karam.fayad@eisti.eu

Corrigé DS4 Algèbre (22/02/2019)

Exercice 1 .

1. On utilise la définition de la loi $\star$ pour remplir le tableau. Par exemple $5 \star 6$ est le reste de la division euclidienne de 30 par 7, ainsi $5 \star 6 = 2$.

a \ b	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

2. Il est clair d'après le tableau précédent que $\star$ est une loi de composition interne sur E.
   Remarque : à priori, si $(a, b) \in E^2$, alors $a \star b$, étant le reste de la division euclidienne de ab par 7, appartient à l'ensemble $\{0, 1, 2, 3, 4, 5, 6\}$. Or ici, comme 7 ne divise ni a ni b, alors 7 ne divise pas ab, donc $a \star b \neq 0$, ainsi $a \star b \in E$.
   La loi $\star$ est par définition commutative : "le reste de la division euclidienne de ab par 7 est égal au reste de la division euclidienne de ba par 7", d'où $a \star b = b \star a$.
   L'élément neutre est bien 1, et d'après le tableau précédent, tous les éléments sont inversibles :
   1 est l'inverse de lui-même ($1 \star 1 = 1$)
   6 est l'inverse de lui-même ($6 \star 6 = 1$)
   2 et 4 sont inverses l'un de l'autre ($2 \star 4 = 4 \star 2 = 1$)
   3 et 5 sont inverses l'un de l'autre ($3 \star 5 = 5 \star 3 = 1$).
3. (a) F est bien un sous-groupe de E : il contient 1, il est stable par la loi $\star$ (voir la table de multiplication de F ci-dessous), et F est stable par passage à l'inverse.

a \ b	1	2	4
1	1	2	4
2	2	4	1
4	4	1	2

   (b) G n'est pas un sous-groupe de E car G n'est pas stable par la loi $\star$: par exemple, $3 \in G$ mais $3 \star 3 = 2 \notin G$.
   (c) H n'est pas un sous-groupe de E car H n'est pas stable par la loi $\star$: par exemple, $(2, 6) \in H^2$ mais $2 \star 6 = 5 \notin H$.

Exercice 2 .

Il suffit de montrer que A est un sous-groupe du groupe multiplicatif $\mathbb{C}^*$.
• $1 \in A$ car $1 = a + ib\sqrt{5}$ avec $(a, b) = (1, 0)$.
• Montrons que A est stable par multiplication : soit (a, b), (c, d) deux couples dans $\mathbb{Q}^2 \setminus \{(0, 0)\}$, et soit $z = a + ib\sqrt{5}$ et $z' = c + id\sqrt{5}$, on a :
$zz' = (a + ib\sqrt{5})(c + id\sqrt{5}) = (ac - 5bd) + (ad + bc)i\sqrt{5} \in A$ car $(ac - 5bd, ad + bc) \in \mathbb{Q}^2 \setminus \{(0, 0)\}$.
Remarquons que $(ac - 5bd, ad + bc) \neq (0, 0)$ car sinon on aurait $zz' = 0$ d'où $z = 0$ ou $z' = 0$ d'où $(a, b) = (0, 0)$ ou $(c, d) = (0, 0)$: impossible.
• Montrons que A est stable par passage à l'inverse : soit $a + ib\sqrt{5} \in A$ avec $(a, b) \in \mathbb{Q}^2 \setminus \{(0, 0)\}$. On a :
$$\frac{1}{a + ib\sqrt{5}} = \frac{a - ib\sqrt{5}}{(a + ib\sqrt{5})(a - ib\sqrt{5})} = \frac{a}{a^2 + 5b^2} + i\frac{-b}{a^2 + 5b^2}\sqrt{5} \in A \text{ car } \left(\frac{a}{a^2 + 5b^2}, \frac{-b}{a^2 + 5b^2}\right) \in \mathbb{Q}^2 \setminus \{(0, 0)\}.$$
Remarquons que comme $(a, b) \neq (0, 0)$ alors $a^2 + 5b^2 \neq 0$.

Exercice 3 .

1. On a : $j^2 = -1 - j$, ainsi j^2 s'écrit sous la forme $a + bj$ avec $(a, b) = (-1, -1)$, d'où $j^2 \in \mathbb{Z}[j]$.
2. Il suffit de montrer que $\mathbb{Z}[j]$ est un sous-anneau de $\mathbb{C}$:
   • $\mathbb{Z}[j]$ est un sous-groupe de $(\mathbb{C}, +)$ car $0 = 0+0j \in \mathbb{Z}[j]$, et pour tout $(a, b, c, d) \in \mathbb{Z}^4$, $(a+bj)-(c+dj) = (a-c)+(b-d)j \in \mathbb{Z}[j]$.
   • $\mathbb{Z}[j]$ est stable par la multiplication car pour tout $(a, b, c, d) \in \mathbb{Z}^4$, on a :
   $(a+bj)(c+dj) = ac+(ad+bc)j+bdj^2 = ac+(ad+bc)j+bd(-1-j) = (ac-bd)+(ad+bc-bd)j \in \mathbb{Z}[j]$.
   • $1 = 1 + 0j \in \mathbb{Z}[j]$.
   Ainsi, $\mathbb{Z}[j]$ est un sous-anneau de $\mathbb{C}$. De façon équivalente, c'est un anneau.
3. (a) Soit $z = a + bj \in \mathbb{Z}[j]$ avec $(a, b) \in \mathbb{Z}^2$. On a : $\overline{z} = \overline{a + bj} = a + b\overline{j} = a + bj^2$ puis
   $$z\overline{z} = (a + bj)(a + bj^2) = a^2 + abj^2 + abj + b^2j^3 = a^2 + ab(j + j^2) + b^2 = a^2 - ab + b^2 = f(z)$$
   en utilisant le fait que $j^3 = 1$ et $j + j^2 = -1$.
   (b) Pour tout $z \in \mathbb{Z}[j]$, $f(z) \in \mathbb{Z}$, de plus, d'après la question précédente, $f(z) = z\overline{z} = |z|^2 \geq 0$, ainsi $f(z) \in \mathbb{N}$.
   Soit $(z, z') \in \mathbb{Z}[j]^2$, on a : $f(zz') = (zz')(\overline{zz'}) = (z\overline{z})(z'\overline{z'}) = f(z)f(z')$.
   (c) $\Rightarrow$) Supposons que $z \in \mathcal{U}(\mathbb{Z}[j])$, alors $\exists\, z' \in \mathbb{Z}[j]$, $zz' = 1$. En appliquant f, et en utilisant la question précédente, on obtient $f(z)f(z') = f(1) = 1$. Or $f(z)$ et $f(z')$ sont des entiers naturels, on en déduit que $f(z) = f(z') = 1$.
   $\Leftarrow$) Supposons que $f(z) = 1$, alors $z\overline{z} = 1$, donc z est inversible d'inverse $\overline{z}$, ainsi $z \in \mathcal{U}(\mathbb{Z}[j])$.
   (d) Calcul élémentaire :
   $(2a - b)^2 + 3b^2 = 4 \Leftrightarrow 4a^2 - 4ab + 4b^2 = 4 \Leftrightarrow a^2 - ab + b^2 = 1 \Leftrightarrow f(a + bj) = 1$.
   (e) D'après les questions précédentes, on a : $z = a + bj \in \mathcal{U}(\mathbb{Z}[j]) \Leftrightarrow f(z) = 1 \Leftrightarrow (2a - b)^2 + 3b^2 = 4$.
   Comme $(2a - b)^2$ et $3b^2$ sont des entiers naturels, on déduit que le couple $((2a - b)^2, 3b^2)$ appartient à l'ensemble $\{(0, 4), (1, 3), (2, 2), (3, 1), (4, 0)\}$.
   On exclut les couples $(0, 4), (2, 2)$ et $(3, 1)$ car on ne peut pas avoir $3b^2 = 4$, ni $3b^2 = 2$ ni $3b^2 = 1$.
   En examinant les cas qui restent, on trouve six couples (a, b) possibles :
   $(a, b) \in \{(1, 0), (-1, 0), (0, 1), (0, -1), (-1, -1), (1, 1)\}$.
   Ainsi,
   $$\mathcal{U}(\mathbb{Z}[j]) = \{1, -1, j, -j, -1 - j, 1 + j\} = \{\pm 1, \pm j, \pm j^2\}.$$
4. $\mathcal{U}(\mathbb{Z}[j])$ étant l'ensemble des éléments inversibles de l'anneau $\mathbb{Z}[j]$, on déduit que c'est un groupe pour la multiplication des nombres complexes.
   Remarque : Son élément neutre est 1, et l'inverse de tout élément étant son conjugué d'après les questions précédentes.
   Ainsi, j et j^2 sont inverses l'un de l'autre, $-j$ et $-j^2$ sont inverses l'un de l'autre, 1 est l'inverse de lui-même et -1 est l'inverse de lui-même.

Exercice 4 .

1. Explicitons les applications $f \circ g : \mathbb{N} \longrightarrow \mathbb{N}$ et $g \circ f : \mathbb{Z} \longrightarrow \mathbb{Z}$.
   Soit $n \in \mathbb{N}$:
   - si n est pair, $f(g(n)) = f\left(\frac{n}{2}\right) = n$.
   - si n est impair, $f(g(n)) = f\left(-\frac{n+1}{2}\right) = -2\left(-\frac{n+1}{2}\right) - 1 = n$.
   Ainsi $f \circ g = \mathrm{Id}_{\mathbb{N}}$.
   De même, pour $n \in \mathbb{Z}$, en distinguant les cas $n \geq 0$ et $n < 0$, on montre que $g \circ f = \mathrm{Id}_{\mathbb{Z}}$.
   On déduit que f et g sont des bijections réciproques l'une de l'autre.
2. Montrons que $(\mathbb{N}, *)$ est un groupe abélien.
   • Il est clair que $*$ est une LCI sur $\mathbb{N}$ car pour $(m, n) \in \mathbb{N}^2$, $m * n \in f(\mathbb{Z}) \subset \mathbb{N}$.
   • La loi $*$ est clairement commutative.
   • L'élément neutre est 0 : $\forall\, n \in \mathbb{N}$, $n * 0 = f(g(n) + g(0)) = f(g(n)) = n$.

• La loi $*$ est associative car pour $(m,n,p) \in \mathbb{N}^3$, on a :
$m*(n*p) = f(g(m)+g(n*p)) = f(g(m)+g(f(g(n)+g(p)))) = f(g(m)+g(n)+g(p))$
en utilisant le fait que $g \circ f = \mathrm{Id}_{\mathbb{Z}}$.
De même, on trouve que $(m*(n*p)) = f(g(m)+g(n)+g(p))$. D'où l'associativité.
• Soit $m \in \mathbb{N}$, montrons que m est inversible pour la loi $*$: en effet, si n est l'inverse de m, on a : $m*n = f(g(m)+g(n)) = 0$, ainsi $g(m)+g(n) = f^{-1}(0) = g(0) = 0$ d'où $g(n) = -g(m)$ puis en appliquant f, on obtient $n = f(-g(m))$. Distinguons deux cas :
- si m est pair non nul, on trouve $n = f(-m/2) = m-1$
- si m est impair, on trouve $n = f((m+1)/2) = m+1$.
On déduit (et on vérifie) que :
- l'inverse d'un entier pair non nul m est $m-1$,
- l'inverse d'un entier impair m est $m+1$,
- l'inverse de 0 est 0.