# Maths 4 : TD 4 Théorie des groupes

23.03.2021

## Exercice 2

**commutativité** : a-t-on $a * b = b * a$ pour tout $a, b \in G$ ?

ici $x * y = t \neq y * x = z$ Donc la loi n'est pas commutative.

**loi de groupe** : vérifier que
1) associativité : $(a * b) * c = a * (b * c) \quad \forall a, b, c \in G$
2) el. neutre e : $e * a = a * e = a \quad \forall a \in G$
3) inverse : $\forall a \in G \ \exists a' \in G$ tq $a * a' = a' * a = e$

Vérifions 2) : ici e est l'élément neutre. On le voit en examinant la table
$e * a = a = a * e \quad \forall a \in G$

Vérifions 3) : en lisant la table, on voit que $\forall a \in G$, $a * a = e$ qui est l'élément neutre.
Chaque élément est son propre inverse.

Vérifions 1) : par exemple on a $(x * y) * z = t * z = x$ et $x * (y * y) = x * t = z$
Donc la loi n'est PAS associative.

Donc $(G, *)$ n'est pas un groupe.

## Exercice 3

Notons $G = \{e, x\}$

On doit avoir $\begin{cases} e * e = e \\ e * x = x \\ x * e = x \end{cases}$ pour que e soit l'élément neutre

On a ou bien $x * x = e$ ou bien $x * x = x$

Supposons que $x * x = x$
Alors on a aussi $\underbrace{(\underbrace{x^{-1} * x}_{e}) * x}_{x} \neq \underbrace{x^{-1} * x}_{e} = x^{-1} * \underbrace{(x * x)}_{x}$

contradictO car $x \neq e$

Donc c'est $x * x = e$

| | e | x |
|---|---|---|
| e | e | x |
| x | x | e |

On vérifie qu'on a bien les 3 axiomes :
2) OK : e est le neutre
3) OK : e inverse de e et x inverse de x
1) OK

deux façons pour vérifier :
a) faire le calcul : on vérifie tous les triplets
ou b) On constate que la table s'identifie avec la table suivante :

| + | $\bar{0}$ | $\bar{1}$ |
|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{0}$ |

qui est la table de multiplication du groupe $(\mathbb{Z}/2\mathbb{Z}, +)$ qui est associative.

Donc c'est bien la table de multiplication du groupe.

## Exercice 4

Soit $G = \{e, x, y\}$

On note $e$ l'élément neutre

| $*$ | $e$ | $x$ | $y$ |
|---|---|---|---|
| $e$ | $e$ | $x$ | $y$ |
| $x$ | $x$ | | |
| $y$ | $y$ | | |

Examinons les possibilités pour $x * x$

- si $x * x = x$ alors $x = e$ (voir ex précédent)
- supposons $x * x = e$. Alors $x = x^{-1}$

Rq sur chaque ligne de la table de multiplication d'un groupe, chaque élément apparait une fois et une seule.

↳ considérons la ligne associée à un élément $g \in G$
Cette ligne contient $g * h$ à la colonne associée à $h \in G$.

On l'application $\lambda_g : G \to G$, $h \mapsto g * h$ est bijective de réciproque $G \to G$, $k \mapsto g^{-1} * k$

(on a $\lambda_g^{-1} \circ \lambda_g(h) = g^{-1} * (g * h) = (g^{-1} * g) * h = e * h = h$ d'où avec $\lambda_g \circ \lambda_g^{-1}(h) = h$)

Donc si $x * x = e$, alors $x * y = y$
Mais alors $y = e$ CONTRADICTION
(multiplier à droite par $y^{-1}$)

| $*$ | $e$ | $x$ | $y$ |
|---|---|---|---|
| $e$ | $e$ | $x$ | $y$ |
| $x$ | $x$ | $e$ | $y$ |
| $y$ | $y$ | | |

- donc $x * x = y$

et alors $x * y = e$ car $e$ doit apparaître sur la ligne

Dans chaque colonne aussi, chaque él doit apparaître une seule fois.

| $*$ | $e$ | $x$ | $y$ |
|---|---|---|---|
| $e$ | $e$ | $x$ | $y$ |
| $x$ | $x$ | $y$ | $e$ |
| $y$ | $y$ | $e$ | $x$ |

On a donc montré qu'un ensemble à 3 éléments admet au plus 1 structure de groupe après avoir choisi un élément neutre.

Il reste à vérifier qu'il existe au moins une structure de groupe, c'est-à-dire que cette table définit bien un groupe.
Deux possibilités :
a) vérification en faisant le calcul pour les $3^3 = 27$ triplets.
ou b) On observe que la table s'identifie avec celle du groupe $(\mathbb{Z}/3\mathbb{Z}, +)$

**Conclusion** : Pour un ensemble à 3 éléments → 3 lois de groupe correspondant aux 3 choix possibles pour l'élément neutre.

## Exercice 5

Abrégeons $x*y$ en $xy$ la notation pour les produits dans $G$.

L'hypothèse est que $x^2 = e \quad \forall x \in G$

Autrement dit $x = x^{-1} \quad \forall x \in G$

Soient $x, y \in G$

On a $xy = (xy)^{-1}$

## Exercice 6

On a $yx = xy^2$ et $xy = yx^2$

Donc $yx = xyy = yx^2y = yxxy$

On multiplie à gauche par $x^{-1}y^{-1}$

$\Rightarrow \quad e = xy \quad \Rightarrow x^{-1} = y$

On $\underbrace{yx}_{=e} = xy^2 = \underbrace{xy}_{=e}y \quad \Rightarrow y = e \quad \Rightarrow x = y^{-1} = e$

On a bien $x = y = e = 1$.

25.03.2021

## Exercice 4 (fin)

$G$ groupe à 4 éléments, $(G, \cdot)$

$G = \{e, x, y, z\}$

$\text{ord}(x) = \min\{n \in \mathbb{N}^* \text{ tq } x^n = e\}$

Rappel: si $H \subset G$ et $H$ et $G$ sont finis, $|H|$ divise $|G|$ (Lagrange)

soit $H = \langle x \rangle = \{e, x, \dots, x^{n-1}\}$ où $n = \text{ord}(x)$

donc $|H| = n$

Donc $\text{ord}(x) \in \{1, 2, 4\}$ $x \neq e$

$\text{ord}(y) \in \{1, 2, 4\}$ $y \neq e$

$\text{ord}(z) \in \{1, 2, 4\}$ $z \neq e$

① $\exists$ un élément d'ordre 4 dans $G = \{e, x, y, z\}$
Par symétrie, on peut supposer que c'est $x$.

Alors $\langle x \rangle \subset G \Rightarrow \langle x \rangle = G$ (tous les 2 d'ordre 4)

$G \cong \mathbb{Z}/4\mathbb{Z}$ ↑ isomorphe à $\qquad G \to (\mathbb{Z}/4\mathbb{Z}, +)$, $x \mapsto \bar{1}$

② $\nexists$ d'él d'ordre 4

Alors $\text{ord}(x) = \text{ord}(y) = \text{ord}(z) = 2$

donc $x^2 = e$, $y^2 = e$ et $z^2 = e$

| | $e$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|
| $e$ | $e$ | $x$ | $y$ | $z$ |
| $x$ | $x$ | $e$ | $z$ | $y$ |
| $y$ | $y$ | $z$ | $e$ | $x$ |
| $z$ | $z$ | $y$ | $x$ | $e$ |

il faut que chaque lettre apparaisse 1 fois sur la ligne et 1 fois sur la colonne

$G \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ ↖ groupe de Klein

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{1},\bar{0}), (\bar{1},\bar{1})\}$
$\quad = e \quad = x \quad = y \quad = z$

Donc en tout y'a **2 groupes**.

## Exercice 7 $\quad n \in \mathbb{N}^*$

$$\mu_n = \{z \in \mathbb{C} \text{ tq } z^n = 1\}$$
$$= \left\{\exp\left(\frac{2ik\pi}{n}\right),\ k = 0, \dots, n-1\right\}$$

1) Pq $\mu_n$ sous-groupe de $(\mathbb{C}^*, \times)$

Vérifions : ① $1 \in \mu_n$ donc $\mu_n \neq \emptyset$

② $x, y \in \mu_n \quad xy \in \mu_n$ stabilité par le produit

③ $x \in \mu_n \quad x^{-1} \in \mu_n$ stabilité par l'inverse

① $1^n = 1$ donc $1 \in \mu_n$

② $x, y \in \mu_n \quad (xy)^n = x^n y^n = 1 \times 1 = 1$
↑ car $x, y \in \mu_n$

donc $xy \in \mu_n$

③ $x \in \mu_n \quad (x^{-1})^n = (x^n)^{-1} = 1$

donc $x^{-1} \in \mu_n$

2) Mq $\mathbb{U}_m$ cyclique d'ordre $m$.

$$\mathbb{U}_m = \left\{ \exp(2i\pi k/m),\ k = 0, 1, \dots, m-1 \right\}$$

$$= \left\{ \exp(\underbrace{2i\pi/m}_{\omega})^k, \dots \right\}$$

$$= \left\{ 1, \omega, \omega^2, \dots, \omega^{m-1} \right\}$$

Donc $\mathbb{U}_m = \langle \omega \rangle \subset \mathbb{C}^*$ et $\text{ord}(\omega) = m$.

3) Mq $\mathbb{U}_m \subseteq \mathbb{U}_n$ ssi $m \mid n$

⇐ On suppose $m \mid n$ $\Leftrightarrow \exists k$ tq $mk = n$

Soit $z \in \mathbb{U}_m$

$$z^n = z^{mk} = (z^m)^k = 1^k = 1$$

donc $z \in \mathbb{U}_n$

On a bien $\mathbb{U}_m \in \mathbb{U}_n$

⇒ On suppose $\mathbb{U}_m \subseteq \mathbb{U}_n$ donc $m \leq n$

$n = qm + r$ (div euclidienne de $n$ par $m$)
$0 \leq r \leq m-1$

$z \in \mathbb{U}_m \subseteq \mathbb{U}_n$ avec $\text{ord}(z) = m$ ($z$ engendre le groupe)

donc $1 = z^n = z^{mq+r} = (z^m)^q z^r = 1^q \times z^r = z^r$

$\Rightarrow z^r = 1$

donc $\text{ord}(z)$ divise $r$ (si $r > 0$)

$r < m = \min \{ k \in \mathbb{N}^* \text{ tq } z^k = 1 \}$
pb $z^r = 1$

$\Rightarrow r = 0$

$\Rightarrow m \mid n$

## Exercice 8

$(\mathbb{Z}/12\mathbb{Z}, +)$

$\text{ord}(\bar{0}) = 1$ → c'est le neutre – L'ordre d'un élément ne peut pas être 0.
$\text{ord}(\bar{1}) = 12$
$\text{ord}(\bar{2}) = 6$ $\quad \langle \bar{2} \rangle = \{ \bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10} \}$
$\text{ord}(\bar{3}) = 4$
$\text{ord}(\bar{4}) = 3$
$\text{ord}(\bar{5}) = 12$
$\text{ord}(\bar{6}) = 2$
$\text{ord}(\bar{7}) = 12$
$\text{ord}(\bar{8}) = 3$
$\text{ord}(\bar{9}) = 4$
$\text{ord}(\bar{10}) = 6$
$\text{ord}(\bar{11}) = 12$

Valeurs possible : 1 et tout ce qui divise 12
$\text{ord}(\bar{k}) \in \{ 1, 2, 3, 4, 6, 12 \}$

on cherche le 1er produit divisible par 12
$\text{ord}(\bar{k}) = \min \{ n \in \mathbb{N}^* \ n\bar{k} = \bar{0} \}$

Formule générale pour $\mathbb{Z}/n\mathbb{Z}$ :

$$\text{ord}(\bar{k}) = n / \text{PGCD}(k, n)$$

$(\mathbb{Z}/12\mathbb{Z})^* = \{ \bar{k} \in \mathbb{Z}/12\mathbb{Z} \mid \exists \bar{l} \in \mathbb{Z}/12\mathbb{Z} \ \ \bar{k}\bar{l} = \bar{1} \}$ → les inversibles pour la multiplication.

$= \{ \bar{1}, \bar{5}, \bar{7}, \bar{11} \}$ = $\{ \bar{k} \in \mathbb{Z}/12\mathbb{Z} \text{ tq } PGCD(k,12) = 1 \}$

↳ groupe d'ordre 4

$ord(\bar{1}) = 1$ car $1^1 \equiv 1 \bmod 12$

$ord(\bar{5}) = 2$ car $5^2 = 25 \equiv 1 \bmod 12$

$ord(\bar{7}) = 2$ car $7^2 = 42 \equiv 1 \bmod 12$

$ord(\bar{11}) = 2$

ici $ord(\bar{k}) = \min \{ n \in \mathbb{N}^* \text{ tq } \bar{k}^n = 1 \}$ ↳ pour la multiplication

$ord(\bar{k}) \in \{2, 4\}$ car $\bar{k} \neq \bar{1}$

$((\mathbb{Z}/12\mathbb{Z})^*, \cdot) \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$

↳ pas un groupe cyclique car pas d'el. d'ordre 4

30.03.2021

## Exercice 9

G abélien : $xy = yx \ \forall (x,y) \in G^2$ la loi du groupe est commutative

$H = \{ x \in G \text{ tq } ord(x) \text{ fini} \}$

$= \{ x \in G \mid \exists n \in \mathbb{N}^* \text{ tq } x^n = e \}$

↑ dépend de l'élément $x$

Mq H est un sous-groupe de G.

ie Mq ① $e \in H$

② si $x \in H$, $y \in H$ alors $xy \in H$

③ si $x \in H$ alors $x^{-1} \in H$

1) $e \in H$ car $e^1 = e$ donc $ord(e) = 1$ (élément neutre est d'ordre fini).

3) Si $x \in H$, $\exists n \in \mathbb{N}^*$ tq $x^n = e$ $\iff$ $(x^{-n})\, x^n = x^{-n}$

$\iff$ $e = x^{-n} = (x^{-1})^n$

donc $ord(x^{-1}) = n$ et $x^{-1} \in H$

2) $x \in H$ donc $\exists n \in \mathbb{N}^*$ tq $x^n = e$

$y \in H$ donc $\exists m \in \mathbb{N}^*$ tq $y^m = e$

alors $(xy)^{n \times m} = x^{nm} \cdot y^{nm} = (x^n)^m \times (y^m)^n = e^m \times e^n = e$ donc $xy$ est d'ordre fini et $xy \in H$.

↑ car G abélien

Q : si $x$ et $y$ d'ordre fini et $xy = yx$ $ord(xy) = ord(x) \times ord(y)$ ?

NON pas en général

par contre on a $ord(xy) = PPCM(ord(x), ord(y))$.

## Exercice 10

$G = \{ e^{2i\pi r}, r \in \mathbb{Q} \} \subset \mathbb{C}^*$

- Montrons que $G$ est un sous-groupe de $(\mathbb{C}^*, \cdot)$

1) $1 \in G$ car $1 = e^{2i\pi \cdot 0}$, $0 \in \mathbb{Q}$

2) $x = \exp(2i\pi r) \in G$, $x' = \exp(2i\pi r') \in G$, avec $(r, r') \in \mathbb{Q}^2$

$x x' = \exp(2i\pi(r+r'))$ avec $r + r' \in \mathbb{Q}$

donc $xx' \in G$

3) $x = \exp(2i\pi r) \in G$, $r \in \mathbb{Q}$

$x^{-1} = (\exp(2i\pi r))^{-1} = \exp(2i\pi(-r))$ et $-r \in \mathbb{Q}$

donc $x^{-1} \in G$

Donc $G$ est un groupe (sous-groupe de $\mathbb{C}^*$)

- Soit $x \in G$, $x = \exp(2i\pi r)$, $r \in \mathbb{Q}$

Alors $r = \frac{p}{q}$, $PGCD(p, q) = 1$

$x^q = \exp(2i\pi \frac{p}{q})^q = \exp(2i\pi \frac{p}{q} q) = \exp(2i\pi p) = \exp(2i\pi)^p = (\cos(2\pi) + i \sin(2\pi))^p = (1 + i.0)^p = 1$

donc $\forall x \in G$, $x$ est d'ordre fini ($ord(x) \leq q$)

- Soit $\{ \omega_n = \exp(\frac{2i\pi}{n}), n \in \mathbb{N}^* \} \subset G$

↑ ensemble infini (car $\omega_n \neq \omega_{n'}$ si $n \neq n'$)

donc $G$ est infini

## Exercice 12

$M_2(\mathbb{Z}) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, (a, b, c, d) \in \mathbb{Z}^4 \}$

$SL_2(\mathbb{Z}) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, (a, b, c, d) \in \mathbb{Z} \text{ avec } ad - bc = 1 \}$

$SL_2(\mathbb{Z}) \subset \underbrace{GL_2(\mathbb{R})}_{\text{c'est un groupe}} = \{ A \in M_2(\mathbb{R}) \text{ tq } \det A \neq 0 \}$

a) Montrons que $(GL_2(\mathbb{R}), \times)$ est un groupe

1) $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R})$

2) $(AB)C = A(BC)$ associativité du produit des matrices

3) $A, B \in GL_2(\mathbb{R})$ alors $AB \in GL_2(\mathbb{R})$

car $\det(AB) = \underbrace{\det(A)}_{\neq} \underbrace{\det(B)}_{\neq} \neq 0$

4) $A \in GL_2(\mathbb{R})$ $\det(A) \neq 0$ alors $A$ est inversible

$$\det(A^{-1}) = \frac{1}{\det(A)} \neq 0 \quad \text{donc } A^{-1} \in GL_2(\mathbb{R})$$

1) • Mq $SL_2(\mathbb{Z})$ est un sous-groupe de $GL_2(\mathbb{R})$

1) $I_2 \in SL_2(\mathbb{Z})$

2) $A \in SL_2(\mathbb{R})$, $A' \in SL_2(\mathbb{Z})$

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad A' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

$\det(AA') = \det(A) \times \det(A') = 1 \times 1 = 1$

et $AA' = \begin{pmatrix} aa'+bc' & ab'+bd' \\ a'c+c'd & b'c+dd' \end{pmatrix} \in M_2(\mathbb{Z})$

3) $A \in SL_2(\mathbb{Z})$ $\det A = 1 \neq 0$ donc $A$ inversible

$A^{-1} \in GL_2(\mathbb{R})$ et $\det A^{-1} = \frac{1}{\det A} = 1$

donc $A^{-1} \in SL_2(\mathbb{Z})$

• $\left\{ \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}, k \in \mathbb{Z} \right\} \subset SL_2(\mathbb{Z})$ donc $SL_2(\mathbb{Z})$ infini.

(infini)

• $SL_2(\mathbb{Z})$ non abélien car

2) $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$

$AB = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \neq BA = \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}$

$A^2 = \dots$

$A^3 = \dots$

$A^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ donc $\text{ord}(A) = 4$

$B^2 = \dots$

$B^3 = I_2$ donc $\text{ord}(B) = 3$

$(AB)^2 = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$ $(AB)^4 = \begin{pmatrix} 1 & -4 \\ 0 & 1 \end{pmatrix}$

$(AB)^3 = \begin{pmatrix} -1 & 3 \\ 0 & -1 \end{pmatrix}$ Par récurrence $(AB)^m = \begin{pmatrix} (-1)^m & (-1)^{m-1} \cdot m \\ 0 & (-1)^m \end{pmatrix}$ donc $AB$ d'ordre infini.

## Exercice 14

$$\left((\mathbb{Z}/13\mathbb{Z})^*, \times\right) = \left\{ \bar{k} \in \mathbb{Z}/13\mathbb{Z},\ \text{PGCD}(k,13) = 1 \right\}$$

$$= \left\{ \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}, \bar{12} \right\}$$

$$\left|(\mathbb{Z}/13\mathbb{Z})^*, \times)\right| = \left|\mathbb{Z}/13\mathbb{Z} \setminus \{\bar{0}\}\right| = 12$$

rattraper la suite

01/04/2021

## Suite de l'exo

Calculer $\text{ord}(\bar{2})$ dans $((\mathbb{Z}/13\mathbb{Z})^*, \times)$ (cardinal = 12)

$\text{ord}(\bar{2}) \in \{2, 3, 4, 6, 12\}$
↳ divise 12
↳ pas 1 car $\bar{2}^1 = \bar{2}$

$\bar{2}^2 = \bar{4} \neq \bar{1}$
$\bar{2}^3 = \bar{8} \neq \bar{1}$
$\bar{2}^4 = \bar{4}^2 = \overline{16} = \bar{3} \neq \bar{1}$
$\bar{2}^6 = \bar{4} \cdot \overline{16} = \bar{4} \cdot \bar{3} = \overline{12} \neq \bar{1}$

donc $\boxed{\text{ord}(\bar{2}) = 12}$

quel groupe est $((\mathbb{Z}/13\mathbb{Z})^*, \times)$ ?

1) $(\mathbb{Z}/12\mathbb{Z}, +)$ ?
2) $(\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ ?
3) $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ ?
4) $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, +)$ ?

**Rappel :** $G$ est un groupe cyclique si $\exists x \in G$ tq $\langle x \rangle = G$

En d'autres termes $G = \{e, x, x^2, \dots, \underbrace{x^{\text{ord}(x)-1}}_{\text{ord}(x)}\}$

Si $G$ est cyclique, $\exists x$ tq $\text{ord}(x) = \text{card}(G)$

$\left((\mathbb{Z}/13\mathbb{Z})^*, \times\right)$ est cyclique car $\text{ord}(\bar{2}) = 12$

Donc $(\mathbb{Z}/13\mathbb{Z})^* = \langle \bar{2} \rangle$

$$\left((\mathbb{Z}/13\mathbb{Z})^*, \cdot\right) \to (\mathbb{Z}/12\mathbb{Z}, +)$$
$$\bar{2} \mapsto \bar{1}$$

On def un morphisme

06. 04. 2021

## Exercice 13

$G$ un groupe, $x, y \in G$ qui commutent $(xy = yx)$

$\left.\begin{array}{l} \text{ord}(x) = a \\ \text{ord}(y) = b \end{array}\right\}$ $\text{PGCD}(a, b) = 1$

Montrer $\text{ord}(xy) = ab$

$(xy)^{ab} = x^{ab} y^{ab}$ car $x$ et $y$ commutent

$= (x^a)^b (y^b)^a$

$= e^b e^a = e$

Donc l'ordre de $xy$ divise $ab$.

Soit $k = \text{ord}(a, b)$

$(xy)^k = x^k y^k = e$ donc $x^k = y^{-k}$ $\Rightarrow$ $x^{ak} = y^{-ak} = e$

or $b = \text{ord}(y)$ donc $b$ divise $ak$

or $a \wedge b = 1$ donc d'après le lemme de Gauss, $b \mid k$

de même $x^{bk} = y^{-bk} = e$ or $a = \text{ord}(x)$ donc $a \mid bk$ donc $a \mid k$ car $a \wedge b = 1$

Donc $a \mid k$ et $b \mid k$

D'après le lemme de Gauss, $ab \mid k$ (car $a \wedge b = 1$)

Donc $k \mid ab$ et $ab \mid k$, $k, a, b \in \mathbb{N}$

Donc $k = ab = \text{ord}(xy)$