

Corrigé du DS 1

Un anneau A commutatif est dit principal lorsque tout idéal de A est engendré par un élément.

1. Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ avec $n \in \mathbb{Z}$ et les idéaux de $\mathbb{K}[X]$ sont les $P\mathbb{K}[X]$ avec $P \in \mathbb{K}[X]$.

Donc : $\mathbb{Z}$ et $\mathbb{K}[X]$ sont des anneaux principaux.

Anneaux $\mathbb{Z}[\sqrt{n}]$

Soit n un entier naturel qui n'est pas le carré d'un entier. On désigne par $\mathbb{Z}[\sqrt{n}]$ l'ensemble des réels de la forme $a + b\sqrt{n}$, où a et b sont des entiers relatifs quelconques.

2. Soit $f : \mathbb{Z}^2 \rightarrow \mathbb{Z}[\sqrt{n}]$ définie par $(a, b) \mapsto a + b\sqrt{n}$.

$\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n}; a, b \in \mathbb{Z}\}$, donc $\mathbb{Z}[\sqrt{n}] = \text{Im } f$.

Soit $(a, b) \in \mathbb{Z}^2$ et $(x, y) \in \mathbb{Z}^2$ tels que $f(a, b) = f(x, y)$

donc : $a - x = \sqrt{n}(y - b)$

supposons par l'absurde $y - b \neq 0$, donc : $\sqrt{n} = \frac{a-x}{y-b} \in \mathbb{Q}$ d'où la contradiction.

Donc : $y - b = 0$ et $a - x = \sqrt{n}(y - b) = 0$

donc : $(a, b) = (x, y)$.

Conclusion :

$f : \mathbb{Z}^2 \rightarrow \mathbb{Z}[\sqrt{n}]$ définie par $(a, b) \mapsto a + b\sqrt{n}$ est bijective.

3. • $\mathbb{Z}[\sqrt{n}] \subset \mathbb{R}$.

• $1 = 1 + 0 \times \sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ car $1, 0 \in \mathbb{Z}$.

• Soit $x, y \in \mathbb{Z}[\sqrt{n}]$,

donc il existe $a, b, c, d \in \mathbb{Z}$ tels que $x = a + b\sqrt{n}$ et $y = c + d\sqrt{n}$.

Donc : $x - y = (a - c) + (b - d)\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ car $a - c \in \mathbb{Z}$ et $c - d \in \mathbb{Z}$.

Et : $x \times y = (ac + bdn) + (ad + cb)\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ car $ac + bdn \in \mathbb{Z}$ et $ad + cb \in \mathbb{Z}$.

Donc :

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

4. $\mathbb{Z}[\sqrt{n}]$ est un sous-anneau de l'anneau intègre $\mathbb{R}$, il est donc intègre.

5. Soit φ de $\mathbb{Z}[\sqrt{n}]$ dans $\mathbb{Z}[\sqrt{n}]$ définie par : $a + b\sqrt{n} \mapsto a - b\sqrt{n}$.

$\varphi(1) = \varphi(1 + 0\sqrt{n}) = 1 - 0\sqrt{n} = 1$.

Soit $x = a + b\sqrt{n}, y = c + d\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ avec $a, b, c, d \in \mathbb{Z}$.

$\varphi(x + y) = \varphi((a + c) + (b + d)\sqrt{n}) = (a + c) - (b + d)\sqrt{n} = \varphi(x) + \varphi(y)$

et $\varphi(xy) = \varphi((ac + bdn) + (ad + cb)\sqrt{n}) = (ac + bdn) - (ad + cb)\sqrt{n}$
de plus $\varphi(x)\varphi(y) = (a - b\sqrt{n})(c - d\sqrt{n}) = (ac + bdn) - (ad + bc)\sqrt{n} = \varphi(xy)$.

Donc : φ est un morphisme d'anneau.

Soit $x = a + b\sqrt{n}$ avec $a, b \in \mathbb{Z}$,

$\varphi \circ \varphi(x) = \varphi(a - b\sqrt{n}) = a + b\sqrt{n} = x$

Donc : $\varphi \circ \varphi = \text{id}$.

Donc :

φ est un morphisme d'anneau involutif de $\mathbb{Z}[\sqrt{n}]$.

6. Pour tout élément x de $\mathbb{Z}[\sqrt{n}]$, on considère le produit $N(x) = x\varphi(x)$.

a) Soit $x \in \mathbb{Z}[\sqrt{n}]$.

$$N(x) = 0 \Leftrightarrow x\varphi(x) = 0$$

$$\Leftrightarrow x = 0 \text{ ou } \varphi(x) = 0 \quad (\text{car } x, \varphi(x) \in \mathbb{R})$$

De plus : φ est un morphisme involutif, donc bijectif, donc :

$$\varphi(x) = 0 \Leftrightarrow \varphi^2(x) = \varphi(0) \Leftrightarrow x = 0$$

Conclusion :

$$\forall x \in \mathbb{Z}[\sqrt{n}], \quad N(x) = 0 \Leftrightarrow x = 0.$$

b) Soit $x = a + b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ et $y = c + d\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ avec $a, b, c, d \in \mathbb{Z}$.

$$N(xy) = xy\varphi(xy)$$

$$= xy\varphi(x)\varphi(y) \quad (\text{car } \varphi \text{ est un morphisme d'anneau})$$

$$= x\varphi(x)y\varphi(y)$$

$$= N(x)N(y).$$

Donc :

$$\forall (x, y) \in \mathbb{Z}[\sqrt{n}]^2, \quad N(xy) = N(x)N(y).$$

7. Soit $x = a + b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ avec $a, b \in \mathbb{Z}$. On suppose x inversible dans $\mathbb{Z}[\sqrt{n}]$.

Soit $y = c + d\sqrt{n}$ avec $c, d \in \mathbb{Z}$ l'inverse de x dans $\mathbb{Z}[\sqrt{n}]$.

Donc : $xy = 1$

$$\text{donc : } N(xy) = N(1) = 1$$

$$\text{donc : } N(x)N(y) = 1.$$

Or : $N(x) = a^2 - nb^2 \in \mathbb{Z}$ et les seuls inversibles de l'anneau $\mathbb{Z}$ sont 1 et -1.

Donc : $N(x) = 1$ ou $N(x) = -1$.

Réciproquement, supposons $N(x) = \pm 1$.

premier cas : $N(x) = 1$,

donc : $x\varphi(x) = 1$ et $\varphi(x) \in \mathbb{Z}[\sqrt{n}]$.

Donc : x est inversible dans $\mathbb{Z}[\sqrt{n}]$ et $x^{-1} = \varphi(x)$

second cas : $N(x) = -1$,

donc : $x\varphi(x) = -1$, donc : $x \times (-\varphi(x)) = 1$ et $-\varphi(x) \in \mathbb{Z}[\sqrt{n}]$ donc : x est inversible dans $\mathbb{Z}[\sqrt{n}]$ et $x^{-1} = -\varphi(x)$.

Conclusion :

un élément x de $\mathbb{Z}[\sqrt{n}]$ est inversible dans $\mathbb{Z}[\sqrt{n}]$ si et seulement si $N(x) = \pm 1$.

Anneau $\mathbb{Z}[\sqrt{5}]$

8. 1, -1 , $2 + \sqrt{5}$ sont inversibles dans $\mathbb{Z}[\sqrt{5}]$, de plus l'ensemble des inversibles d'un anneau forme un groupe multiplicatif.

Donc : $\forall n \in \mathbb{N}, (2 + \sqrt{5})^n \in \mathbb{Z}[\sqrt{5}]^*$ et comme $2 + \sqrt{5} > 1$, les $(2 + \sqrt{5})^n$ pour $n \in \mathbb{N}$ sont deux à deux distincts. Il y a donc une infinité d'éléments inversibles dans $\mathbb{Z}[\sqrt{5}]$.

9. a) Soit $\gamma, \delta \in \mathbb{Z}/4\mathbb{Z}$, donc : $\gamma \in \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$,

donc : $\gamma^2 \in \{\bar{0}, \bar{1}, \bar{4}, \bar{9}\} = \{\bar{0}, \bar{1}\}$.

Donc : $\gamma^2 - 5\delta^2 \in \{\bar{0} - 5 \cdot \bar{0}, \bar{0} - 5 \cdot \bar{1}, \bar{1} - 5 \cdot \bar{0}, \bar{1} - 5 \cdot \bar{1}\} = \{\bar{0}, \bar{3}, \bar{1}\}$

Donc :

$$\gamma^2 - 5 \cdot \delta^2 \in \{\bar{0}, \bar{1}, \bar{3}\}.$$

b) Supposons par l'absurde qu'il existe $c, d \in \mathbb{Z}$ tels que : $c^2 - 5 \cdot d^2 \in \{-2, 2\}$.

Or, dans $\mathbb{Z}/4\mathbb{Z}$, $\bar{-2} = \bar{2}$

donc : $\overline{c^2 - 5 \cdot d^2} = \bar{2}$

donc : $\bar{c}^2 - 5 \cdot \bar{d}^2 = \bar{2} \notin \{\bar{0}, \bar{1}, \bar{3}\}$, d'où la contradiction d'après la question précédente.

Conclusion :

il n'existe pas d'entiers relatifs c et d tels que $c^2 - 5 \cdot d^2 = \pm 2$.

c) Soit $x = a + b\sqrt{n}, y = c + d\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ avec $a, b, c, d \in \mathbb{Z}$ tels que : $xy = 2$.

Donc : $N(xy) = N(2)$

donc : $N(x)N(y) = 4$

Or $N(x), N(y) \in \mathbb{Z}$ et la décomposition en produit de nombre premiers de 4 est 2×2 .

Donc : $(N(x) = \pm 1 \text{ et } N(y) = \pm 4) \text{ ou } (N(x) = \pm 4 \text{ et } N(y) = \pm 1) \text{ ou } (N(x) = \pm 2 \text{ et } N(y) = \pm 2)$.

Or, d'après la question précédente, il n'existe pas d'entiers relatifs c, d tels que $N(c + d\sqrt{5}) = c^2 - 5 \cdot d^2 = \pm 2$.

Donc $N(x) = 1$ ou $N(y) = 1$, c'est à dire d'après la question 7 : x ou y est inversible.

Conclusion :

l'élément 2 est irréductible dans l'anneau $\mathbb{Z}[\sqrt{5}]$,

c'est à dire : $\forall x, y \in \mathbb{Z}[\sqrt{5}]$

$$xy = 2 \Rightarrow x \in (\mathbb{Z}[\sqrt{5}])^* \text{ ou } y \in (\mathbb{Z}[\sqrt{5}])^*$$

10. Soit I l'ensemble des éléments $x = a + b\sqrt{5}$ de $\mathbb{Z}[\sqrt{5}]$ tels que les entiers a et b soient de même parité.

• $I \subset \mathbb{Z}[\sqrt{5}]$

• soit $x = a + b\sqrt{5}, y = c + d\sqrt{5} \in I$ avec $a, b, c, d \in \mathbb{Z}$.

$$x - y = (a - c) + (b - d)\sqrt{5}.$$

On considère les classes d'équivalences dans $\mathbb{Z}/2\mathbb{Z}$: comme $x, y \in I : \bar{a} = \bar{b}$ et $\bar{c} = \bar{d}$ donc : $\overline{(b - d)} = \overline{(a - c)}$, c'est à dire : $b - d$ et $a - c$ ont même parité ; donc $x - y \in I$.

• Soit $x = a + b\sqrt{5} \in I$ et $y = c + d\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$ avec $a, b, c, d \in \mathbb{Z}$.

$$xy = (ac + 5bd) + (bc + ad)\sqrt{5}.$$

On considère les classes dans $\mathbb{Z}/2\mathbb{Z}$, comme $x \in I, \bar{a} = \bar{b}$.

$$\text{Donc : } \overline{(ac + 5bd)} = \bar{a}\bar{c} + \bar{a}\bar{d} \text{ (en effet } \bar{5} = \bar{1})$$

$$\text{et } \overline{(bc + ad)} = \bar{a}\bar{c} + \bar{a}\bar{d}.$$

On a : $\overline{(ac + 5bd)} = \overline{(bc + ad)}$, c'est à dire que $ac + 5bd$ et $bc + ad$ ont même parité.

Donc : $xy \in I$.

Conclusion :

I est un idéal de l'anneau $\mathbb{Z}[\sqrt{5}]$.

11. On suppose que l'idéal I est engendré par un élément x .

a) $2 = 2 + 0\sqrt{5}$ et 2 et 0 sont pairs, donc : $2 \in I = x\mathbb{Z}[\sqrt{5}]$,

donc :

il existe $y \in \mathbb{Z}[\sqrt{5}]$ tel que $xy = 2$.

De même $1 + \sqrt{5} \in I = x\mathbb{Z}[\sqrt{5}]$, donc

il existe $z \in \mathbb{Z}[\sqrt{5}]$ tel que $xz = 1 + \sqrt{5}$.

b) D'après la question 9.c, 2 est irréductible dans $\mathbb{Z}[\sqrt{5}]$ et d'après la question précédente, $xy = 2$, donc : x est inversible ou y est inversible.

Or : $I = x\mathbb{Z}[\sqrt{5}] \neq \mathbb{Z}[\sqrt{5}]$, donc : x n'est pas inversible.

Donc : y est inversible, donc : $xy = 2$ est générateur de I .

Mais : $2\mathbb{Z}[\sqrt{5}]$ est l'ensemble des éléments $a + b\sqrt{5}$ avec a et b entiers pairs, donc : $1 + \sqrt{5} \notin 2\mathbb{Z}[\sqrt{5}]$, d'où la contradiction avec la question précédente.

c) D'après le raisonnement par l'absurde ci-dessus, I n'est pas engendré par un élément, donc :

l'anneau $\mathbb{Z}[\sqrt{5}]$ n'est pas principal.

Matrices d'ordre 2 à coefficients entiers

Soit $\mathcal{M}_2(\mathbb{Z})$ l'ensemble des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ carrées d'ordre 2 à coefficients dans l'anneau $\mathbb{Z}$ des entiers relatifs. On note $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

1. Montrons que $\mathcal{M}_2(\mathbb{Z})$ est un sous-anneau de $\mathcal{M}_2(\mathbb{R})$:

- $\mathcal{M}_2(\mathbb{Z}) \subset \mathcal{M}_2(\mathbb{R})$
- $I_2 \in \mathcal{M}_2(\mathbb{Z})$
- Soit $A, B \in \mathcal{M}_2(\mathbb{Z})$,

$$A - B = \begin{pmatrix} a_{1,1} - b_{1,1} & a_{1,2} - b_{1,2} \\ a_{2,1} - b_{2,1} & a_{2,2} - b_{2,2} \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z})$$

et

$$A \times B = \begin{pmatrix} a_{1,1}b_{1,1} + a_{2,1}b_{1,2} & \dots \\ \dots & \dots \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z})$$

car $\mathbb{Z}$ est un anneau.

Donc : $\mathcal{M}_2(\mathbb{Z})$ est un sous-anneau de $\mathcal{M}_2(\mathbb{R})$.

Donc :

l'ensemble $\mathcal{M}_2(\mathbb{Z})$ est un anneau.

2. a) $(GL_2(\mathbb{Z}), \times)$ est le groupe des inversibles de l'anneau $(\mathcal{M}_2(\mathbb{Z}), +, \times)$. C'est donc un groupe.

b) On suppose $|ad - bc| = 1$. Donc : $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est inversible dans $\mathcal{M}_2(\mathbb{R})$ et son inverse est :

$$M^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \pm \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}).$$

donc : M est inversible dans $\mathcal{M}_2(\mathbb{Z})$.

Réciproquement, on suppose $M \in GL_2(\mathbb{Z})$.

Donc $M^{-1} \in \mathcal{M}_2(\mathbb{Z})$ et $M \times M^{-1} = I_2$

donc : $\det M \times \det M^{-1} = 1$

de plus M et M^{-1} sont à coefficients entiers, donc leurs déterminants sont dans $\mathbb{Z}$ et les seuls inversibles de $\mathbb{Z}$ sont 1 et -1 , donc $|\det M| = 1$.

Conclusion :

$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est inversible dans $\mathcal{M}_2(\mathbb{R})$ si et seulement si $|ad - bc| = 1$.

3. On pose $SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}) : ad - bc = 1 \right\}$.

a) Soit $f : GL_2(\mathbb{Z}) \rightarrow \{-1, 1\}, A \mapsto \det A$.

Donc : $\forall A, B \in GL_2(\mathbb{Z}), \det(AB^{-1}) = \det(A) \det(B)^{-1}$,

donc : f est un morphisme de groupe de $(GL_2(\mathbb{Z}), \times)$ dans $(\{-1, 1\}, \times)$, et $SL_2(\mathbb{Z}) = \text{Ker}(f)$.

Donc :

$SL_2(\mathbb{Z})$ est un groupe pour la multiplication des matrices.

b) Soit $c, d \in \mathbb{Z}$,

$$\begin{pmatrix} 3 & 5 \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \Leftrightarrow 3d - 5c = 1$$

Or : $3 \times (-3) - 5 \times (-2) = 1$,

donc :

$$\begin{aligned} 3d - 5c = 1 &\Leftrightarrow 3d - 5c = 3 \times (-3) - 5 \times (-2) \\ &\Leftrightarrow 3(d + 3) = 5(c + 2) \end{aligned}$$

Or : $3 \wedge 5 = 1$, donc d'après le théorème de Gauss,

$$3(d + 3) = 5(c + 2) \Rightarrow 3 \mid (c + 2) \text{ et } 5 \mid (d + 3)$$

donc :

$$\begin{aligned} 3d - 5c = 1 &\Leftrightarrow \begin{cases} c + 2 = 3q, \text{ avec } q \in \mathbb{Z} \\ d + 3 = 5k, \text{ avec } k \in \mathbb{Z} \\ 3 \times 5 \times k = 5 \times 3 \times q \end{cases} \\ &\Leftrightarrow \exists k \in \mathbb{Z} \mid c = -2 + 3k, d = -3 + 5k \end{aligned}$$

Conclusion :

l'ensemble des couples $(c, d) \in \mathbb{Z} \times \mathbb{Z}$ tels que la matrice $\begin{pmatrix} 3 & 5 \\ c & d \end{pmatrix}$ est dans $SL_2(\mathbb{Z})$ est :

$\{(-2 + 3k, -3 + 5k); \text{ avec } k \in \mathbb{Z}\}$

c) Soit $c, d \in \mathbb{Z}$,

$$\begin{pmatrix} 3 & 5 \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}) \Leftrightarrow 3d - 5c = 1 \text{ ou } 3d - 5c = -1$$

et de même qu'à la question précédente,

$$3d - 5c = 1 \Leftrightarrow \exists k \in \mathbb{Z} \mid c = 2 + 3k, d = 3 + 5k$$

Conclusion :

l'ensemble des couples $(c, d) \in \mathbb{Z} \times \mathbb{Z}$ tels que la matrice $\begin{pmatrix} 3 & 5 \\ c & d \end{pmatrix}$ est dans $GL_2(\mathbb{Z})$ est :

$\{(2 + 3k, 3 + 5k); \text{ avec } k \in \mathbb{Z}\} \cup \{(-2 + 3k, -3 + 5k); \text{ avec } k \in \mathbb{Z}\}$

d) Soit $a, b \in \mathbb{Z}$,

$$\begin{aligned} \exists c, d \in \mathbb{Z} \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R}) &\Leftrightarrow \exists c, d \in \mathbb{Z} \mid ad - bc = \pm 1 \\ &\Leftrightarrow 1 \in a\mathbb{Z} + d\mathbb{Z} \text{ ou } -1 \in a\mathbb{Z} + b\mathbb{Z} \\ &\Leftrightarrow a \wedge b = 1 \end{aligned}$$

d'après le théorème de Bézout.

Donc :

il existe une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ appartenant à $GL_2(\mathbb{Z})$ si et seulement si a et b sont premiers entre eux.

4. On cherche les matrices A de $SL_2(\mathbb{Z})$ telles que $A^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$.

a) Soit A une telle matrice et $f : X \in \mathbb{R}^2 = \mathcal{M}_{2,1}(\mathbb{R}) \mapsto AX \in \mathbb{R}^2$ l'endomorphisme canoniquement associé à A .

On sait que $A^2 = I_2$, donc $f^2 = \text{id}$, donc f est la symétrie par rapport à $E_1 = \text{Ker}(f - \text{id})$ parallèlement à $E_2 = \text{Ker}(f + \text{id})$, avec $E_1 \oplus E_2 = \mathbb{R}^2$.

Si on choisit une base adaptée à cette décomposition, la matrice de f dans cette base est diagonale et les coefficients diagonaux sont 1 ou -1.

Donc : $B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$ (si $E_1 = \mathbb{R}^2$) ou $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ (si $\dim E_1 = 1$) ou

$B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_2$ (si $E_1 = \{0\}$).

De plus A et B sont semblables, donc il existe $P \in GL_n(\mathbb{R})$ tel que $B = P^{-1}AP$.

Donc : $\det B = \det(P^{-1}) \det(A) \det(P) = \det(A) = 1$ car $A \in SL_2(\mathbb{Z})$.

Donc : $B \neq \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Conclusion :

$$B = I_2 \text{ ou } B = -I_2.$$

b) Soit A solution, alors $B = I_2$ ou $B = -I_2$ et il existe $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_n(\mathbb{R})$ tel que $A = PBP^{-1}$.

premier cas : $B = I_2$, donc $A = I_2$,

deuxième cas : $B = -I_2$, donc $A = -I_2$.

Synthèse : Supposons $A = I_2$ ou $A = -I_2$.

Donc : $A \in SL_2(\mathbb{Z})$ et $A^2 = I_2$.

Conclusion :

les solutions sont I_2 et $-I_2$.

Un algorithme de calcul de l'inverse

1. Comme l'ordre de a divise le cardinal N du groupe G , on obtient $a^N = e$. Or $N = (N-1) + 1$ avec $N-1$ dans $\mathbb{N}$ (car $N \geq 1$), donc $a^{N-1} \times a = a \times a^{N-1} = a^{N-1+1} = a^N = e$.

Ainsi

$$a^{N-1} \text{ est l'inverse de } a \text{ dans } G.$$

2. Montrons par récurrence : $\forall i \in \llbracket 0; k+1 \rrbracket$,

$$\mathcal{P}(i) : b_i = a^{(2^i)}$$

Initialisation : pour $i = 0$,

$b_0 = a$ et $a^{2^0} = a^1 = a$, d'où $\mathcal{P}(0)$.

Hérédité : soit $i \in \llbracket 0; k \rrbracket$, on suppose $\mathcal{P}(i)$, montrons $\mathcal{P}(i+1)$.

$b_{i+1} = b_i^2$ et par hypothèse de récurrence, $b_i = a^{(2^i)}$

donc : $b_{i+1} = a^{2 \times (2^i)} = a^{(2^{i+1})}$, d'où $\mathcal{P}(i+1)$.

Donc : par principe de récurrence, $\forall i \in \llbracket 0; k+1 \rrbracket$, $b_i = a^{(2^i)}$.

Ainsi

$$a_{k+1} = a_0 \times b_0^{x_0} \cdots b_k^{x_k} = e \times \prod_{i=0}^k b_i^{x_i} = \prod_{i=0}^k (a^{2^i})^{x_i} = a^{\left(\sum_{i=0}^k 2^i x_i\right)} = a^{N-1}$$

donc d'après la question 1,

$$a_{k+1} \text{ est l'inverse de } a \text{ dans } G.$$

3. a) Un algorithme itératif basé sur des divisions euclidiennes successives par 2.

def base2(n):

 """détermine la liste des chiffres en binaire de n

 n entier strictement positif"""

 q = n

 binaire = []

 while q != 0:

 binaire.append(q%2)

 q = q//2

 return binaire

b) def inverse(a,N):

 binaire = base2(N-1)

 ai = E # on suppose E variable globale, neutre de G

 bi = a

 for i in range(len(binaire)):

 if binaire[i] == 1:

 ai = multi(ai,bi)

 bi = multi(bi,bi)

 return ai

c) Dans le pire des cas, tous les chiffres de $N-1$ valent 1, donc on fait 2 multiplications par valeur de i et il y a $k+1$ valeurs de i (de 0 à k). Ainsi la complexité est linéaire en k avec $2(k+1)$ multiplications dans le groupe G .

4. a) Le cardinal du groupe des inversibles de $\mathbb{Z}/148\mathbb{Z}$ est $N = \varphi(148)$ où φ est la fonction d'Euler. Or $148 = 2 \times 74 = 2^2 \times 37$ avec 37 qui est premier donc $N = 2^1(2-1) \times (37-1) = 72$.

b) Comme 5 est premier avec 148, la classe $\bar{5}$ est bien inversible dans $\mathbb{Z}/148\mathbb{Z}$.

Ici $N-1 = 72-1 = 71 = 1+2 \times 35 = 1+2+2^2 \times 17 = 1+2+2^2+2^2 \times 16 = 1+2+2^2+2^6$ donc $N-1$ s'écrit en binaire 1 000 111.

Écrivons la liste des valeurs des a_i et b_i dans un tableau

i	0	1	2	3	4	5	6	
x_i	1	1	1	0	0	0	1	
b_i	5	$\overline{5^2} = \overline{25}$	$\overline{25^2} = \overline{625} = \overline{33}$	$\overline{33^2} = \overline{53}$	$\overline{53^2} = \overline{-3}$	$\overline{9}$	$\overline{81}$	
a_i	e	$\bar{5}$	$\overline{25 \times 5} = \overline{125} = \overline{-23}$	$\overline{-23 \times 33} = \overline{-19}$	$\overline{-19}$	$\overline{-19}$	$\overline{-19}$	$\overline{-19 \times 81} = \overline{89}$

$$\text{car } \overline{33^2} = \overline{1089} = \overline{148 \times 7 + 53} = \overline{53}$$

$$\overline{-23 \times 33} = \overline{-759} = \overline{-19}$$

$$\overline{-59} = \overline{89}$$

$$\overline{53^2} = \overline{2089} = \overline{145} = \overline{-3}$$

$$\overline{-19 \times 81} = \overline{-(1620 - 81)} = \overline{-(140 - 81)} =$$

L'inverse de $\bar{5}$ est donc $\overline{89}$.

c) Cherchons un couple de Bézout pour 148 et 5 via l'algorithme d'Euclide :

$148 = 5 \times 29 + 3$ et $5 = 3 \times 1 + 2$ et enfin $3 = 2 \times 1 + 1$.

Donc $1 = 3 - (5 - 3) = -5 + 2 \times 3 = -5 + 2 \times (148 - 5 \times 29)$ i.e. $1 = 5 \times (-59) + 2 \times 148$

Ainsi en passant aux classes modulo 148, on obtient $\bar{1} = \bar{5} \times \overline{(-59)}$ d'où dans l'anneau commutatif $\mathbb{Z}/148\mathbb{Z}$, $\bar{5}$ est inversible d'inverse $\overline{-59} = \overline{89}$.