

DS n°6 : corrigé

Exercice 1 : la confiture à la Chandeleur (21 pts)

1) Résoudre dans \mathbb{Z}^2 l'équation $13x + 18y = 1$. (7 pts)

$13 \wedge 18 = 1$ et $1 \mid 1$, donc l'équation admet des solutions.

Cherchons un couple de coefficients de Bézout pour 13 et 18.

	18	13		
18 = 13 × 1 + 5	5 = 18 - 13 × 1	18	1	0
13 = 5 × 2 + 3	3 = 13 - 5 × 2	13	0	1
5 = 3 × 1 + 2	2 = 5 - 3 × 1	5	1	-1
3 = 2 × 1 + 1	1 = 3 - 2 × 1	3	-2	3
		2	3	-4
		1	-5	7

(On peut omettre le détail du calcul ci-dessus) On a $13 \times 7 + 18 \times (-5) = 1$. Par conséquent $(7, -5)$ est solution particulière de l'équation.

On a alors

$$\mathcal{S} = \{(7 - 18k, -5 + 13k) \mid k \in \mathbb{Z}\}$$

2) Résoudre dans \mathbb{Z}^2 l'équation $13x + 18y = 200$. (2 pts)

Puisque

$$13 \times 7 + 18 \times (-5) = 1$$

on obtient que

$$13 \times 1400 + 18 \times (-1000) = 200$$

et donc $(1400, -1000)$ est solution particulière de $13x + 18y = 200$. On en déduit que

$$\mathcal{S} = \{(1400 - 18k, -1000 + 13k) \mid k \in \mathbb{Z}\}$$

3) Parmi les solutions trouvées à la question précédente, déterminer celles qui sont dans \mathbb{N}^2 . On pourra utiliser les divisions euclidiennes suivantes :

$$1000 = 76 \times 13 + 12 \qquad 1400 = 77 \times 18 + 14$$

(9 pts)

Soit $k \in \mathbb{Z}$ et $(x, y) = (1400 - 18k, -1000 + 13k)$ une solution de l'équation.

$$\begin{aligned}
 (x, y) \in \mathbb{N}^2 &\iff \begin{cases} 1400 - 18k \geq 0 \\ -1000 + 13k \geq 0 \end{cases} \\
 &\iff \begin{cases} 18k \leq 1400 \\ 13k \geq 1000 \end{cases} \\
 &\iff \begin{cases} 18k \leq 77 \times 18 + 14 \\ 13k \geq 76 \times 13 + 12 \end{cases} \\
 &\iff \begin{cases} k \leq 77 + \frac{14}{18} \\ k \geq 76 + \frac{12}{13} \end{cases}
 \end{aligned}$$

Or, k étant entier, la première équation impose $k \leq 77$, et la seconde $k > 76$. D'où $k = 77$. On a ainsi

$$x = 1400 - 18 \times 77 = 14$$

$$y = -1000 + 13 \times 77 = -(76 \times 13 + 12) + 13 \times 77 = 13 - 12 = 1$$

Il y a donc une unique solution $(14, 1) \in \mathbb{N}^2$.

4) Répondre au problème posé. (3 pts)

x étant le nombre de crêpes, et y étant le nombre de gaufres, le groupe d'élèves devra nécessairement faire

14 crêpes et une gaufre

Problème 1 : Anneau $\mathbb{Z}[\sqrt{2}]$ (36 pts)

On considère l'ensemble $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$.

1) Montrer que $(\mathbb{Z}[\sqrt{2}], +, \times)$ est un anneau. (8 pts)

$\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$ donc il suffit de montrer que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de \mathbb{R} :

- $1 = 1 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$
- Soit $x, y \in \mathbb{Z}[\sqrt{2}]$, on pose $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$. Alors

$$\begin{aligned}
 x - y &= (a + b\sqrt{2}) - (c + d\sqrt{2}) \\
 &= (a - c) + (b - d)\sqrt{2}
 \end{aligned}$$

et comme $a - c \in \mathbb{Z}$ et $b - d \in \mathbb{Z}$, $x - y \in \mathbb{Z}[\sqrt{2}]$.

- Avec les mêmes notations,

$$\begin{aligned}
 xy &= (a + b\sqrt{2})(c + d\sqrt{2}) \\
 &= ac + ad\sqrt{2} + bc\sqrt{2} + 2bd \\
 &= (ac + 2bd) + (ad + bc)\sqrt{2}
 \end{aligned}$$

et comme $ac + 2bd \in \mathbb{Z}$ et $ad + bc \in \mathbb{Z}$, on en déduit que $xy \in \mathbb{Z}[\sqrt{2}]$

Ainsi, $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de \mathbb{R} .

2) Montrer que l'anneau $(\mathbb{Z}[\sqrt{2}], +, \times)$ est commutatif et intègre. (5 pts)

Montrons que $\mathbb{Z}[\sqrt{2}]$ est commutatif. Soit $x, y \in \mathbb{Z}[\sqrt{2}]$. Comme $x, y \in \mathbb{R}$ (et que \times est commutative sur \mathbb{R}), on a

$$xy = yx$$

et donc $\mathbb{Z}[\sqrt{2}]$ est commutatif. Montrons que $\mathbb{Z}[\sqrt{2}]$ est intègre. Soit $x, y \in \mathbb{Z}[\sqrt{2}]$ tels que $xy = 0$. Alors, comme $x, y \in \mathbb{R}$ et que \mathbb{R} est intègre, on a nécessairement $x = 0$ ou $y = 0$. Ainsi, $\mathbb{Z}[\sqrt{2}]$ est intègre.

3) Pour tout $x = a + b\sqrt{2}$ dans $\mathbb{Z}[\sqrt{2}]$, on pose $N(x) = a^2 - 2b^2$.

a) Montrer que l'application

$$\begin{aligned} N : \mathbb{Z}[\sqrt{2}] &\rightarrow \mathbb{Z} \\ x &\mapsto N(x) \end{aligned}$$

vérifie la propriété suivante : $\forall x, y \in \mathbb{Z}[\sqrt{2}] \quad N(xy) = N(x)N(y)$. (6 pts)

Soit $x, y \in \mathbb{Z}[\sqrt{2}]$. On pose $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$. Alors

$$\begin{aligned} N(x)N(y) &= N(a + b\sqrt{2})N(c + d\sqrt{2}) \\ &= (a^2 - 2b^2)(c^2 - 2d^2) \\ &= a^2c^2 - 2a^2d^2 - 2b^2c^2 + 4b^2d^2 \end{aligned}$$

$$\begin{aligned} N(xy) &= N\left((ac + 2bd) + (ad + bc)\sqrt{2}\right) \\ &= (ac + 2bd)^2 - 2(ad + bc)^2 \\ &= a^2c^2 + 4b^2d^2 + 4abcd - 2(a^2d^2 + b^2c^2 + 2abcd) \\ &= a^2c^2 + 4b^2d^2 - 2a^2d^2 - 2b^2c^2 \end{aligned}$$

On a donc bien $N(xy) = N(x)N(y)$.

b) Rappeler (sans justification) quels éléments de \mathbb{Z} sont inversibles (pour la multiplication). (2 pts)

1 et -1 sont les seuls éléments inversibles dans \mathbb{Z} (on a vu que le groupe des inversibles de \mathbb{Z} est $\{-1, 1\}$).

c) Dédurre des questions précédentes que si x est inversible dans $\mathbb{Z}[\sqrt{2}]$ (pour la multiplication), alors $N(x) \in \{-1, 1\}$. (7 pts)

Soit $x \in \mathbb{Z}[\sqrt{2}]$ inversible. Alors

$$\begin{aligned} N(x)N(x^{-1}) &= N(xx^{-1}) = N(1) \\ &= N(1 + 0\sqrt{2}) = 1 - 2 \times 0^2 = 1 \end{aligned}$$

Ainsi, $N(x)$ est inversible dans \mathbb{Z} . Par la question précédente, on en déduit que $N(x) \in \{-1, 1\}$.

3) En déduire que $x \in \mathbb{Z}[\sqrt{2}]$ est inversible si et seulement si $x = a + b\sqrt{2}$, avec $a^2 - 2b^2 \in \{-1, 1\}$. (8 pts)

D'après la question précédente, si x est inversible dans $\mathbb{Z}[\sqrt{2}]$, alors en posant $x = a + b\sqrt{2}$, on a $N(x) = a^2 - 2b^2 \in \{-1, 1\}$.

Montrons la réciproque. Supposons $x = a + b\sqrt{2}$ tel que $a^2 - 2b^2 \in \{-1, 1\}$ et montrons que x est inversible dans $\mathbb{Z}[\sqrt{2}]$.

- Si $a^2 - 2b^2 = 1$, alors $(a - b\sqrt{2})(a + b\sqrt{2}) = 1$. De plus $a - b\sqrt{2} = a + (-b)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Donc $a + b\sqrt{2}$ est inversible d'inverse $a - b\sqrt{2}$.
- Si $a^2 - 2b^2 = -1$, alors $(a - b\sqrt{2})(a + b\sqrt{2}) = -1$, donc

$$(-a + b\sqrt{2})(a + b\sqrt{2}) = 1$$

On montre de même que $-a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Ainsi, $a + b\sqrt{2}$ est inversible.

On a donc bien montré l'équivalence.

Exercice 2 : Un groupe avec deux lois (24 pts)

Soit (G, \cdot) un groupe et $a \in G$. On définit une loi de composition interne \top sur G par

$$x \top y = xay$$

Pour tout $x \in G$, on notera x^{-1} son symétrique pour \cdot , et (lorsqu'il existe) x' son symétrique pour \top .

1) Montrer que (G, \top) est un groupe. (10 pts)

Soit $x, y, z \in G$.

- $x \top y = xay$ et comme \cdot est une l.c.i. sur G , on a $xay \in G$. Ainsi, $x \top y \in G$ et \top est une l.c.i. sur G .
- Comme \cdot est associative,

$$(x \top y) \top z = (xay)az = xa(yaz) = x \top (y \top z)$$

Donc \top est associative.

- On a

$$x \top a^{-1} = xaa^{-1} = x$$

$$a^{-1} \top x = a^{-1}ax = x$$

donc a^{-1} est l'élément neutre pour \top .

- Enfin,

$$x \top (a^{-1}x^{-1}a^{-1}) = xaa^{-1}x^{-1}a^{-1} = xx^{-1}a^{-1} = a^{-1}$$

$$(a^{-1}x^{-1}a^{-1}) \top x = a^{-1}x^{-1}a^{-1}ax = a^{-1}x^{-1}x = a^{-1}$$

Ainsi, x est symétrisable pour \top et $x' = a^{-1}x^{-1}a^{-1}$.

Finalement, (G, \top) est un groupe.

2) Soit $\varphi : G \rightarrow G$ définie par $\varphi(x) = xa^{-1}$. Montrer que φ est un morphisme de (G, \cdot) dans (G, \top) . (6 pts)

Soit $x, y \in G$.

$$\varphi(xy) = xya^{-1}$$

$$\varphi(x) \top \varphi(y) = (xa^{-1}) \top (ya^{-1}) = xa^{-1}aya^{-1} = xya^{-1}$$

On a donc bien $\varphi(xy) = \varphi(x) \top \varphi(y)$. φ est donc un morphisme de (G, \cdot) dans (G, \top) .

3) Est-ce que φ est un endomorphisme ? Un isomorphisme ? Un automorphisme ? (8 pts)

φ n'est pas un endomorphisme, car les lois sur les ensembles de départ et d'arrivée ne sont pas identiques. En particulier, φ n'est pas un automorphisme.

Vérifions si φ est bijective. Soit $y \in G$. Résolvons l'équation $\varphi(x) = y$ d'inconnue $x \in G$.

$$\varphi(x) = y \iff xa^{-1} = y \iff x = ya$$

Pour tout $y \in G$, l'équation $\varphi(x) = y$ admet une unique solution $x = ya$. Ainsi, φ est bijective. Comme φ est de plus un morphisme, il s'agit donc d'un isomorphisme.

(Remarque : on pouvait aussi poser

$$f : G \rightarrow G \\ x \mapsto xa$$

et montrer que $\varphi \circ f = f \circ \varphi = id_G$).

Problème 2 : suite récurrente linéaire d'ordre 3 (41 pts)

$$\begin{cases} u_{n+3} = u_{n+2} + u_{n+1} - u_n & \text{pour tout } n \in \mathbb{N} \\ u_2 = -1 \\ u_1 = 1 \\ u_0 = 0 \end{cases}$$

$$U_n = \begin{pmatrix} u_{n+2} \\ u_{n+1} \\ u_n \end{pmatrix} \quad A = \begin{pmatrix} 1 & 1 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

1) Montrer que pour tout $n \in \mathbb{N}$, $U_{n+1} = AU_n$. En déduire une expression de U_n en fonction de A , n et U_0 . (4 pts)

$$AU_n = \begin{pmatrix} 1 & 1 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} u_{n+2} \\ u_{n+1} \\ u_n \end{pmatrix} = \begin{pmatrix} u_{n+2} + u_{n+1} - u_n \\ u_{n+2} \\ u_{n+1} \end{pmatrix} = \begin{pmatrix} u_{n+3} \\ u_{n+2} \\ u_{n+1} \end{pmatrix} = U_{n+1}$$

Ainsi, par récurrence immédiate,

$$U_n = A^n U_0$$

2) Déterminer les valeurs des réels x, y, z, t, u, v tels que la matrice $P = \begin{pmatrix} 1 & 1 & 1 \\ x & y & z \\ t & u & v \end{pmatrix}$ vérifie $AP = PB$. (6 pts)

On a

$$AP = \begin{pmatrix} 1 & 1 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ x & y & z \\ t & u & v \end{pmatrix} = \begin{pmatrix} 1+x-t & 1+y-u & 1+z-v \\ 1 & 1 & 1 \\ x & y & z \end{pmatrix}$$

$$PB = \begin{pmatrix} 1 & 1 & 1 \\ x & y & z \\ t & u & v \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & -1 \\ x & x+y & -z \\ t & t+u & -v \end{pmatrix}$$

Ainsi, $AP = PB$ si et seulement si

$$\begin{cases} 1 = 1 + x - t \\ 2 = 1 + y - u \\ -1 = 1 + z - v \\ 1 = x \\ 1 = x + y \\ 1 = -z \\ x = t \\ y = t + u \\ z = -v \end{cases} \quad \begin{cases} x = 1 \\ z = -1 \\ t = x = 1 \\ v = -z = 1 \\ y = 1 - x = 0 \\ u = y - t = -1 \\ 1 = 1 + (1) - (1) \\ 2 = 1 + (0) - (-1) \\ -1 = 1 + (-1) - (1) \end{cases}$$

On trouve donc une unique solution :

$$P = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & -1 \\ 1 & -1 & 1 \end{pmatrix}$$

3) On admet que $P^{-1} = \frac{1}{4} \begin{pmatrix} 1 & 2 & 1 \\ 2 & 0 & -2 \\ 1 & -2 & 1 \end{pmatrix}$. Montrer que $A = PBP^{-1}$. (2 pts)

Comme $AP = PB$ et qu'on admet que P est inversible, alors $A = PBP^{-1}$.

(Cette façon de faire est correcte, mais on peut aussi faire le calcul complet pour vérifier que la matrice P est correcte). Par la question précédente,

$$\begin{aligned} PBP^{-1} &= \begin{pmatrix} 1 & 2 & -1 \\ x & x+y & -z \\ t & t+u & -v \end{pmatrix} P^{-1} \\ &= \begin{pmatrix} 1 & 2 & -1 \\ 1 & 1 & 1 \\ 1 & 0 & -1 \end{pmatrix} \times \frac{1}{4} \begin{pmatrix} 1 & 2 & 1 \\ 2 & 0 & -2 \\ 1 & -2 & 1 \end{pmatrix} \\ &= \frac{1}{4} \begin{pmatrix} 4 & 4 & -4 \\ 4 & 0 & 0 \\ 0 & 4 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = A \end{aligned}$$

4) En déduire A^n en fonction de P , B et n . (5 pts)

Par la question précédente,

$$\begin{aligned} A^n &= \underbrace{(PBP^{-1})(PBP^{-1}) \dots (PBP^{-1})}_{n \text{ fois}} \\ &= P \underbrace{BB \dots B}_{n \text{ fois}} P^{-1} \quad \text{par associativité et puisque } P^{-1}P = I_n \\ &= PB^n P^{-1} \end{aligned}$$

5) On introduit les matrices suivantes :

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \quad N = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Déterminer N^n et D^n pour tout $n \in \mathbb{N}$. (4 pts)

D étant diagonale, pour tout $n \in \mathbb{N}^*$

$$D^n = \begin{pmatrix} 1^n & 0 & 0 \\ 0 & 1^n & 0 \\ 0 & 0 & (-1)^n \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (-1)^n \end{pmatrix}$$

et par ailleurs $D^0 = I_n$ par convention. Pour la matrice N , on a $N^0 = I_n$, $N^1 = N$ et

$$N^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = 0$$

Ainsi, pour tout $n \geq 2$, on a $N^n = N^2 N^{n-2} = 0 N^{n-2} = 0$. Donc on a déterminé N^n pour tout $n \in \mathbb{N}$.

6) En déduire B^n pour tout $n \in \mathbb{N}$. (10 pts)

On remarque que $B = D + N$. Or,

$$DN = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$ND = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

donc par la formule du binôme

$$B^n = (D + N)^n = \sum_{k=0}^n \binom{n}{k} N^k D^{n-k}$$

Distinguons des cas :

- Si $n \leq 1$, on a directement $B^n = \begin{cases} B & \text{si } n = 1 \\ I_3 & \text{si } n = 0 \end{cases}$

- Si $n \geq 2$, alors

$$\begin{aligned}
B^n &= \sum_{k=0}^1 \binom{n}{k} N^k D^{n-k} + \sum_{k=2}^n \binom{n}{k} N^k D^{n-k} \\
&= \binom{n}{0} N^0 D^{n-0} + \binom{n}{1} N^1 D^{n-1} + 0 && (\text{car } N^k = 0 \text{ si } k \geq 2) \\
&= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (-1)^n \end{pmatrix} + n \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (-1)^{n-1} \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (-1)^n \end{pmatrix} + n \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \\
&= \begin{pmatrix} 1 & n & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (-1)^n \end{pmatrix}
\end{aligned}$$

7) Déterminer u_n pour tout $n \in \mathbb{N}$. (10 pts)

Si $n \leq 2$, on connaît u_n par définition. Soit donc $n \geq 3$. Pour déterminer u_n , il suffit de connaître le dernier coefficient de U_n .

Par la question 1, $U_n = A^n U_0$. Par la question 4, on a donc $U_n = P B^n P^{-1} U_0$. Par la question 6, comme $n \geq 3$,

$$\begin{aligned}
U_n &= P B^n P^{-1} U_0 \\
&= \frac{1}{4} P B^n \begin{pmatrix} 1 & 2 & 1 \\ 2 & 0 & -2 \\ 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} \\
&= \frac{1}{4} P \begin{pmatrix} 1 & n & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (-1)^n \end{pmatrix} \begin{pmatrix} 1 \\ -2 \\ -3 \end{pmatrix} \\
&= \frac{1}{4} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & -1 \\ 1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 - 2n \\ -2 \\ -3(-1)^n \end{pmatrix} \\
&= \frac{1}{4} \begin{pmatrix} * \\ * \\ 1 - 2n + 2 - 3(-1)^n \end{pmatrix}
\end{aligned}$$

(seul le dernier coefficient nous intéresse). D'où

$$\begin{pmatrix} * \\ * \\ u_n \end{pmatrix} = U_n = \frac{1}{4} \begin{pmatrix} * \\ * \\ (3 - 3(-1)^n - 2n) \end{pmatrix}$$

Finalement, pour tout $n \geq 3$,

$$\boxed{u_n = \frac{1}{4} (3 - 3(-1)^n - 2n)}$$

Pour se rassurer (et laisser une bonne impression au correcteur), on peut regarder si la formule marche

pour $n = 3$:

$$u_3 = \frac{1}{4}(-6 + 3 + 3) = 0$$

$$u_2 + u_1 - u_0 = -1 + 1 + 0 = 0$$

Si on remarque une erreur de cette manière, on peut ensuite en chercher l'origine, et si on ne voit pas où est l'erreur, on écrit noir sur blanc qu'il y a sûrement une erreur car la formule ne marche pas pour $n = 3$. Non seulement c'est honnête, c'est aussi une preuve que vous vérifiez vos calculs. C'est une bonne qualité pour un ingénieur... et en plus cela vaut des points !!