Exercice 07 : (08)

i) a) les sous groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ et l'image de $n\mathbb{Z}$ par π.

on a :

Soit H un sous groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$, puisque la surjection canonique :

$\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ est un morphisme de groupes

$\pi^{-1}(H)$ est un sous groupe de $\mathbb{Z}$ (d'après l'exercice 02)

alors il existe $k \in \mathbb{Z}$ tel que $\pi^{-1}(H) = k\mathbb{Z}$ (d'après l'exercice 8).

(02)

comme π est surjective, on a :

$$H = \pi(\pi^{-1}(H)) = \pi(k\mathbb{Z}) = d\mathbb{Z}/n\mathbb{Z} \quad \text{t.q } d = PGCD(k, n).$$

donc les sous groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $k'\mathbb{Z}/n\mathbb{Z}$ t.q $k' \in \mathbb{Z}$ et k'/n.

l'image de $n\mathbb{Z}$ est $\pi(n\mathbb{Z}) = d\mathbb{Z}/n\mathbb{Z}$ t.q $d = PGCD(n, n)$.

b) Soit $(G, *)$ est cyclique i.e $G = \{a^k / k \in \mathbb{Z}\}$ d'ordre finie et $(G', *')$ est cyclique.

i.e $G' = \{b^{k'}$ t.q $k' \in \mathbb{Z}\}$ d'ordre finie. M.q G et G' sont isomorphes.

on a G est cyclique i.e $\exists f_1 : G \longrightarrow \mathbb{Z}/n\mathbb{Z}$ isomorphisme

G' est cyclique i.e $\exists f_2 : \mathbb{Z}/n\mathbb{Z} \longrightarrow G'$ isomorphisme.

(02)

$f_2 \circ f_1$ est un isomorphisme car.

$f_2 \circ f_1 : G \xrightarrow{f_1} \mathbb{Z}/n\mathbb{Z} \xrightarrow{f_2} G'$ est bien définie car $\forall x \in G ; f_2 \circ f_1(x) \in G'$

$\forall x_1, x_2 \in G \quad f_2 \circ f_1(x_1 * x_2) = f_2(f_1(x_1) + f_1(x_2)) = f_2(f(x_1)) *' f_2(f_1(x_2))$

i.e $f_2 \circ f_1$ est un morphisme de groupe

$\ker(f_2 \circ f_1) = (f_2 \circ f_1)^{-1}(e_{G'}) = f_1^{-1} \circ f_2^{-1}(e_{G'}) = f_1^{-1}(\overline{0}) = e_G$ car f_1 est injective, car f_2 est injective

i.e $f_2 \circ f_1$ est injective

car f_1 est surjective

$\text{Im } f_2 \circ f_1 = f_2 \circ f_1(G) = f_2(\mathbb{Z}/n\mathbb{Z}) = G'$ car f_2 est surjective.

i.e $f_2 \circ f_1$ est une application bijective + morphisme donc isomorphisme

alors G et G' sont isomorphes.

II) 1) Déterminer les morphismes de groupes entre $(\mathbb{Z}/p\mathbb{Z}, +)$ et $(\mathbb{Z}/q\mathbb{Z}, +)$.

on note $d = PGCD(p,q)$.

EXO: 01

$\exists$ n'et n' t.q $p = dp'$ et $q = dq'$ et $q' \wedge p' = 1$.

soit f un morphisme de groupes de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathbb{Z}/q\mathbb{Z}$. i.e $x \in \{0, \dots, p-1\}$ i.e $x \in \{0, 1, \dots, p-1\}$.

$\bar{x} = \bar{1} + \bar{1} + \dots + \bar{1} = x\bar{1}$. on a

$f(\bar{x}) = \underbrace{f(\bar{1}) + \dots + f(\bar{1})}_{x \text{ fois}} = x f(\bar{1})$.

on pose $f(\bar{1}) = \bar{a}$ $a \in \{0, 1, 2, \dots, q-1\}$.

$p\bar{a} = p f(\bar{1}) = f(\bar{p}) = f(\bar{0}) = \bar{0}$. car f est un morphisme. (02)

donc q/pa en simplifiant par d $dq'/dp'a$ i.e $q'/p'a$.

d'on q'/a (car p' et q' sont premiers entres eux)

donc il existe $k \in \{0, 1, \dots, k-1\}$ tel que $a = kq'$ ($t.q$ $q' = \frac{q}{d}$)

alors les morphisme de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathbb{Z}/q\mathbb{Z}$ sont

$f(\bar{x}) = \overline{xkq'}$ et $k \in \{0, 1, \dots, d-1\}$.

inversement pour $k \in \{0, \dots d-1\}$ $f_k : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/q\mathbb{Z}$.

$\bar{x} \longrightarrow \overline{kq'x}$

est un morphisme de groupes.

III) 1) Montrer que $(\mathbb{Z}/7\mathbb{Z}^*, \times)$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, +)$. (02)

il suffit de montrer que les deux groupes sont cycliques de même ordre. on a $\mathbb{Z}/7\mathbb{Z}^* = \{1, 2, 3, 4, 5, 6\} = \{3^k / k \in \mathbb{Z}\}$ est un groupe cyclique d'ordre 6.

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\} = \{k(1,1) / k \in \mathbb{Z}\}$ est un groupe cyclique d'ordre 6 donc les deux groupe sont isomorphe

$f(k(1,1)) = 3^k$ isomorphisme

Exercice 02 :

1) M.q le groupe de Klein $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ n'est pas isomorphe à $(\mathbb{Z}/4\mathbb{Z})$

le groupe $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ n'est pas cyclique car n'est pas homogène (n'admet pas un élément générateur), le groupe $(\mathbb{Z}/4\mathbb{Z})$ est un groupe cyclique donc les deux groupes ne sont pas isomorphes. (01)

2) le même raisonnement de question 1). (01)

3) M.q $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes $\Leftrightarrow$ PGCD $(m,n)=1$.

Supposons que $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes alors $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est cyclique i.e $\exists (x,y) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ d'ordre mn (l'élément générateur)

i.e $mn(x,y) = (mnx, mny) = (0,0)$ avec

$mn = \min \{k \in \mathbb{N}^* \text{ t.q } k(x,y) = (0,0)\}$. (01.)

Si PGCD $(m,n) = d \neq 1$ alors $\exists m_1, n_1 \in \mathbb{N}$ t.q $m = dm_1$ et $n = dn_1$ avec $n_1 \wedge m_1 = 1$ on a $dm_1 n_1 = m n_1 = n m_1$ est un multiple de m et est un multiple de n donc.

~~$dm_1 n_1 = mn_1 = nm_1$ est un multiple de n et est un multiple de m~~

$d_{m_1 n_1}(x,y) = (mn_1 x, nm_1 y) = (0,0)$ avec $d_{m_1 n_1} < mn = dm_1 dn_1$ contradiction tel que l'ordre de $(x;y)$ est $\min \{k \in \mathbb{N}^*$ tel que $k(x,y) = (0,0)\}$ donc $d = 1$

Supposons maintenant que PGCD $(m,n) = d \neq 1$ alors PPCM $(m,n) = mn$

donc $mn(1,1) = (mn, mn) = (0,0)$ tel que $mn = \min \{k \in \mathbb{N}^*$ tel que $k(1,1) = (0,0)\}$

donc $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} = \langle (1,1) \rangle$ alors $(1,1)$ est d'ordre mn i.e $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre mn) donc $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{Z}/mn\mathbb{Z}$.

Exercice 03: Soit q un nombre premier et k un entier premier avec $q-1$

Montrer que l'application $\mathcal{T}: \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ définie par $\mathcal{T}(x) = x^k$ est bijective.

on a $k \wedge (q-1) = 1$ d'après l'égalité de Bézout

$\exists\, u$ et v tels que $ku + (q-1)v = 1$.

Considérons alors l'application $\mathcal{Y}: \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ définie par.

$\mathcal{Y}(x) = x^u$

alors

$$\mathcal{Y}(\mathcal{T}(x)) = x^{ku} = x^{(q-1)v+1}$$

$$= x \times x^{(q-1)v}$$

donc si $x = 0$ alors $\mathcal{Y}(\mathcal{T}(x)) = 0 = x$.

si $x \neq 0$ alors par le petit théorème de Fermat.

$x^{q-1} = 1$. puis $x^{(q-1)u} = 1$. donc $\mathcal{Y}(\mathcal{T}(x)) = x$.

Ainsi $\mathcal{Y} \circ \mathcal{T} = Id$ et de même $\mathcal{T} \circ \mathcal{Y} = Id$.

i.e $\mathcal{T}$ est bijective.

03

Exercice 04 :

Soit $\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 5 & 6 & 8 & 1 & 7 & 3 \end{pmatrix}$.

$\tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 2 & 8 & 1 & 3 & 4 & 7 & 5 \end{pmatrix}$.

06

1) Calculer $\tau_1 \circ \tau_2$, que peut-on déduire ?

on a $\tau_1 \circ \tau_2 = Id$ i.e $\tau_1 = (\tau_2)^{-1}$ et $\tau_2 = (\tau_1)^{-1}$. (01)

2) décomposition de τ_1 :

on a $\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 3 & 6 & 5 & 1 & 7 & 8 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 5 & 4 & 8 & 6 & 7 & 3 \end{pmatrix}$. (01)

$= \Gamma_{1,6} \circ \Gamma_{1,4} \circ \Gamma_{3,8} \circ \Gamma_{3,5}$ (01)

donc $(\tau_1)^{-1} \tau_2 = \Gamma_{3,5} \circ \Gamma_{3,8} \circ \Gamma_{1,4} \circ \Gamma_{1,6}$. (car $(\Gamma_{3,6} \circ \Gamma_{1,4} \circ \Gamma_{3,8} \circ \Gamma_{3,5})^{-1} = (\Gamma_{3,5})^{-1} \circ (\Gamma_{3,8})^{-1} \circ (\Gamma_{1,4})^{-1} \circ (\Gamma_{3,6})^{-1}$ (01)

la signature alors ~~l'ordre~~ de $\tau_1 = (-1)^4 = 1$ et ~~d'ordre~~ de $(\Gamma_{i,j})^{-1} = \Gamma_{i,j}$

$\tau_2 = (-1)^4 = 1$. (01)

~~L'ordre~~ de

$ord(\tau_1) = PPCM(3,3) = 3$.

et $ord(\tau_2) = PPCM(3,3) = 3$.

$2019 = 0 [3]$.

donc $\tau_1^{2019} = Id$. et $\tau_2^{2019} = Id$. (01)