DS de mathématiques n°6

Arithmétique, Structures algébriques, Matrices, Systèmes linéaires – Corrigé

Noté sur 130 pts ±5 pts pour le soin et la clarté,
puis la note est ramené sur 20 en multipliant par 1/5.

Glossaire des abbréviations sur la copie :
NJ : Non Justifié. TI : Théorème Inventé. NI : Non Introduit. NEPAP : N'Existe Pas A Priori. PC : Pas Clair. ! : **Grosse lacune à corriger !**

/15 Exercice 1 : Un système linéaire

Soit $\lambda \in \mathbb{R}$. En utilisant la méthode du pivot et en discutant selon les valeurs de λ, résoudre le système suivant :

$$\begin{cases} x+y+\lambda z = \lambda \\ x+(2-\lambda)y+z = 1 \\ \lambda x+y+z = 2-\lambda \end{cases}$$

En matrice augmentée, on obtient :

$$\left(\begin{array}{ccc|c} 1 & 1 & \lambda & \lambda \\ 1 & 2-\lambda & 1 & 1 \\ \lambda & 1 & 1 & 2-\lambda \end{array}\right) \quad \left(\begin{array}{ccc|c} 1 & 1 & \lambda & \lambda \\ 0 & 1-\lambda & 1-\lambda & 1-\lambda \\ 0 & 1-\lambda & 1-\lambda^2 & 2-\lambda-\lambda^2 \end{array}\right) \begin{array}{l} \\ L_2-L_1 \\ L_3-\lambda L_1 \end{array}$$

- Si $\lambda = 1$, la matrice devient :

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

En repassant en système, on en déduit que $x+y+z=1$, ou encore $x = 1-y-z$. Donc

$$\boxed{\mathcal{S} = \left\{(x,y,z) \in \mathbb{R}^3 \mid x = 1-y-z\right\}}$$

- Si $\lambda \neq 1$, $1-\lambda$ est alors un pivot et on peut poursuivre l'algorithme :

$$\left(\begin{array}{ccc|c} 1 & 1 & \lambda & \lambda \\ 0 & 1-\lambda & 1-\lambda & 1-\lambda \\ 0 & 0 & \lambda-\lambda^2 & 1-\lambda^2 \end{array}\right) \begin{array}{l} \\ \\ L_3+L_2 \end{array}$$

La matrice est échelonnée (et ce peu importe si $\lambda-\lambda^2$ est nul ou non). On repasse en système :

$$\begin{cases} x+y+\lambda z = \lambda \\ (1-\lambda)y+(1-\lambda)z = 1-\lambda \\ (\lambda-\lambda^2)z = 1-\lambda^2 \end{cases}$$

(On aimerait diviser par $\lambda-\lambda^2$ dans la troisème équation... Or, $\lambda-\lambda^2 = 0$ ssi $\lambda = 1$ (cas exclu) ou $\lambda = 0$ (cas à traiter)).

- Si $\lambda = 0$, alors la troisième équation donne $0 = 1$. Dans ce cas, le système n'admet pas de solution : $\boxed{\mathcal{S} = \varnothing}$.
- Si $\lambda \neq 0$, alors comme $\lambda \neq 1$, on a $\lambda-\lambda^2 = \lambda(1-\lambda) \neq 0$. Le système devient :

$$\begin{cases} x = \lambda - y - \lambda z \\ y+z = 1 \\ z = \dfrac{(1-\lambda)(1+\lambda)}{\lambda(1-\lambda)} \end{cases} \quad \text{(division par } 1-\lambda \neq 0\text{)}$$

$$\begin{cases} z = \dfrac{1+\lambda}{\lambda} \\ y = 1-z = 1-\dfrac{1+\lambda}{\lambda} \\ x = \lambda - y + 1 + \lambda \end{cases} \quad \begin{cases} z = \dfrac{1+\lambda}{\lambda} = \dfrac{1}{\lambda}+1 \\ y = -\dfrac{1}{\lambda} \\ x = \lambda + \dfrac{1}{\lambda} - (1+\lambda) = \dfrac{1}{\lambda}-1 \end{cases}$$

Finalement, dans ce cas,

$$\boxed{\mathcal{S} = \left\{\left(\frac{1}{\lambda}-1, -\frac{1}{\lambda}, \frac{1}{\lambda}+1\right)\right\}}$$

(λ est une valeur fixée et non une inconnue, ce n'est pas une variable libre et $\mathcal{S}$ ne contient bien qu'un seul élément).

/30,5 **Exercice 2 : Commutant des matrices diagonales**

Soit $n \geq 2$ un entier et $B \in \mathcal{M}_n(\mathbb{C})$. On définit le *commutant* de B comme étant l'ensemble des matrices qui commutent avec B, c'est-à-dire :

$$\mathrm{Com}(B) = \{M \in \mathcal{M}_n(\mathbb{C}) \mid MB = BM\}$$

/3,5 **1)** Montrer que $\mathrm{Com}(B)$ est un sous-groupe de $(\mathcal{M}_n(\mathbb{C}), +)$.

$\mathrm{Com}(B)$ est bien un sous-ensemble de $\mathcal{M}_n(\mathbb{C})$ par définition.

- La matrice nulle de $\mathcal{M}_n(\mathbb{C})$, qu'on notera $0_{n,n}$, commute avec B car $0_{n,n}B = 0_{n,n} = B0_{n,n}$. Ainsi $0_{n,n} \in \mathrm{Com}(B)$.
- Soit $M, N \in \mathrm{Com}(B)$. Montrons que $M - N \in \mathrm{Com}(B)$. On a

$$\begin{aligned}(M-N)B &= MB - NB \\ &= BM - BN \qquad \text{car } M, N \in \mathrm{Com}(B) \\ &= B(M-N)\end{aligned}$$

donc $M - N \in \mathrm{Com}(B)$.

Ainsi, $\mathrm{Com}(B)$ est bien un sous-groupe de $(\mathcal{M}_n(\mathbb{C}), +)$.

Dans la suite, on considère $\lambda_1, \lambda_2, \cdots, \lambda_n$ des nombres complexes et $D = \mathrm{diag}(\lambda_1, \lambda_2, \cdots, \lambda_n)$, i.e. D est la matrice diagonale de $\mathcal{M}_n(\mathbb{C})$ avec pour diagonale les coefficients $\lambda_1, \cdots, \lambda_n$.

/3 **2)** On suppose que $\lambda_1 = \lambda_2 = \ldots = \lambda_n$. Que vaut $\mathrm{Com}(D)$?

On note $\lambda = \lambda_1 = \lambda_2 = \ldots = \lambda_n$, on a donc $D = \lambda I_n$. Montrons que $\mathrm{Com}(D) = \mathcal{M}_n(\mathbb{C})$. Il est clair que $\mathrm{Com}(D) \subset \mathcal{M}_n(\mathbb{C})$. Réciproquement, pour toute matrice M de $\mathcal{M}_n(\mathbb{C})$, on a

$$MD = M(\lambda I_n) = \lambda M I_n = \lambda M$$

et de même on montre que $DM = \lambda M$. Ainsi, $MD = DM$, donc $M \in \mathrm{Com}(D)$. Finalement, $\mathcal{M}_n(\mathbb{C}) \subset \mathrm{Com}(D)$. On en déduit que

$$\boxed{\mathrm{Com}(D) = \mathcal{M}_n(\mathbb{C})}$$

3) On suppose dans toute cette question que $\lambda_1, \cdots, \lambda_n$ sont *distincts* deux à deux. Soit M une matrice quelconque de $\mathcal{M}_n(\mathbb{C})$.

/4 **a)** On pose $L = MD$ et $R = DM$. Pour tous $i, j \in [\![1, n]\!]$, exprimer L_{ij} et R_{ij} en fonction des coefficients de M et de D.

$$L_{ij} = [MD]_{ij} = \sum_{k=1}^{n} M_{ik} D_{kj}$$

Or, D étant diagonale, $D_{kj} = 0$ si $k \neq j$. On en déduit que

$$L_{ij} = M_{ij} D_{jj} = \boxed{\lambda_j M_{ij}}$$

De même, pour la matrice R :

$$R_{ij} = [DM]_{ij} = \sum_{k=1}^{n} D_{ik} M_{kj} = D_{ii} M_{ii} = \boxed{\lambda_i M_{ij}}$$

/6 **b)** En déduire que $\mathrm{Com}(D) = D_n(\mathbb{C})$, où $D_n(\mathbb{C})$ est l'ensemble des matrices diagonales.

On procède par double inclusion. Si $M \in D_n(\mathbb{C})$, alors comme M et D sont diagonales, elles commutent. On a donc $M \in \mathrm{Com}(D)$. Ainsi, $D_n(\mathbb{C}) \subset \mathrm{Com}(D)$.

Montrons l'autre inclusion. Soit $M \in \mathrm{Com}(D)$ et montrons que M est diagonale. Puisque $MD = DM$, on a donc $L = R$, ou encore $L_{ij} = R_{ij}$ pour tous $i, j \in [\![1, n]\!]$. Par la question précédente, on en déduit :

$$\lambda_i M_{ij} = \lambda_j M_{ij} \qquad \text{i.e.} \qquad (\lambda_i - \lambda_j) M_{ij} = 0$$

Si $i = j$, cette égalité ne nous apprend rien ($0 = 0$). En revanche, si $i \neq j$, alors comme $\lambda_i \neq \lambda_j$, on en déduit que $M_{ij} = 0$. Ainsi, pour tous $i, j \in [\![1, n]\!]$ distincts, $M_{ij} = 0$, ce qui entraine que M est diagonale, d'où $M \in D_n(\mathbb{C})$. Donc $\mathrm{Com}(D) \subset D_n(\mathbb{C})$.

2) Déduire de la question précédente qu'il existe exactement 125 matrices M de $\mathcal{M}_4(\mathbb{C})$, que l'on précisera, telles que :

$$M^5 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 32 \end{pmatrix}$$

/14

On raisonne par analyse-synthèse.

- Analyse : soit $M \in \mathcal{M}_4(\mathbb{C})$ une matrice solution. On pose $D = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 32 \end{pmatrix}$ de sorte que $M^5 = D$. En particulier, M commute avec D car
$$MD = MM^5 = M^6 = M^5M = DM$$
De plus, D est diagonale avec des valeurs distinctes deux à deux sur sa diagonale. On en déduit par la question précédente que $\mathrm{Com}(D) = D_n(\mathbb{C})$. Comme $M \in \mathrm{Com}(D)$, on a donc $M \in D_n(\mathbb{C})$. On peut alors écrire
$$M = \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & d \end{pmatrix} \qquad \text{avec } a,b,c,d \in \mathbb{C}$$
Par suite, $M^5 = \begin{pmatrix} a^5 & 0 & 0 & 0 \\ 0 & b^5 & 0 & 0 \\ 0 & 0 & c^5 & 0 \\ 0 & 0 & 0 & d^5 \end{pmatrix} = D$. On en déduit que
$$\begin{cases} a^5 = 0 \\ b^5 = 1 \\ c^5 = -1 \\ d^5 = 32 \end{cases} \quad \begin{cases} a = 0 \\ b \in \{1, \omega, \omega^2, \omega^3, \omega^4\} \\ c \in \{-1, -\omega, -\omega^2, -\omega^3, -\omega^4\} \\ d \in \{2, 2\omega, 2\omega^2, 2\omega^3, 2\omega^4\} \end{cases} \qquad \text{avec } \omega = e^{\frac{2i\pi}{5}}$$
- Synthèse : si on pose
$$M = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & d \end{pmatrix}$$
avec b, c, d appartenant respectivement aux ensembles écrits ci-dessus, on trouve que $M^5 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & b^5 & 0 & 0 \\ 0 & 0 & c^5 & 0 \\ 0 & 0 & 0 & d^5 \end{pmatrix} = D$ donc M est bien solution.

Finalement, on a trouvé toutes les solutions de $M^5 = D$. Il y a 5 choix possibles pour b, 5 pour c et 5 pour d. On en conclut qu'il y a un total de 125 solutions.

/27,5 Exercice 3 : Anneau de Boole

On considère un anneau $(A, +, \cdot)$, dont on note 0 et 1 les éléments neutres respectifs pour les lois $+$ et $\cdot$. On suppose que A vérifie la propriété suivante (on dit que A est un anneau de Boole) :
$$\forall a \in A \quad a^2 = a$$

/3 **1)** En calculant $(a+b)(a+b)$, montrer que pour tout $a, b \in A$, $ab = -ba$.

D'une part,
$$\begin{aligned}(a+b)(a+b) &= a^2 + ab + ba + b^2 \\ &= a + ab + ba + b\end{aligned}$$
car A est un anneau de Boole. D'autre part,
$$(a+b)(a+b) = (a+b)^2 = a + b$$
En égalisant, on trouve
$$a + ab + ba + b = a + b$$
et donc $ab + ba = 0$. Ainsi, $ab = -ba$.

/3,5 **2)** Montrer que pour tout $a \in A$, $a = -a$.

En utilisant le résultat de la question précédente avec $b = a$, on trouve $aa = -aa$, ou encore $a^2 = -a^2$. Comme A est un anneau de Boole, on a donc $a = -a$.

/3 **3)** En déduire que A est un anneau commutatif.

Soit $a, b \in A$. Montrons que $ab = ba$. Par la question 1, on a $ab = -ba$. Or, par la question 2, on a aussi $(ba) = -(ba)$, de sorte que $ab = ba$. D'où le résultat.

/4,5 **4)** Montrer que tous les éléments de A sauf 0 et 1 sont des diviseurs de zéro. On rappelle que $a \in A \backslash \{0\}$ est un diviseur de zéro (pour la loi $\cdot$) s'il existe $b \in A \backslash \{0\}$ tel que $ab = 0$.

Soit $a \in A \setminus \{0, 1\}$. Montrons qu'il existe $b \in A \setminus \{0\}$ tel que $ab = 0$. On pose (après recherche au brouillon) $b = 1 - a$. On a $b \neq 0$ car $a \neq 1$. De plus,
$$ab = a(1-a) = a - a^2 = a - a = 0$$
D'où le résultat voulu.

5) On considère la relation $\leq$ sur A définie par : $a \leq b \iff ab = a$.

/5 **a)** Montrer que $\leq$ est une relation d'ordre sur A.

Soit $a, b, c \in A$.

- On a $a \leq a \iff aa = a \iff a^2 = a$. Comme A est un anneau de Boole, cette dernière assertion est vraie. Donc la relation $\leq$ est réflexive.
- On suppose $a \leq b$ et $b \leq a$. On a donc $ab = a$ et $ba = b$. Comme A est commutatif, on en déduit que $a = ab = ba = b$. Ainsi, $a = b$: la relation $\leq$ est antisymétrique.
- On suppose $a \leq b$ et $b \leq c$. On a donc $ab = a$ et $bc = b$. Par produit, on a donc $abbc = ab$. Comme $bb = b$ (car A est un anneau de Boole), on a donc $abc = ab$. Or, $ab = a$, donc on en déduit que $ac = a$, ou encore $a \leq c$. Ainsi, la relation $\leq$ est transitive.

Finalement, $\leq$ est bien une relation d'équivalence.

/4 **b)** Montrer que pour tous $a, b \in A$, on a $ab \leq a$ et $ab \leq b$.

On a

$$\begin{aligned} ab \leq a &\iff aba = ab \\ &\iff aab = ab \quad \text{car } A \text{ est commutatif} \\ &\iff ab = ab \quad \text{car } aa = a \end{aligned}$$

Cette dernière assertion est vraie. D'où $\boxed{ab \leq a}$. Par ailleurs :

$$\begin{aligned} ab \leq b &\iff abb = ab \\ &\iff ab = ab \quad \text{car } bb = b \end{aligned}$$

Là encore, on en déduit que $\boxed{ab \leq b}$

/4,5 **c)** Montrer que 0 est le plus petit élément de A (pour $\leq$). Quel est le plus grand élément de A ?

Soit $a \in A$. Montrons que $0 \leq a$. On a :

$$0 \leq a \iff 0a = 0$$

Or cette dernière assertion est vraie dans tout anneau. Ainsi, 0 est le plus petit élément de A. Soit $a \in A$. On a :

$$a \leq 1 \iff a1 = a \iff a = a$$

Cette dernière assertion est vraie. Donc 1 est le plus grand élément de A.

/35 Exercice 4 : Triplets pythagoriciens

On appelle triplet pythagoricien tout triplet (x, y, z) d'entiers dans $\mathbb{N}^*$ tel que

$$x^2 + y^2 = z^2$$

Le but de cet exercice est de déterminer tous les triplets pythagoriciens. On raisonne par analyse-synthèse en se donnant un triplet pythagoricien (x, y, z). On note $d = x \wedge y$.

/4,5 **1)** Montrer que pour tous entiers a et b, on a $b \mid a$ si et seulement si $b^2 \mid a^2$.

Supposons que $b \mid a$. Alors il existe $k \in \mathbb{Z}$ tel que $a = bk$. Dans ce cas, $a^2 = b^2k^2$ et comme $k^2 \in \mathbb{Z}$, on a bien $b^2 \mid a^2$.

Réciproquement, supposons $b^2 \mid a^2$. Soit p un nombre premier quelconque. Comme $b^2 \mid a^2$, on en déduit que $v_p(b^2) \leq v_p(a^2)$, ou encore $2v_p(b) \leq 2v_p(a)$. Ainsi, $v_p(b) \leq v_p(a)$. Par arbitraire sur p, on en déduit que $b \mid a$. D'où l'équivalence voulue.

/2,5 **2)** En déduire que d divise z.

On a $d \mid x$ et $d \mid y$, donc par la question précédente, on a $d^2 \mid x^2$ et $d^2 \mid y^2$. On en déduit que $d^2 \mid x^2 + y^2$ donc $d^2 \mid z^2$. En utilisant à nouveau la question précédente, cela conduit à $d \mid z$.

Dans la suite, on pose $x' = \dfrac{x}{d}$, $y' = \dfrac{y}{d}$ et $z' = \dfrac{z}{d}$. Par la question précédente, x', y' et z' sont tous dans $\mathbb{N}^*$.

/1,25 **3)** Montrer que (x', y', z') est un triplet pythagoricien.

En divisant par d^2 l'équation $x^2 + y^2 = z^2$, on trouve $(x')^2 + (y')^2 = (z')^2$. Donc (x', y', z') est un triplet pythagoricien.

/4 **4)** Que peut-on dire de $x' \wedge y'$? Montrer également que $x' \wedge z' = 1$ et $y' \wedge z' = 1$.

En divisant x et y par leurs PGCD, on obtient des nombres premiers entre eux. Ainsi $x' \wedge y' = 1$.

Montrons que $x' \wedge z' = 1$. On pose $D = x' \wedge z'$. Alors $D \mid x'$ et $D \mid z'$ donc (par la question **1)**), on a $D^2 \mid (x')^2$ et $D^2 \mid (z')^2$, donc $D^2 \mid (x')^2 - (z')^2$, ou encore $D^2 \mid (y')^2$. Ainsi, $D \mid y'$. Comme par ailleurs $D \mid x'$, on a donc

$D \mid x' \wedge y'$, si bien que $D \mid 1$. Comme D est positif, on a $D = 1$. On en conclut que $\boxed{x' \wedge z' = 1}$. On montre de même que $y' \wedge z' = 1$.

5) Étant donné a et b sont deux entiers impairs, montrer que a^2+b^2-2 est divisible par 4. **/1,25**

Comme a et b sont impairs, on peut écrire $a = 2k+1$ et $b = 2h+1$ avec $k, h \in \mathbb{Z}$. Alors :

$$\begin{aligned} a^2+b^2-2 &= 4k^2+4k+1+4h^2+4h+1-2 \\ &= 4\left(k^2+k+h^2+h\right) \end{aligned}$$

On en déduit que a^2+b^2-2 est divisible par 4.

6) En déduire que x' et y' ne peuvent pas être tous les deux impairs. **/3,25**

Supposons par l'absurde que x' et y' soient impairs. Alors par la question précédente l'entier $(z')^2-2 = (x')^2+(y')^2-2$ serait divisible par 4.

Or on peut faire une table de congruence modulo 4 :

z'	$(z')^2$	$(z')^2-2$
0	0	-2
1	1	-1
2	0	-2
3	1	-1

et on constate que $(z')^2-2$ ne peut en aucun cas être divisible par 4. Contradiction. D'où x' et y' ne peuvent être tous deux impairs.

7) Montrer que x' et y' sont de parités différentes. Quelle est la parité de z' ? **/2**

Supposons par l'absurde que x' et y' soient pairs. Alors $2 \mid x'$ et $2 \mid y'$ donc $2 \mid x' \wedge y'$ donc $2 \mid 1$. Contradiction. Ainsi, x' et y' ne peuvent être tous les deux pairs. De plus, par la question précédente, x' et y' ne peuvent être tous les deux impairs. Donc x' et y' sont de parités différentes.

De ce fait, on peut considérer deux cas :

- Si x' est pair et y' est impair, on peut écrire $x' = 2k$ et $y' = 2h+1$ avec $k, h \in \mathbb{Z}$. On montre alors facilement que $(x')^2+(y')^2$ est impair. Donc $(z')^2$ est impair. Cela entraine que z' est impair car s'il était pair, on aurait $(z')^2$ pair également.
- Si x' est impair et y' est pair, alors on montre de même que $(z')^2$, donc z' est impair.

Finalement z' est impair.

Note : on pouvait aussi utiliser le fait que z' est premier avec x' et y', donc comme l'un de ces entiers est pair, z' ne peut être divisible par 2.

On suppose, dans la suite, que x' est pair et que y' est impair.

8) On pose $a = \dfrac{x'}{2} \in \mathbb{N}^*$. Montrer qu'il existe deux entiers strictement positifs b et c tels que $b+c = z'$ et $b-c = y'$. En déduire que $a^2 = bc$. **/2,75**

On pose $b = \dfrac{z'+y'}{2}$ et $c = \dfrac{z'-y'}{2}$. Comme z' est impair par la question **7)** et que y' est impair par hypothèse, les entiers $z'+y'$ et $z'-y'$ sont pairs. Ainsi, b et c sont des entiers. De plus, comme $y' > 0$ et $z' > 0$, on a aussi $b > 0$. Enfin, puisque $(z')^2 = (x')^2+(y')^2 > (y')^2$ (car $x' \neq 0$), on en déduit que $z' > y'$ (car z' et y' sont positifs). Ainsi, $z'-y' > 0$ donc $c > 0$.

Montrons que $a^2 = bc$. On a

$$bc = \left(\frac{z'+y'}{2}\right)\left(\frac{z'-y'}{2}\right) = \frac{1}{4}\left((z')^2-(y')^2\right) = \frac{1}{4}(x')^2 = \left(\frac{x'}{2}\right)^2 = a^2$$

D'où le résultat voulu.

9) Montrer que b et c sont premiers entre eux. En déduire qu'il existe deux entiers naturels u et v tels que $b = u^2$ et $c = v^2$. **/7,5**

On pose $D = b \wedge c$. On a $D \mid b$ et $D \mid c$. On en déduit que $D \mid b+c$ et $D \mid b-c$, ou encore $D \mid y'$ et $D \mid z'$. En particulier, $D \mid y' \wedge z'$, càd $D \mid 1$. Comme $D \geq 0$, on en conclut que $D = 1$. D'où b et c sont premiers entre eux.

On a $bc = a^2$. Soit p un nombre premier. Alors $v_p(bc) = v_p(a^2)$, ou encore

$$v_p(b)+v_p(c) = 2v_p(a)$$

De plus, comme $b \wedge c = 1$, on en déduit que $v_p(b \wedge c) = v_p(1) = 0$. Cela entraine que $0 = \min(v_p(b), v_p(c))$. Ainsi $v_p(b) = 0$ ou $v_p(c) = 0$. En particulier, $v_p(c) = 2v_p(a)$ ou $v_p(b) = 2v_p(a)$ et ce pour chaque nombre premier p. On en déduit que chaque valuation de b et de c est paire. Or, si on note $\mathbb{P}$ l'ensemble des nombres premiers, la décomposition de b en produits de facteurs premiers peut s'écrire :

$$b = \prod_{p \in \mathbb{P}} p^{\beta_p}$$

avec $\beta_p = v_p(b) \in \mathbb{N}$. Comme β_p est pair, on peut écrire $\beta_p = 2B_p$ avec $B_p \in \mathbb{N}$. On en conclut que

$$b = \prod_{p\in\mathbb{P}} p^{2B_p} = \left(\prod_{p\in\mathbb{P}} p^{B_p}\right)^2 = u^2 \qquad \text{avec } u = \prod_{p\in\mathbb{P}} p^{B_p} \quad \in \mathbb{N}$$

On montre de même qu'on peut écrire $c = v^2$ avec $v \in \mathbb{N}$.

/1,5 **10)** En déduire que $x = 2duv$, $y = d(u^2 - v^2)$ et $z = d(u^2 + v^2)$.

On remarque que

$$(2uv)^2 = 4u^2v^2 = 4bc = 4a^2 = 4\left(\frac{x'}{2}\right)^2 = (x')^2$$

Ainsi, en passant à la racine carrée, comme $2uv \geq 0$ et $x' \geq 0$, on a $2uv = x'$. D'où $2duv = dx' = x$. De plus,

$$d(u^2 - v^2) = d(b - c) = dy' = y$$

$$d(u^2 + v^2) = d(b + c) = dz' = z$$

D'où les résultats voulus.

/4,5 **11)** Conclure en déterminant tous les triplets pythagoriciens.

Toutes les questions qui précèdent nous montrent que tout triplet pythagoricien peut s'écrire, lorsque x' est pair (et y' impair) :

$$(x, y, z) = (\,2duv, d(u^2 - v^2), d(u^2 + v^2)\,)$$

avec $d, u, v \in \mathbb{N}^*$. Lorsque y' est pair (et x' est impair), en échangeant les rôles de x et y, on montre de même que

$$(x, y, z) = (\,d(u^2 - v^2), 2duv, , d(u^2 + v^2)\,)$$

avec $d, u, v \in \mathbb{N}^*$.

Synthèse : Vérifions si ces triplets sont bien solutions. Prenons le cas

$$(x, y, z) = (\,2duv, d(u^2 - v^2), d(u^2 + v^2)\,)$$

avec $d, u, v \in \mathbb{N}^*$. Tout d'abord, il faut que $v < u$ pour s'assurer que $y > 0$. Avec cette condition, on a bien $x, y, z \in \mathbb{N}^*$. De plus,

$$\begin{aligned} x^2 + y^2 &= (2duv)^2 + (du^2 - dv^2)^2 \\ &= 4d^2u^2v^2 + d^2u^4 + d^2v^4 - 2d^2u^2v^2 \\ &= 2d^2u^2v^2 + d^2u^4 + d^2v^4 \\ &= (du^2 + dv^2)^2 \\ &= z^2 \end{aligned}$$

Ainsi, (x, y, z) est bien solution. On montre de même que la seconde famille de triplets est solution si et seulement si $v < u$. Finalement,

$$\begin{aligned} \mathcal{S} = &\left\{ \left(2duv,\, du^2 - dv^2,\, du^2 + dv^2\right) \,\middle|\, d, u, v \in \mathbb{N}^*,\, v < u \right\} \\ &\bigcup \left\{ \left(du^2 - dv^2,\, 2duv,\, du^2 + dv^2\right) \,\middle|\, d, u, v \in \mathbb{N}^*,\, v < u \right\} \end{aligned}$$

/22 Exercice 5 : Arithmétique sur le groupe $\mathbb{U}_n$

Soit $n \in \mathbb{N}^*$. On rappelle que $\mathbb{U}_n$ est l'ensemble des racines n-ièmes de l'unité, défini par $\mathbb{U}_n = \{z \in \mathbb{C}^* \mid z^n = 1\}$. On admet que $(\mathbb{U}_n, \times)$ est un groupe abélien. Pour tout $\omega \in \mathbb{U}_n$, on définit l'ensemble dit "engendré par ω" par :

$$G_\omega = \{\omega^q \mid q \in \mathbb{N}^*\} = \left\{\omega,\, \omega^2,\, \omega^3,\, \cdots\right\}$$

/1,5 **1)** Montrer que $G_\omega \subset \mathbb{U}_n$.

Comme $\omega \in \mathbb{U}_n$, et que $(\mathbb{U}_n, \times)$ est un groupe, on a $\omega^2 = \omega \times \omega \in \mathbb{U}_n$. Par récurrence immédiate, on en déduit que pour tout $q \in \mathbb{N}^*$, $\omega^q \in \mathbb{U}_n$. Finalement, $\boxed{G_\omega \subset \mathbb{U}_n}$.

2) Dans cette question, on suppose $n = 6$ et on pose $u = e^{\frac{2i\pi}{6}}$. Expliciter l'ensemble $\mathbb{U}_6$ en fonction de u, puis expliciter (sans justification) les ensembles G_u, G_{u^2}, G_{u^3} et G_{u^5} en fonction de u. Combien d'éléments possèdent ces ensembles ?

/1,5

$$\mathbb{U}_6 = \left\{ e^{\frac{2ik\pi}{6}} \,\middle|\, k \in [\![0, 5]\!] \right\} = \boxed{\left\{1, u, u^2, u^3, u^4, u^5\right\}}$$

$$G_u = \boxed{\left\{u, u^2, u^3, u^4, u^5, 1\right\}} \qquad \text{donc } G_u \text{ possède 6 éléments}$$

$$G_{u^2} = \boxed{\left\{u^2, u^4, 1\right\}} \qquad \text{donc 3 éléments}$$

$$G_{u^3} = \boxed{\{u^3, 1\}} \qquad \text{donc 2 éléments}$$

$$G_{u^5} = \boxed{\{u^5, u^4, u^3, u^2, u, 1\}} \qquad \text{donc 6 éléments}$$

/2,75 **3)** Montrer que $(G_\omega, \times)$ est un groupe.

Montrons que G_ω est un sous-groupe de $\mathbb{U}_n$. Par la question 1, on a bien $G_\omega \subset \mathbb{U}_n$.

- Montrons que $1 \in G_\omega$. Par définition de G_ω, on sait que $\omega^n \in G_\omega$. Or $\omega^n = 1$ d'où $1 \in G_\omega$. *Note : fait rare, il eût été plus rapide de montrer que G_ω est non vide.*
- Soit $x, y \in G_\omega$. Montrons que $xy \in G_\omega$. Comme $x, y \in G_\omega$, il existe $p, q \in \mathbb{N}^*$ tels que $x = \omega^p$ et $y = \omega^q$. Alors $xy = \omega^p\omega^q = \omega^{p+q} \in G_\omega$ (car $p + q \in \mathbb{N}^*$).
- Soit $x \in G_\omega$. Montrons que $x^{-1} \in G_\omega$. Là encore, $x = \omega^p$ avec $p \in \mathbb{N}^*$. Dans ce cas, $x^{-1} = \omega^{-p}$. On réalise la division euclidienne de $-p$ par n : il existe donc des entiers q, r tels que

$$-p = nq + r \qquad \text{avec } 0 \leq r < n$$

Ainsi :

$$\omega^{-p} = \omega^{nq+r} = (\omega^n)^q\omega^r = 1^q\omega^r = \omega^r$$

Si $r = 0$, alors $\omega^r = 1 \in G_\omega$. Si $r \neq 0$, alors $r \in \mathbb{N}^*$ donc $\omega^r \in G_\omega$ par définition de G_ω. Finalement, $\omega^{-p} \in G_\omega$.

Finalement, G_ω est bien un groupe.

4) Dans cette question, on fixe $k \in [\![0, n-1]\!]$, $\omega = e^{\frac{2ik\pi}{n}}$ et on définit l'ordre de ω comme étant le plus petit entier $p \geq 1$ tel que $\omega^p = 1$.

/3,25 **a)** Montrer que pour tout $q \in \mathbb{N}^*$, on a $n \mid kq$ si et seulement si q est un multiple de l'entier $n' = \dfrac{n}{k \wedge n}$.

On pose $d = n \wedge k$, et $k' = \dfrac{k}{d}$. Comme $n' = \dfrac{n}{d}$, on a

$$n \mid kq \iff dn' \mid dk'q \iff n' \mid k'q \qquad \text{car } d \neq 0$$

On veut montrer que $n' \mid k'q \iff n' \mid q$. Le sens réciproque est évident. Supposons $n' \mid k'q$. Comme $n' = \dfrac{n}{d}$ et $k' = \dfrac{k}{d}$, on en déduit que n' et k' sont premiers entre eux. Ainsi, par le lemme de Gauss, on a $n' \mid q$. D'où le résultat.

/1,25 **b)** Dans cette question, on suppose $n = 6$. Donner l'ordre de chaque élément de $\mathbb{U}_6$.

On a vu que $\mathbb{U}_6 = \{1, u, u^2, u^3, u^4, u^5\}$ avec $u = e^{\frac{2i\pi}{6}}$.

- Il est clair que 1 est d'ordre 1.
- u^3 est d'ordre 2.
- u^2 et u^4 sont d'ordre 3.
- u et u^5 sont d'ordre 6.

/3,75 **c)** Montrer que l'ordre de ω est $\dfrac{n}{k \wedge n}$.

On pose $n' = \dfrac{n}{k \wedge n}$. Pour montrer que l'ordre de ω est n', il faut montrer que :

- $\omega^{n'} = 1$
- Pour tout $q \in [\![1, n'-1]\!]$, on a $\omega^q \neq 1$.

Soit $q \in [\![1, n'-1]\!]$. Montrons que $\omega^q \neq 1$. Supposons par l'absurde que $\omega^q = 1$. Alors :

$$\begin{aligned}
&\left(e^{\frac{2ik\pi}{n}}\right)^q = 1 \\
\implies &e^{\frac{2ikq\pi}{n}} = 1 \\
\implies &\frac{2\pi kq}{n} \equiv 0\ [2\pi] \\
\implies &kq \equiv 0\ [n] \\
\implies &n \mid kq \\
\implies &n' \mid q \qquad \text{par la question 4.a)}
\end{aligned}$$

Or, $1 \leq q < n'$, donc ceci est contradictoire. D'où $\omega^q \neq 1$. Montrons à présent que $\omega^{n'} = 1$. On a

$$\begin{aligned}
\omega^{n'} = \left(e^{\frac{2ik\pi}{n}}\right)^{n'} &= \exp\left(\frac{2ik\pi}{n} \times n'\right) \\
&= \exp\left(\frac{2ik\pi}{k \wedge n}\right) \\
&= \exp\left(2ik'\pi\right) \qquad \text{avec } k' = \frac{k}{k \wedge n} \in \mathbb{Z} \\
&= 1 \qquad\qquad\qquad\quad \text{car } k' \in \mathbb{Z}
\end{aligned}$$

/4 **d)** Montrer que si $k \wedge n = 1$, alors $G_\omega = \mathbb{U}_n$.

L'inclusion $G_\omega \subset \mathbb{U}_n$ est évidente. Montrons l'autre inclusion. Soit $x \in \mathbb{U}_n$. Alors il existe $m \in [\![0, n-1]\!]$ tel que

$$x = \exp\left(\frac{2im\pi}{n}\right)$$

Montrons que $x \in G_\omega$, i.e. qu'il existe $q \in \mathbb{N}^*$ tel que $x = \omega^q$. Or,

$$\omega^q = \exp\left(q\frac{2ik\pi}{n}\right)$$

Et par suite,

$$\begin{aligned} x = \omega^q &\iff \frac{2m\pi}{n} \equiv q\frac{2k\pi}{n} \ [2\pi] \\ &\iff m \equiv qk \ [n] \\ &\iff qk \equiv m \ [n] \end{aligned}$$

Comme $k \wedge n = 1$, il existe $c \in \mathbb{Z}$ tel que $kc \equiv 1 \ [n]$. On en déduit que $x = \omega^q \iff q \equiv mc \ [n]$. Ainsi, on peut poser

$$q = mc + An \qquad \text{avec } A \in \mathbb{N} \text{ assez grand pour assurer que } q \geq 1$$

Dans ce cas, on a bien $x = \omega^q$, donc $x \in G_\omega$. Ainsi, $\boxed{G_\omega = \mathbb{U}_n}$.

/4 **5)** On pose $\mathbb{U}_\infty = \bigcup_{n=1}^{+\infty} \mathbb{U}_n$. Montrer que $(\mathbb{U}_\infty, \times)$ est un groupe, et que $\mathbb{U}_\infty \neq \mathbb{U}$.

Montrons que $\mathbb{U}_\infty$ est un sous-groupe de $(\mathbb{C}^*, \times)$

Comme pour tout $n \in \mathbb{N}^*$ on a $\mathbb{U}_n \subset \mathbb{C}^*$, on en déduit que $\mathbb{U}_\infty \subset \mathbb{C}^*$.

- $1 \in \mathbb{U}_1$ donc $1 \in \mathbb{U}_\infty$.
- Soit $x, y \in \mathbb{U}_\infty$. Montrons que $xy^{-1} \in \mathbb{U}_\infty$. Par définition de $\mathbb{U}_\infty$, il existe $N, M \in \mathbb{N}^*$ tels que $x \in \mathbb{U}_N$ et $y \in \mathbb{U}_M$. Montrons que $xy^{-1} \in \mathbb{U}_{NM}$. On a
$$\left(xy^{-1}\right)^{NM} = \frac{x^{NM}}{y^{NM}} = \frac{(x^N)^M}{(y^M)^N} = \frac{1^M}{1^N} = 1$$
On peut donc affirmer que $xy^{-1} \in \mathbb{U}_{NM}$, d'où $xy^{-1} \in \mathbb{U}_\infty$.

Finalement, $\mathbb{U}_\infty$ est bien un sous-groupe de $\mathbb{C}^*$, donc un groupe pour la loi $\times$.

Montrons que $\mathbb{U}_\infty \neq \mathbb{U}$. On pose $x = e^i = e^{i\times 1}$. Il est clair que $x \in \mathbb{U}$. Supposons par l'absurde que $x \in \mathbb{U}_\infty$. Alors, il existe $n \in \mathbb{N}^*$ tel que $x^n = 1$. Cependant :

$$\begin{aligned} x^n = 1 &\iff e^{i\,n} = 1 \\ &\iff n \equiv 0 \ [2\pi] \\ &\iff \exists k \in \mathbb{Z}^* \quad n = 2k\pi \qquad (\text{on a } k \neq 0 \text{ car } n > 0) \\ &\iff \exists k \in \mathbb{Z}^* \quad \pi = \frac{n}{2k} \end{aligned}$$

Or, on sait que π est irrationnel, on aboutit donc à une contradiction. Ainsi, $x \notin \mathbb{U}_\infty$. Cela permet de conclure que $\boxed{\mathbb{U} \neq \mathbb{U}_\infty}$.