb{N}}$ et $\{a^2,b^2\}=\{0,1\}$ et donc $z\in\{-1,1,\mathrm{i},-\mathrm{i}\}$.
   Réciproquement, $-1,1,\mathrm{i},-\mathrm{i}$ sont bien inversibles dans $\mathbb{Z}[i]$.
   Donc $U_{\mathbb{Z}[i]}=\mathbb{U}_4=\{-1,1,\mathrm{i},-\mathrm{i}\}$.

3. Il suffit d'écrire (par exemple) $2=(1+\mathrm{i})(1-\mathrm{i})$ avec $1\pm\mathrm{i}\notin U_{\mathbb{Z}[i]}$.
   Ainsi 2 n'est pas irréductible.

4. (a) On a $\varphi(\mathrm{i})^2=\varphi\left(\mathrm{i}^2\right)=\varphi(-1)=-\varphi(1)=-1$. Donc $\varphi(i)\in\{-\mathrm{i},\mathrm{i}\}$.

   (b) On a par récurrence que pour tout $n\in\mathbb{N}$, $\varphi(n)=n$ (car $\varphi(0)=0$ et si pour un $n\in\mathbb{N}$, $\varphi(n)=n$, alors $\varphi(n+1)=\varphi(n)+1=n+1$).
   Puis pour tout $n\in\mathbb{N}$, $\varphi(-n)=-\varphi(n)=-n$ donc pour tout $k\in\mathbb{Z}$, $\varphi(k)=k$.
   En suite, si $a,b\in\mathbb{Z}$, $\varphi(a+\mathrm{i}b)=\varphi(a)+\varphi(\mathrm{i})\varphi(b)=a+\varphi(i)b$.
   Donc si $\varphi(\mathrm{i})=\mathrm{i}$, $\varphi=\mathrm{id}_{\mathbb{Z}[i]}$ et si $\varphi(\mathrm{i})=-\mathrm{i}$, $\varphi:z\mapsto\overline{z}$.
   Réciproquement, ces deux applications sont bien des morphismes d'anneau.

5. (a) Le point d'abscisse s se trouve dans au moins un carré de côté 1 dont les sommets sont quatre entiers de Carl Friedrich Gauss [1]. En regardant la distance de s à chaque sommet du carré, l'une au moins est inférieure à la demi-diagonale du carré. On a donc bien $z\in\mathbb{Z}[\mathrm{i}]$ tel que $|z-s|\leqslant\frac{\sqrt{2}}{2}$.



1. 

Carl Friedrich Gauss (Brunswick 1777 - Göttingen 1855) est un mathématicien, astronome et physicien allemand. Surnommé *le prince des mathématiciens*, il est considéré comme l'un des plus grands mathématiciens de tous les temps. Gauss était un génie particulièrement précoce : à 7 ans (ou 10 selon les sources), il donne la formule calculant $1+2+\cdots+100$. À 19 ans, il fut le premier à démontrer la loi de réciprocité quadratique. Parmi ses autres prouesses, on peut citer la démonstration du théorème fondamental de l'algèbre, dans sa thèse en 1799, l'invention de la théorie des congruences, la résolution de problèmes de construction à la règle et au compas...Il est considéré comme le fondateur de la géométrie différentielle.

(b) Avec $y \neq 0$, soit $s = \dfrac{x}{y}$ et $q \in \mathbb{Z}[i]$ tel que $\left|\dfrac{x}{y} - q\right| \leqslant \dfrac{\sqrt{2}}{2} < 1$.

On a alors $|x - qy| < |y|$. On pose $r = x - qy \in \mathbb{Z}[\mathrm{i}]$ (car $(\mathbb{Z}[\mathrm{i}], +, \times)$ est un anneau).
On a donc finalement bien $q, r \in \mathbb{Z}[\mathrm{i}]$ tels que

$$\begin{cases} x = qy + r \\ N(r) < N(y) \end{cases}$$

---

6. $\mathbb{Q}[i]$ est un sous-corps de $(\mathbb{C}, +, \times)$.
   - $\mathbb{Q}[i] \subset \mathbb{C}$
   - $1 = 1 + 0 \cdot \mathrm{i} \in \mathbb{Q}[i] \neq \varnothing$
   - Si $a, b, a', b' \in \mathbb{Q}$,
   $$(a + \mathrm{i}b) - (a' + \mathrm{i}b') = (a - a') + \mathrm{i}(b - b') \in \mathbb{Q}[i]$$
   et si $a' + \mathrm{i}b' \neq 0$,
   $$\frac{a + \mathrm{i}b}{a' + \mathrm{i}b'} = \frac{(a + \mathrm{i}b)(a' - \mathrm{i}b')}{a'^2 + b'^2} = \frac{aa' + bb'}{a'^2 + b'^2} + \mathrm{i}\frac{ba' - ab'}{a'^2 + b'^2} \in \mathbb{Q}[i]$$

   Donc $(\mathbb{Q}[i], +, \times)$ est un corps.

---

7. Comme dans la question 4, on démontre que si φ est un endomorphisme de $\mathbb{Q}[\mathrm{i}]$, $\varphi(\mathrm{i}) \in \{\pm \mathrm{i}\}$ et pour tout $k \in \mathbb{Z}$, $\varphi(k) = k$.

   Puis, si $r = \dfrac{p}{q} \in \mathbb{Q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$, alors $\varphi(r) = \varphi\left(\dfrac{p}{q}\right) = \dfrac{\varphi(p)}{\varphi(q)} = \dfrac{p}{q} = r$. Donc pour tout $a, b \in \mathbb{Q}$, $\varphi(a + \mathrm{i}b) = a + \varphi(\mathrm{i})b$.

   Donc les morphismes de corps de $\mathbb{Q}[i]$ sont $z \mapsto z$ et $z \mapsto \overline{z}$.

Solution de 18 :

1. Semblable à la question 6 de l'exercice sur les entiers de Gauß (en remplaçant conjugué par quantité conjuguée).
2. Si f isomorphisme de corps de $\mathbb{Q}(\sqrt{\alpha})$ sur $\mathbb{Q}^2$, alors pour $p\in\mathbb{Z}$ et $q\in\mathbb{N}^*$,
$$f(r)=f\left(\frac{p}{q}\right)=\frac{f(p)}{f(q)}=\frac{pf(1)}{qf(1)}=r1_{\mathbb{Q}^2}=(r,r)$$
puis $f\left(\sqrt{\alpha}^2\right)=f(\alpha)=(\alpha,\alpha)=f\left(\sqrt{\alpha}\right)^2$ donc $f\left(\sqrt{\alpha}\right)=\left(\varepsilon_1\sqrt{\alpha},\varepsilon_2\sqrt{\alpha}\right)$ avec $\varepsilon_1,\varepsilon_2\in\{-1,1\}$ et donc $f\left(\sqrt{\alpha}\right)\notin\mathbb{Q}^2$ ce qui est contradictoire.
3. Si f est un isomorphisme de corps de $\mathbb{Q}(\sqrt{2})$ sur $\mathbb{Q}(\sqrt{3})$, alors pour tout $r\in\mathbb{Q}$, $f(r)=r$ et $2=f(2)=f\left(\sqrt{2}^2\right)=f\left(\sqrt{2}\right)^2$ donc $f\left(\sqrt{2}\right)=\pm\sqrt{2}\in\mathbb{Q}\left(\sqrt{3}\right)$ et $\sqrt{2}\in\mathbb{Q}\left(\sqrt{3}\right)$.
On a alors $r,r'\in\mathbb{Q}$ tels que $\sqrt{2}=r+\sqrt{3}r'$, en élevant au carré, $2=r^2+2\sqrt{3}rr'+3r'^2$ donc $2\sqrt{3}rr'\in\mathbb{Q}$, puis, comme $2\sqrt{3}\notin\mathbb{Q}$, $rr'=0$.
Soit $r'=0$ et $\sqrt{2}=r\in\mathbb{Q}$ ce qui est contradictoire, soit $r=0$ et $\sqrt{2}=\sqrt{3}r'$ donc $\sqrt{6}=3r'\in\mathbb{Q}$ ce qui est aussi contradictoire.

3. Arithmétique entière

Solution de 20 :

1. $(n^3+n)\wedge(2n+1)=1$ si et seulement si
$$n(n^2+1)\wedge(2n+1)=1$$
si et seulement si
$$\begin{cases}n\wedge(2n+1)=1\\(n^2+1)\wedge(2n+1)=1\end{cases}$$
Il s'agit de la propriété $ab\wedge c=1\iff a\wedge c=1$ et $b\wedge c=1$: le sens direct s'obtient avec le théorème de Bézout ou en s'intéressant au diviseurs communs possibles de a et c d'une part et de b et c d'autre part, le sens réciproque s'obtient en multipliant des relations de Bézout : $1=(au+cv)(bu'+cv')=abU+cV\ldots$
Or, en se souvenant de la propriété d'Euclide $a\wedge b=(a-bq)\wedge b$ (pas nécessairement une division euclidienne), on obtient $n\wedge(2n+1)=n\wedge 1=1$ toujours vrai.
Puis, toujours avec cette propriété $(n^2+1)\wedge(2n+1)=(n^2-2n)\wedge(2n+1)=n(n-2)\wedge(2n+1)$.
Donc
$$(n^3+n)\wedge(2n+1)=1\iff\begin{cases}n\wedge(2n+1)=1\\(n-2)\wedge(2n+1)=1\end{cases}\iff(n-2)\wedge(2n+1)=1\iff(n-2)\wedge\big(2n+1-2(n-2)\big)=(n-2)\wedge 5=1$$
Comme 5 est premier, on en déduit que les solutions sont les entiers n tels que $5\nmid(n-2)$ c'est-à-dire tels que $\boxed{n\not\equiv 2\ [5]}$.
2. On écrit $2n^2+9n+13=2(n+2)^2+n+5=2(n+2)^2+(n+2)+3$.
Donc $(n+2)|(2n^2+9n+13)$ si et seulement si $n+2|3$ si et seulement si $n+2\in\{-1,1,-3,3\}$. Les solutions sont $\boxed{-3,-1,-5,1}$ (ce que l'on peut effectivement vérifier).
3. Avec la propriété d'Euclide, si $n\in\mathbb{Z}$,
$$(21n+4)\wedge(14n+3)=\big(21n+4-(14n+3)\big)\wedge(14n+3)=(7n+1)\wedge\big(14n+3-2(7n+1)\big)=(7n+1)\wedge 1=1$$
Autre méthode, avec une relation de Bézout :
$$-2(21n+4)+3(14n+3)=1.$$

Solution de 21 : Nombres de Mersenne[5] - Très classique - Oral Centrale

La factorisation

$$a^n-1=(a-1)(a^{n-1}+\cdots+1)$$

donne la première réponse, puis

$$2^{n_1n_2}-1=(2^{n_1})^{n_2}-1=(2^{n_1}-1)(\ldots)$$

donne la deuxième.

Solution de 22 : Nombres de Fermat[7] - Très classique - Oral Mines

Si n a un facteur premier impair p, on écrit

$$2^n+1=2^{mp}+1=(2^m)^p+1$$

Or on connaît très bien

$$a^n-b^n=(a-b)(\ldots)$$

Mais, si n est impair, remplaçant b par $-b$, on en déduit

$$a^n+b^n=(a+b)(a^{n-1}-ba^{n-2}+\cdots+b^{n-1})$$

Appliqué à notre situation, on trouve

$$2^n+1=(2^m+1)(2^{m(p-1)}-2^{m(p-2)}\cdots+1)$$

On prend bien soin de justifier que c'est une vraie factorisation ($1<2^m+1<2^n+1$). Et on a résolu la première question. Comme souvent, c'est l'exercice classique sur les nombres de Mersenne (si a^n-1 est premier, $a=2$ et n est premier) qui peut donner l'idée

Solution de 23 :

S'intéresser aux diviseurs premiers de $N=4p_1\cdots p_n-1$ si les nombres premiers de la forme $4k-1$ sont exactement $p_1,\ldots,p_n$.

Solution de 24 :

Il suffit de considérer les entiers de $1001!+2$ à $1001!+1001$.

Solution de 25 : Formule de Legendre - Très classique - Oraux divers

Les multiples de q s'écrivent $k=q\ell$ avec $\ell\in\mathbb{Z}$ uniquement déterminé par k et q, et alors $1\leqslant k=q\ell\leqslant n$ si et seulement si $\frac{1}{q}\leqslant\ell\leqslant\frac{n}{q}$ si et seulement si $1\leqslant\ell\leqslant\left\lfloor\frac{n}{q}\right\rfloor$ avec $\ell\in\mathbb{Z}$.

Le nombre de multiples de q entre 1 et n est donc $\left\lfloor\frac{n}{q}\right\rfloor$.

Ainsi, la valuation p-adique de $n!$ avec p premier s'obtient en ajoutant les valuations p-adiques des entiers entre 1 et m, d'après la question précédente :

- les $\left\lfloor\frac{n}{p}\right\rfloor$ multiples de p fournissent chacun (au moins) un facteur p,
- les $\left\lfloor\frac{n}{p^2}\right\rfloor$ multiples de p^2 fournissent chacun (au moins) un facteur p supplémentaire,
- les $\left\lfloor\frac{n}{p^3}\right\rfloor$ multiples de p^3 fournissent chacun (au moins) un facteur p supplémentaire,
- et ainsi de suite.

Le décompte s'arrête car la suite entière $\left(\left\lfloor\frac{n}{p^i}\right\rfloor\right)_{i\in\mathbb{N}^*}$ finit par s'annuler et on obtient la formule de Legendre (avec un nombre fini de termes non nuls) :

$$\boxed{v_p(n!)=\sum_{i=1}^{+\infty}\left\lfloor\frac{n}{p^i}\right\rfloor.}$$

On peut aussi, plus élégamment, remarquer que $v_p(k)=\left|[\![1,v_p(k)]\!]\right|=\left|\left\{i\in\mathbb{N}^*,\ p^i|k\right\}\right|$. Alors

$$v_p(n!)=\sum_{k=1}^{n}v_p(k)=\sum_{k=1}^{n}\sum_{i=1}^{+\infty}\delta_{p^i|k}=\sum_{i=1}^{+\infty}\sum_{k=1}^{n}\delta_{p^i|k}=\sum_{i=1}^{+\infty}\left|\left(p^i\mathbb{N}\right)\cap[\![1,n]\!]\right|=\sum_{i=1}^{+\infty}\left\lfloor\frac{n}{p^i}\right\rfloor.$$

Autre rédaction possible : on peut dénombrer les entiers entre 1 et n ayant une valuation q-adique exactement égale à $i\in\mathbb{N}$: il s'agit des multiples de q^i qui ne sont pas multiples de q^{i+1} et qui sont au nombre de $\left\lfloor\frac{n}{q^i}\right\rfloor-\left\lfloor\frac{n}{q^{i+1}}\right\rfloor$, d'où la formule (les sommes étant toujours faussement infinies)

$$v_p(n!)=\sum_{i=0}^{+\infty}i\cdot\left(\left\lfloor\frac{n}{p^i}\right\rfloor-\left\lfloor\frac{n}{p^{i+1}}\right\rfloor\right)=\sum_{i=1}^{+\infty}i\cdot\left\lfloor\frac{n}{p^i}\right\rfloor-\sum_{i=1}^{+\infty}(i-1)\cdot\left\lfloor\frac{n}{p^i}\right\rfloor=\sum_{i=1}^{+\infty}\left\lfloor\frac{n}{p^i}\right\rfloor.$$

Solution de 28 : Oral Centrale

7

Solution de 29 :

$f : k \mapsto$ (somme des chiffres de k). Calculer $f \circ f \circ f(n)$.

$f(n) \equiv n$ [9]. Or $4444 = 9 \times 493 + 7$, donc $4444 \equiv 7$ [9] et $4444^{4444} \equiv 7^{4444}$ [9].

Mais $7^2 \equiv 4$ [9], $7^3 \equiv -2$ [9] et $7^3 \equiv 1$ [9]. D'où $7^{4444} = 7^{3k+1} \equiv 7$ [9] donc $f(n) \equiv 7$ [9]. Puis $f(f(f(n))) \equiv 7$ [9].

De plus, $n \leqslant 10000^{5000} = 10^{20000}$. Donc n possède au plus 20 000 chiffres et $f(n) \leqslant 9 \times 20000 = 180000$.

Puis $f(f(n)) \leqslant 1 + 8 + 4 \times 9 = 45$ et $f(f(n)) \equiv f(n) \equiv 7$ [9].

Donc $f(f(f(n))) < 4 + 9 = 13$ et $f(f(f(n))) \equiv 7$ [9]. Donc $f(f(f(n))) = 7$.

Solution de 30 : Oral Mines

p est congru à 1 ou à -1 modulo 3 (car $p > 3$), donc $p+1$ ou $p-1$ est divisible par 3. Donc p^2-1, leur produit, l'est. De plus, p, premier et impair car > 2, est congru à 1, 3, 5 ou 7 modulo 8. Donc son carré est congru à 1, 1, 1 ou 1 modulo 8. Donc p^2-1 est divisible par 3 et par 8, qui sont premiers entre eux, il est donc divisible par 24.

Autre méthode : remarquer que parmi $p-1$, p et $p+1$, l'un est divisible par 3 et parmi $p-1$, p, $p+1$, $p+2$, l'un est divisible par 4.

4. Anneaux $\mathbb{Z}/n\mathbb{Z}$

Solution de 39 : Théorème de Wilson (un test de primalité)

1. On suppose que $(p-1)! \equiv -1 \ [p]$, donc que p divise $(p-1)!+1$.
   Si k est un diviseur positif strict de p, alors k divise aussi $(p-1)!$ et $(p-1)!+1$, donc il divise 1 et vaut ainsi 1.
   Cela prouve que p est premier.
2. Réciproquement, on suppose que p est premier.
   (a) On cherche à quelle condition sur $k \in \mathbb{Z}$ on a $k^2 \equiv 1 \ [p]$ soit $(k-1)(k+1) \equiv 0 \ [p]$.
   Comme on travaille dans un corps qui est donc intègre, cela équivaut à $k \equiv \pm 1 \ [p]$.
   (b) En rassemblant les termes du produit par paires, justifier que $(p-1)! \equiv -1 \ [p]$.
   On rassemble dans $(p-1)! = 1 \times 2 \times \cdots \times (p-1)$ (produit de tous les inversibles modulo p) chaque terme avec son inverse modulo p, sauf ceux égaux à leur propre inverse. On obtient

$$(p-1)! \equiv \underbrace{1 \times (-1)}_{\text{égaux à leur inverse}} \times \underbrace{1 \times 1 \cdots \times 1}_{\text{termes rassemblés avec leur inverse}} \equiv -1 \ [p].$$

Solution de 41 :

Soit ϕ un tel morphisme. Si on connaît $\phi(\overline{1})$, on connaît ϕ.

[Plus généralement, pour connaître un morphisme d'un groupe cyclique $(G, *)$ dans un groupe $(H, \cdot)$, il suffit de connaître l'image par ce morphisme d'un générateur de G. En effet, si g est un tel générateur, on a pour tout $n \in \mathbb{Z}$: $\phi(g^n) = (\phi(g))^n$, ce qui donne l'image par ϕ de tous les éléments de G].

Soit $\omega = \phi(\overline{1})$. On a, par propriété de morphisme (en essayant de ne pas trop se tromper de loi : au départ, l'addition, à l'arrivée la multiplication),

$$\phi(n\overline{1}) = \omega^n$$

Mais $n\overline{1} = \overline{n} = \overline{n} = \overline{0}$, et un morphisme transforme l'élément neutre du groupe de départ en l'élément neutre du groupe d'arrivée. Donc $\omega^n = 1$. Et donc $\omega \in \mathbb{U}_n$.

Réciproquement, soit ω un élément de $\mathbb{U}_n$. On montre que l'application

$$\phi_\omega : \left| \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{C}^* \\ \overline{a} & \longmapsto & \omega^a \end{array} \right.$$

est bien définie (il s'agit pour cela de montrer que, si $a \equiv b[n]$, $\omega^a = \omega^b$, ce qui se fait sans trop de mal). C'est assez clairement un morphisme. Les ϕ_ω, $\omega \in \mathbb{U}_n$ sont les morphismes cherchés.

Solution de 42 : Déterminants arithmétiques

1. (a) Si $i,j\in[\![1,n]\!]$,
$$a_{i,j}=\sum_{k|i\text{ et }k|j}\psi(k)=\sum_{k=1}^{n}\delta_{k|i}\psi(k)\delta_{k|j}=\sum_{k=1}^{n}b_{k,i}\psi(k)b_{k,j}=(B^{\mathsf{T}}DB)_{i,j}$$
avec $D=\operatorname{diag}(\psi(1),\dots,\psi(n))$.

   (b) Pour tout i,j, $i|i$ et si $i>j$, $i\nmid j$ donc B est triangulaire supérieure avec des 1 sur la diagonale, donc $\det B=1$.

   (c) On a obtenu dans la question précédente $A=B^{\mathsf{T}}CB$ donc $\det A=\det B^{\mathsf{T}}\det C\det B$. Et comme $\det B^{\mathsf{T}}=\det B=1$ d'après **b)**, $\det A=\det C=\begin{vmatrix}\psi(1)&&\\&\ddots&\\&&\psi(n)\end{vmatrix}$. Finalement, $\boxed{\det A=\prod_{k=1}^{n}\psi(k).}$

2. (a) Remarquons que le nombre de diviseurs communs à i et j est $a_{i,j}=\sum_{k|i\text{ et }k|j}1$. On peut donc appliquer le résultat de la question **1.** avec $\psi\equiv 1$ et donc $\boxed{\det A=1.}$

   (b) Remarquons que la somme des diviseurs communs à i et j est $a_{i,j}=\sum_{k|i\text{ et }k|j}k$. On peut donc appliquer le résultat de la question **1.** avec $\psi=\mathrm{id}$ et donc $\boxed{\det A=\prod_{k=1}^{n}k=k!.}$

3. (a) i. Notons F_k l'ensemble des nombres rationnels de la forme $\frac{q}{m}$ où $1\leqslant q\leqslant m$ qui s'écrivent sous forme irréductible avec k au dénominateur et $E_k=\{\ell\in[\![0,k-1]\!]\mid \ell\wedge k=1\}$ si $k\neq 1$ (remarquons qu'alors $0\notin E_k$), $E_1=\{1\}$.

   L'application $f:\begin{vmatrix}E_k&\longrightarrow&F_k\\ \ell&\longmapsto&\frac{\ell}{k}\end{vmatrix}$ est *bijective*[11]. En effet,

   - si $k=1$, f est l'identité de $F_1=E_1=\{1\}$;
   - sinon,
     - ⋆ elle est *bien définie* car si $\ell\in E_k$, $\frac{\ell}{k}$ est un nombre rationnel de la forme $\frac{q}{m}$ car $k|m$ avec $1\leqslant q\leqslant m$ car $\frac{\ell}{k}\in]0,1]$, qui s'écrit sous forme irréductible avec k au dénominateur car $\ell\wedge k=1$ et donc $f(\ell)\in F_k$;
     - ⋆ elle est *injective* car si $\ell,\ell'\in E_k$ tels que $f(\ell)=f(\ell')$, alors $\frac{\ell}{k}=\frac{\ell'}{k}$ donc $\ell=\ell'$;
     - ⋆ elle est *surjective* car si $r\in F_k$, $r\in\mathbb{Q}\cap]0,1]$ et r s'écrit forme irréductible avec k au dénominateur, donc on a $l\in[\![1,k]\!]$ avec $k\wedge\ell=1$ tel que $r=\frac{\ell}{k}$. Comme $k\neq 1$, $\ell\neq k$ donc $\ell\in[\![1,k-1]\!]$, $\ell\in E_k$ et donc $r=f(\ell)$.

   Ainsi, le nombre de rationnels de la forme $\frac{q}{m}$ où $1\leqslant q\leqslant m$ qui s'écrivent sous forme irréductible avec k au dénominateur est le nombre d'entiers l tels que $0\leqslant l\leqslant k-1$ et $k\wedge l=1$ si $k\neq 1$, 1 sinon : il y en a donc $\varphi(k)$.

   ii. Si on note $F=\left\{\frac{q}{m}\ ;\ 1\leqslant q\leqslant m\right\}$, alors $F=\bigsqcup_{k|m}F_k$ car tout rationnel de F s'écrit de manière unique sous forme irréductible avec un diviseur de m au dénominateur.

   Donc $|F|=\sum_{k|m}|F_k|$, et comme $|F|=|[\![1,m]\!]|=m$, $\boxed{m=\sum_{k|m}\varphi(k)}$ d'après la question précédente.

   (b) $\det\big((i\wedge j)_{i,j}\big)$: D'après la question précédente, pour tous i,j, $i\wedge j=\sum_{k|i\wedge j}\varphi(k)$, donc comme $k|i\wedge j$ si et seulement si $k|i$ et $k|j$, $a_{i,j}=i\wedge j=\sum_{k|i\text{ et }k|j}\varphi(k)$. On peut donc appliquer la question 1. qui nous dit que $\boxed{\det A=\prod_{k=1}^{n}\varphi(k).}$

11. On peut aller un peu plus vite oralement en invoquant simplement l'existence et l'unicité de la forme irréductible des fractions.