DM 1

ex1 (a) d'abord pour $x, y \in]-1, 1[$, on a $\frac{x+y}{1+xy} \in]-1, 1[$.

en effet, comme $x, y \in]-1, 1[\Rightarrow xy \in]-1, 1[\Rightarrow 1+xy > 0$

comme $(x-1)(y-1) > 0$, on a $1+xy > xy$, d'où $\frac{xy}{1+xy} < 1$

De m̂, comme $(x+1)(y+1) > 0 \Rightarrow 1+xy+x+y > 0 \Rightarrow \frac{x+y}{1+xy} > -1$

Ainsi, $\frac{x+y}{1+xy} \in]-1, 1[$, donc l'application $G \times G \longrightarrow G, (x,y) \longmapsto x * y$ est bien définie

<u>Associativité de $*$</u> : pour $x, y, z \in G$, $(x*y)*z = \frac{x+y}{1+xy} * z = \left(\frac{x+y}{1+xy} + z\right) \Big/ \left(1 + \frac{x+y}{1+xy} \cdot z\right)$

$$= \frac{x+y+z+xyz}{1+xy+xz+yz}$$

$$x*(y*z) = x * \left(\frac{y+z}{1+yz}\right) = \left(x + \frac{y+z}{1+yz}\right) \Big/ \left(1 + x \cdot \frac{y+z}{1+yz}\right)$$

$$= \frac{x+y+z+xyz}{1+yz+xy+xz}$$

d'où $(x*y)*z = x*(y*z)$

<u>élément neutre</u> : c'est $0 \in G$: $x * 0 = \frac{x+0}{1+x\cdot 0} = x$ $\quad 0 * x = \frac{0+x}{1+0\cdot x} = x$

<u>inverse d'un élément</u> : pour $x \in G$, $x^{-1} := -x$ est l'inverse de x

En effet. $x * x^{-1} = \frac{x+(-x)}{1+x(-x)} = 0$, de m̂, $x^{-1} * x = 0$

Ainsi, $(G, *)$ est un groupe

D'autre part, $x*y = y*x$, ainsi G est abélien.

(b) $G = \mathbb{R}^2$, $(x,y) \otimes (x',y') := (x+x', ye^{x'} + y'e^{x})$

<u>associativité</u> : $[(x,y)\otimes(x',y')]\otimes(x'',y'') = (x+x', ye^{x'}+y'e^{x}) \otimes (x'',y'')$

$$= (x+x'+x'', (ye^{x'}+y'e^{x})e^{x''} + y''e^{x+x'})$$

$$= (x+x'+x'', ye^{x'+x''} + y'e^{x+x''} + y''e^{x+x'})$$

$$(x,y)\otimes[(x',y')\otimes(x'',y'')] = (x,y)\otimes(x'+x'', y''e^{x'} + y'e^{x''})$$

$$= (x+x'+x'', ye^{x'+x''} + (y''e^{x'} + y'e^{x''})e^{x})$$

$$= (x+x'+x'', ye^{x'+x''} + y''e^{x'+x} + y'e^{x+x''})$$

d'où $[(x,y)\otimes(x',y')]\otimes(x'',y'') = (x,y)\otimes[(x',y')\otimes(x'',y'')]$

<u>l'élément neutre</u>: c'est $(0,0)$.

$$(x,y)\otimes(0,0) = (x+0,\ ye^0+0\cdot e^x) = (x,y)$$

de $\hat{m}$, $(0,0)\otimes(x,y) = (x,y)$

<u>l'inverse d'un élément</u>: soit $(x,y)\in G$. alors $(x,y)^{-1} = (-x, ye^{-2x})$

$(G,\otimes)$ est abélien. car $(x,y)\otimes(x',y') = (x+x',\ ye^{x'}+y'e^{x}) = (x',y')\otimes(x,y)$ $\square$

(2). $\exists$ 6 ss-gpes de S_3, à savoir:

$\{e\}$, S_3, $\{e,(1\,2)\}$, $\{e,(1\,3)\}$, $\{e,(2\,3)\}$, $\{e,(1\,2\,3),(1\,3\,2)\}$

(3) Rappel: $\bar{1}\in \mathbb{Z}/n\mathbb{Z}$ est d'ordre n, et $\mathbb{Z}/n\mathbb{Z}$ est engendré par $\bar{1}$

Ainsi, un morphisme $f: \mathbb{Z}/n\mathbb{Z}\to G$ (avec G un gpe) est complètement déterminé par $f(\bar{1})$.

De plus, pour $g\in G$, il existe un morphisme $\varphi: \mathbb{Z}/n\mathbb{Z}\to G$ vérifiant $\varphi(\bar{1}) = g$

si et seulement si $g\in G$ est d'ordre divisant n

Ainsi, on a une bijection entre

$$\{\text{morphismes } \mathbb{Z}/n\mathbb{Z}\to G\} \xrightarrow{1:1} \{\text{élément d'ordre divisant } n\} \qquad (*)$$

$$\varphi \longmapsto \varphi(\bar{1})$$

<u>Donc</u>: <u>morphisme $\mathbb{Z}/3\mathbb{Z}\to\mathbb{Z}/7\mathbb{Z}$</u>: $\bar{1}\in\mathbb{Z}/3\mathbb{Z}$ est d'ordre 3, et les seuls éléments d'ordre divisant 3 de $\mathbb{Z}/7\mathbb{Z}$ est $\bar{0}$

donc il n'y a qu'un seul morphisme : c'est le morphisme trivial.

<u>morphisme $\mathbb{Z}/3\mathbb{Z}\to\mathbb{Z}/12\mathbb{Z}$</u>: encore une fois, l'élément $\bar{1}\in\mathbb{Z}/3\mathbb{Z}$ est d'ordre 3

les élément de $\mathbb{Z}/12\mathbb{Z}$ d'ordre divisant 3 sont:

$$\bar{0},\ \bar{4},\ \bar{8}\in\mathbb{Z}/12\mathbb{Z}$$

Ainsi, il y a 3 morphismes de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$, qui sont donnés par

(a) $\mathbb{Z}/3\mathbb{Z} \xrightarrow{f_1} \mathbb{Z}/12\mathbb{Z}$, $f_1(\bar{1}) = \bar{0}$

(b) $\mathbb{Z}/3\mathbb{Z} \xrightarrow{f_2} \mathbb{Z}/12\mathbb{Z}$, $f_2(\bar{1}) = \bar{4}$

(c) $\mathbb{Z}/3\mathbb{Z} \xrightarrow{f_3} \mathbb{Z}/12\mathbb{Z}$, $f_3(\bar{1}) = \bar{8}$

<u>morphisme de $\mathbb{Z}/12\mathbb{Z}$ dans $\mathbb{Z}/3\mathbb{Z}$</u>: Cette fois-ci, l'élément $\bar{1} \in \mathbb{Z}/12\mathbb{Z}$ est d'ordre 12, mais les éléments de $\mathbb{Z}/3\mathbb{Z}$ sont tous d'ordre divisant 3. Ainsi, il y a 3 morphismes de $\mathbb{Z}/12\mathbb{Z}$ dans $\mathbb{Z}/3\mathbb{Z}$, à savoir.

(a) $g_1: \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, $g_1(\bar{1}) = \bar{0}$

(b) $g_2: \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, $g_2(\bar{1}) = \bar{1}$

(c) $g_3: \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, $g_3(\bar{1}) = \bar{2}$

$\square$

<u>Ex 2</u>. $f: G \to G$, $x \mapsto x^2$

(1) <u>mq</u>. f est un morphisme $\Leftrightarrow$ G est abélien.

"$\Leftarrow$" Si G est abelien, on a $f(xy) = (xy)^2 = xy \cdot xy = xxyy = x^2y^2 = f(x)f(y)$ $\forall x, y$

cela dit, f est un morphisme.

"$\Rightarrow$" Si f est un morphisme, on a $f(xy) = f(x)f(y)$ $\forall x, y \in G$

d'où $(xy)^2 = x^2y^2$ $\forall x, y \in G$

d'où $xyxy = x^2y^2$ $\forall x, y \in G$

d'où $yx = xy$ $\forall x, y \in G$

c-à-d. G est abélien

(2) $K = \ker(f)$, $|G|$ est impair $\overset{??}{\Longrightarrow}$ $K = \{1\}$

Soit $x \in K = \ker(f) \Rightarrow f(x) = 1$ cela dit: $x^2 = 1$, d'où $\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\} = \{1, x\}$

donc $<x>$ est d'ordre divisant 2. c-à-d: $|<x>| \in \{1,2\}$

or par Lagrange, $|<x>|$ divise $|G|$, et $|G|$ est un nombre impair

$\Rightarrow$ $|<x>|$ est également un nombre impair

d'où $|<x>| = \{1\}$ et $x = 1$

donc $K = \{1\}$ et $f: G \to G$ est injective

Enfin, comme G est un ensemble fini, $f: G \to G$ est injective,

nécessairement f est bijective.

d'où $Im(f) = G$, c-à-d: $Q = G$

(3). $G = (\mathbb{Z}/p\mathbb{Z})^*$. mq $K = \{\bar{1}, \bar{-1}\}$

Soit $\bar{x} \in (\mathbb{Z}/p\mathbb{Z})^\times$, avec $x \in \mathbb{Z}$ (premier à p)

alors $\bar{x}^2 = \overline{x^2}$

donc $\bar{x} \in K \Leftrightarrow \bar{x}^2 = \bar{1} \Leftrightarrow \overline{x^2} = \bar{1} \Leftrightarrow x^2 \equiv 1 \pmod p$

$\Leftrightarrow x^2 - 1 \equiv 0 \pmod p$

$\Leftrightarrow p \mid (x^2 - 1)$

$\Leftrightarrow p \mid (x-1)(x+1)$

$\Leftrightarrow p \mid (x-1)$ ou $p \mid (x+1)$ (car p est un premier)

$\Leftrightarrow x \equiv 1 \pmod p$ ou $x \equiv -1 \pmod p$

$\Leftrightarrow \bar{x} = \bar{1}$ ou $\bar{x} = \overline{-1}$

ainsi, $K = \{\bar{1}, \bar{-1}\} = \{1, -1 \bmod p\}$

ex3. $A=\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ $B=\begin{pmatrix} j & 0 \\ 0 & j^2 \end{pmatrix}$ où $i=\sqrt{-1}$, $j=\exp(\frac{2\pi}{3}i)$. En particulier, $j^3=1$.

(1) $A^2=\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. $A^3=\begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$, $A^4=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=I_2$ (l'élément neutre de $GL(2,\mathbb{C})$)

donc A est d'ordre 4

$B^2=\begin{pmatrix} j^2 & 0 \\ 0 & j^4 \end{pmatrix}=\begin{pmatrix} j^2 & 0 \\ 0 & j \end{pmatrix}$ (car $j^3=1$!)

$B^3=\begin{pmatrix} j^3 & 0 \\ 0 & j^6 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. donc B est d'ordre 3

(2) calcul direct.

(3) G n'est pas commutatif : Sinon, par (2), on a $ABA^{-1}=B^2$

Si G commutatif, on aurait alors $B=B^2$, contradiction !

donc, G n'est pas commutatif

(4). mq $G=\{A^h B^k \mid h\in\{0,1,2,3\}, k\in\{0,1,2\}\}$

posons $\Gamma:=\{A^h B^k \mid \begin{smallmatrix} 0\leq h\leq 3 \\ 0\leq k\leq 2 \end{smallmatrix}\}$, clairement $\Gamma\subseteq G$

De plus, $\Gamma\leq G$ est un ss-gpe. comme A est d'ordre 4, B d'ordre 3

on a aussi $\Gamma=\{A^h B^k / \begin{smallmatrix} h\in\mathbb{Z} \\ k\in\mathbb{Z} \end{smallmatrix}\}$

Ensuite, on montre que $\Gamma\subseteq G$ est un sous gpe :

* $\Gamma\neq\emptyset$ c'est clair car $A\in\Gamma$
* pour $x=A^h B^k$, $y=A^{h'}B^{k'}$, on a

$$xy^{-1}=A^h B^k (A^{h'}B^{k'})^{-1}=A^h B^k B^{-k'} A^{-h'}$$
$$=A^h B^{k-k'} A^{-h'}$$

donc, on se ramène à montrer que $B^b A^a\in\Gamma$ pour tout $a,b\in\mathbb{Z}$

comme $A,B\in GL_2(\mathbb{C})$ sont d'ordre fini, on peut m̂ supposer $a,b\geq 0$

on va raisonner par récurrence sur a.

Si $a=0$, alors $B^bA^0 = B^b \in \Gamma$

Supposons maintenant que l'assertion a été vérifiée pour $a = a_0 \geq 0$; c-à-d : $B^bA^{a_0} \in \Gamma$

Autrement dit, $\exists\, h, k \geq 0$ avec $B^bA^{a_0} = A^hB^k$

Ainsi, $B^bA^{a_0+1} = B^bA^{a_0} \cdot A = A^hB^k \cdot A$

$$= A^h B^{k-1} B A$$
$$= A^h B^{k-1} A B^2 \quad (\text{on utilise (2) ici})$$
$$= A^h B^{k-2} B A B^2$$
$$= A^h B^{k-2} A B^2 B^2 = A^h B^{k-2} A B^4$$
$$= \cdots = A^h A B^{2k} = A^{h+1} B^{2k} \in \Gamma$$

ceci finit la récurrence, et on a $B^bA^a \in \Gamma$

par suite $\Gamma \leq G$ est un sous-gpe, contenant A, B

or G est engendré par A, B, on a forcément $G = \Gamma$

<u>donc</u> : $G = \Gamma = \left\{ A^hB^k \;\middle|\; \begin{array}{l} 0 \leq h \leq 3 \\ 0 \leq k \leq 2 \end{array} \right\}$

(5). par (4), on a $|G| \leq 4 \times 3 = 12$

D'autre part, soient $h, h' \in \{0,1,2,3\}$, et $k, k' \in \{0,1,2\}$ tels que $A^hB^k = A^{h'}B^{k'}$

d'où $A^{h-h'} = B^{k'-k}$

or par (2), A est d'ordre 4, donc $A^{h-h'}$ est d'ordre divisant 4,

B est d'ordre 3, donc $B^{k'-k}$ est d'ordre divisant 3

par suite, $A^{h-h'} = B^{k'-k}$ est d'ordre divisant à la fois 4 et 3

donc, $A^{h-h'} = B^{k'-k}$ est d'ordre 1

C-à-d : $A^{h-h'} = B^{k'-k} = I_2$

d'où $A^h = A^{h'}$ et $B^k = B^{k'}$. Enfin, comme $h, h' \in \{0, \ldots, 3\}$, $k, k' \in \{0,1,2\}$

nécessairement $h = h'$ et $k = k'$

Ainsi, parmi les 12 éléments suivants : A^hB^k $(0 \leq h \leq 3,\ 0 \leq k \leq 2)$

il n'y a pas de répétition. donc $|G| \geq 12$, et enfin on a $|G| = 12$ $\square$