Devoir libre $n°01$
Correction

N'hésitez pas de me signaler les erreurs rencontrées.

•••••••••

Exercice 1 :

1. L'ensemble des éléments inversibles de $\mathbb{Z}/_{2^n\mathbb{Z}}$ est égal à $U_n = \left\{ \overline{k} \;\middle|\; k \text{ imapir} \right\}$, on en déduit que cet ensemble est cardinal $\varphi(2^n) = 2^n - 2^{n-1} = 2^{n-1}$ (φ l'indicateur d'Euler) .

2. et 3. Pour tout $p \in \mathbb{N}^*$ on a :

$$\begin{aligned} 5^{2^p} - 1 &= (5^{2^{p-1}} - 1)(5^{2^{p-1}} + 1) \\ &= (5^{2^{p-2}} - 1)(5^{2^{p-2}} + 1)(5^{2^{p-1}} + 1) \\ &= 4(5^{2^0} + 1)(5^{2^1} + 1)...(5^{2^{p-1}} + 1) \end{aligned}$$

2 divise $5^s + 1\ \forall s \in \mathbb{N}$, mais 4 ne divise pas $5^s + 1$ car $5^s + 1 \equiv 2[4]$, donc l'exposant de 2 dans la décomposition en facteurs premiers de $5^{2^p} - 1$ est $p + 2$. Donc $5^{2^{n-2}} - 1 = 2^n\alpha$ avec α un nombre impair. Donc $\overline{5}^{2^{n-2}} = \overline{1}$ mais $5^{2^{n-3}} - 1 = 2^{n-1}\beta$ avec β un nombre impair. Donc $\overline{5}^{2^{n-3}} \neq \overline{1}$ et $\overline{5}^{2^{n-2}} = \overline{1}$, donc $\overline{5}$ est d'ordre 2^{n-2} dans U_n.
D'autre part, on a :

$$5^{2^{n-3}} - 1 - 2^{n-1} = 2^{n-1}\beta - 2^{n-1} = 2^{n-1}(\beta - 1)$$

avec $\beta - 1$ pair. Donc $5^{2^{n-3}} \equiv 2^{n-1} + 1[2^n]$.

4. $(\overline{5}) = \{\overline{5}^k / k \in \mathbb{Z}\}$ est un sous-groupe de U_n de cardinal 2^{n-2}. Montrons que

$$U_n = \left\{ \pm\overline{5}^k \;\middle|\; 0 \leq k < 2^{n-2} \right\}$$

Cette dernière ensemble inclus dans U_n est de cardinal 2^{n-1}, donc il suffit de montrer que $\left\{ \overline{5}^k \;\middle|\; 0 \leq k < 2^{n-} \right.$ $\left\{ -\overline{5}^k \;\middle|\; 0 \leq k < 2^{n-2} \right\} = \emptyset$.
Supposons qu'il existe i et j, $i \neq j$ tel que $\overline{5}^i = -\overline{5}^j$ et $\overline{5}^i + \overline{5}^j = 0$ ou encore $\overline{5}^{i-j} + 1 = \overline{0}$ ($j < i$) ceci est absurde car 4 ne divise pas $5^{i-j} + 1$, donc pour tout $\overline{x} \in U$, il existe $0 \leq k < 2^{n-2}$ tel que $\overline{x} = \overline{5}^k$ ou $\overline{x} = -\overline{5}^k$.

5. $U_n = \left\{ \overline{5}^k \;\middle|\; 0 \leq k < 2^{n-2} \right\} \cup \left\{ -\overline{5}^k \;\middle|\; 0 \leq k < 2^{n-2} \right\}$, donc U_n n'est pas cyclique.

Exercice 2 :

1. On considère les matrices suivantes :

$$e = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \; i = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \; j = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \text{ et } k = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

On a donc $H = \text{Vect}\{e, i, j, k\}$. Le tableau suivant résume tous les produits possibles des éléments de la famille génératrice $\{e, i, j, k\}$ de l'espace vectoriel H.

$\swarrow$	e	i	j	k
e	e	i	j	k
i	i	$-e$	$-k$	j
j	j	k	$-e$	$-i$
k	k	$-j$	i	$-e$

H est un sous-espace vectoriel de $\mathscr{M}_4(\mathbb{R})$ puisque c'est l'ensemble des combinaisons linéaires de e, i, j, k, c'est-à-dire le sous-espace vectoriel engendré par la famille $\mathscr{B} = (e, i, j, k)$. La famille $\mathscr{B}$ est génératrice de H ; montrons qu'elle est libre : soient $w, x, y, z \in \mathbb{K}$ tels que $we+xi+yj+zk = 0$. On a donc

$$0 = \begin{pmatrix} w & -x & -y & -z \\ x & w & -z & y \\ y & z & w & -x \\ z & -y & x & w \end{pmatrix}$$

de sorte que, par identification, $w = x = y = z = 0$.

Comme H est un espace vectoriel, c'est en particulier un groupe abélien vis-à-vis de l'addition. Pour montrer que c'est un anneau (en fait un sous-anneau de $\mathscr{M}_4(\mathbb{R})$), il reste à montrer qu'il contient l'élément neutre et est stable par produit. Le fait que H contienne l'élément neutre, c'est-à-dire la matrice identité e, vient de ce que cette matrice est obtenue avec $w = 1$ et $x = y = z = 0$. Montrons maintenant que H est stable par produit en considérant $M = M(w, x, y, z) = we + xi + yj + zk$ et $M' = M(w', x', y', z') = w'e + x'i + y'j + z'k$. Les propriétés du produit matriciel (associativité et distributivité par rapport à l'addition) permettent d'écrire, en tenant compte de la multiplication explicitée dans tableau précédent :

$$\begin{aligned} MM' &= (we + xi + yj + zk)(w'e + x'i + y'j + z'k) \\ &= ww'e + wx'i + wy'j + wz'k + xw'i + xx'(-e) + xy'k + xz'(-j) \\ &\quad + yw'j + yx'(-k) + yy'(-e) + yz'i + zw'k + zx'j + zy'(-i) + zz'(-1) \\ &= (ww' - xx' - yy' - zz')e + (wx' + xw' + yz' - zy')i \\ &\quad + (wy' + yw' - xz' + zx')j + (wz' + zw' + xy' - yx')k \quad (*) \end{aligned}$$

ce qui montre que $MM' \in H$.
La multiplication n'est pas commutative puisque, par exemple, $ij \neq ji$.

2. Soit $M = we + xi + yj + zk \in H\backslash\{0\}$. Cherchons une condition pour que l'inverse de M (inverse au sens du produit matriciel !) existe et appartient encore à H.
En observant la formule $(*)$, on constate qu'en choisissant $w' = w$, et $(x', y', z') = (-x, -y, -z)$, on

obtient

$$\begin{aligned} MM' &= (w^2+x^2+y^2+z^2)e+(-wx+xw-yz+zy)i+(-wy+yw+xz-zx)j+(-wz+zw+xy-y \\ &= (w^2+x^2+y^2+z^2)e. \end{aligned}$$

Donc une condition nécessaire et suffisante pour que M soit inversible est que $w^2+x^2+y^2+z^2 \neq 0$.
Dans ce cas, $M\dfrac{1}{w^2+x^2+y^2+z^2}M' = e$ donc M est inversible et

$$M^{-1} = \frac{1}{w^2+x^2+y^2+z^2}(we-xi-yj-zk) \in H.$$

3. Si $\mathbb{K}=\mathbb{R}$, on remarque que $M = we+xi+yj+zk \in H\backslash\{0\}$ si, et seulement si, $w^2+x^2+y^2+z^2 \neq 0$, donc tous les éléments de $H\backslash\{0\}$ sont inversibles, donc H est un corps. Par contre si $\mathbb{K}=\mathbb{C}$, il y a des éléments non nuls dans H qui ne sont pas inversibles, par exemple $M(1,i,0,0)$.

Exercice 3 :

1. Soient α et β dans $\mathbb{Z}[i]$. Notons $\alpha = a+ib$ et $\beta = c+id$ où a,b,c et d sont dans $\mathbb{Z}$. Alors $\alpha+\beta = (a+c)+i(b+d)$ et $a+c$ et $b+d$ sont dans $\mathbb{Z}[i]$, donc $\alpha+\beta \in \mathbb{Z}[i]$.
De même $\alpha\beta = (ac-bd)+i(ad+bc)$ et $ac-bd$ et $ad+bc$ sont dans $\mathbb{Z}$, donc $\alpha\beta \in \mathbb{Z}[i]$.

2. Soit $\alpha \in \mathbb{Z}[i]$ un élément inversible. Il existe donc $\beta \in \mathbb{Z}[i]$ tel que $\alpha\beta = 1$. Ainsi, $\alpha \neq 0$ et $\dfrac{1}{\alpha} \in \mathbb{Z}[i]$.
Remarquons que pour tout $z \in \mathbb{Z}[i]\backslash\{0\}$, on a $|z| \geq 1$. En effet, pour tout $z \in \mathbb{C}$, $|z| \geq \sup(Re(z), Im(z))$ et si $z \in \mathbb{Z}[i]$, $\sup(Re(z), Im(z)) \geq 1$. Si $|\alpha| \neq 1$, alors $|\alpha| > 1$ et $\left|\dfrac{1}{\alpha}\right| < 1$. On en déduit que $\dfrac{1}{\alpha} = 0$ ce qui impossible. Ainsi $|\alpha| = 1$, ce qui implique $\alpha \in \{-1, 1, -i, i\}$. Réciproquement $1^{-1} = 1 \in Z[i]$, $(-1)^{-1} = 1 \in \mathbb{Z}[i]$, $i^{-1} = -i \in \mathbb{Z}[i]$ et $(-i)^{-1} = i \in \mathbb{Z}[i]$.
Les éléments inversibles de $\mathbb{Z}[i]$ sont : $1, -1, i, -i$.

3. Soit $w \in \mathbb{C}$. Notons $w = x+iy$ où $x, y \in \mathbb{R}$. On désigne par $[x]$ la partie entière de x. Si $x \leq [x]+\dfrac{1}{2}$, notons $n_x = [x]$, et si $x > [x]+\dfrac{1}{2}$, notons $n_x = [x]+1$. Dans les deux cas $|x-n_x| \leq \dfrac{1}{2}$. De même, notons n_y l'entier associé à y.
Soit alors $\alpha = n_x + in_y$. On a $\alpha \in \mathbb{Z}[i]$ et

$$|w-\alpha|^2 = (x-n_x)^2+(y-n_y)^2 \leq \frac{1}{4}+\frac{1}{4} = \frac{1}{2} < 1.$$

D'où $|w-\alpha| < 1$.

4. Soit $\alpha, \beta \in \mathbb{Z}[i]$, avec $\beta \neq 0$. Soit alors $q \in \mathbb{Z}[i]$ tel que $\left|\dfrac{\alpha}{\beta} - q\right| < 1$ (q existe d'après la question précédente). Soit $r = \alpha - \beta q$. Comme $\alpha \in \mathbb{Z}[i]$ et $\beta q \in \mathbb{Z}[i]$, alors $r \in \mathbb{Z}[i]$. De plus $\left|\dfrac{r}{\beta}\right| = \left|\dfrac{\alpha}{\beta} - q\right| < 1$, donc $|r| < |\beta|$.

●●●●●●●●●●