•
$$\exists_{3} \in \mathcal{H}_{3}(\mathbb{R})$$

• Soient $M = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \end{pmatrix} \in \mathcal{H}_{3}(\mathbb{R})$ et $M' = \begin{pmatrix} 1 & a' & c' \\ 0 & 1 & b \end{pmatrix} \in \mathcal{H}_{3}(\mathbb{R})$
 $MM' = \begin{pmatrix} 1 & a+a' & c+c'+ab' \\ 0 & 1 & b+b' \\ 0 & 0 & 1 \end{pmatrix} \in \mathcal{H}_{3}(\mathbb{R})$
et $M'' = \begin{pmatrix} 1 & -a & -c+ab \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix} \in \mathcal{H}_{3}(\mathbb{R})$

2)
$$\mathbb{R} \xrightarrow{\phi} \mathcal{H}_3(\mathbb{R})$$
 on $\mathbb{R} \xrightarrow{\psi} \mathcal{H}_3(\mathbb{R})$ on $\mathbb{R} \xrightarrow{\psi} \mathcal{H}_3(\mathbb{R})$.

 $\alpha \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Exercice 3

-1. L'associativité se vérifie à la main. L'élément neutre est la matrice

$$\left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array}\right)$$

L'inverse d'une matrice

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

est tout simplement

$$\left(\begin{array}{cc} d & -b \\ -c & a \end{array}\right)$$

Astuce : ad-bc étant un élément non-nul de $\mathbb{Z}/2\mathbb{Z}$, il est forçément égal à 1. De plus, pour tout x dans $\mathbb{Z}/2\mathbb{Z}$, on a -x=x, donc on peut aussi écrire l'inverse comme étant :

$$\left(\begin{array}{cc} d & b \\ c & a \end{array}\right)$$

-2. Il y a $2^4=16$ matrices carrées de taille 2 à coefficients dans $\mathbb{Z}/2\mathbb{Z}$. Pour que ad-bc=ad+bc soit non-nul, il faut qu'au moins deux des coefficients soient non-nuls. On vérifie à la main quand le déterminant est (non-)nul, on obtient la liste :

$$id = \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array}\right)$$

$$g_1 = \left(\begin{array}{cc} 1 & 0 \\ 1 & 1 \end{array}\right)$$

$$g_2 = \left(\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array}\right)$$

$$g_3 = \left(\begin{array}{cc} 1 & 1 \\ 1 & 0 \end{array}\right)$$

$$g_4 = \left(\begin{array}{cc} 0 & 1\\ 1 & 0 \end{array}\right)$$

$$g_5 = \left(\begin{array}{cc} 0 & 1\\ 1 & 1 \end{array}\right)$$

G est donc d'ordre 6.

-3. On regarde la première puissance non-nulle qui devient égale à id.

Pour id, l'ordre est 1. Pour $g_1: g_1^2=id$, donc ordre 2; de même pour g_2 qui est d'ordre 2. Pour $g_3: g_3^2=g_5$ et $g_3^3=id$, donc g_3 est d'ordre 3; calcul similaire pour g_5 qui est d'ordre 3, et enfin g_4 est d'ordre 2.

- -4. G n'est pas cyclique puisqu'il n'y a aucun élément d'ordre 6. Par ailleurs, tout sous-groupe H de G, différent de G est de cardinal 1, 2 ou 3 (puisque $\mid H \mid$ doit diviser $\mid G \mid$).
- 2 et 3 sont des nombres premiers, or pour tout g dans H non-trivial, le sous-groupe engendré par g doit diviser ce nombre premier tout en étant >1, donc $\langle g \rangle$ est de cardinal $\mid H \mid$ donc égal à H.
 - -5. Il suffit de lister selon le générateur. On obtient les sous-groupes :
 - $(1) \{id\},\$
 - $(2) \langle g_1 \rangle = \{id, g_1\},\$
 - $(3) \langle g_2 \rangle = \{id, g_2\},\$
 - $(4) \langle g_4 \rangle = \{id, g_4\},\$
 - (5) $\langle g_3 \rangle = \{id, g_3, g_5\} = \langle g_5 \rangle$,