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) él. 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 $x * (y * z) = x * t = z$
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 $x = x^{-1}$

Mq 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 $\lambda_g^{-1} \circ \lambda_g (h) = g^{-1} * (g * h) = (g^{-1} * g) * h = e * h = h$ de m̂ 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) vérificatO 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 élément → 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 $x^{-1}y^{-1}$

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

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

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

25.03.2021

Exercice 4 (fin)

G groupe à 4 éléments, $(G, \cdot)$

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

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

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 $n = \operatorname{ord}(x)$

donc $|H| = n$

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

$\operatorname{ord}(y) \in \{\cancel{1}, 2, 4\}$ $\quad y \neq e$

$\operatorname{ord}(z) \in \{\cancel{1}, 2, 4\}$ $\quad z \neq e$

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)

$G \cong \mathbb{Z}/4\mathbb{Z}$ $\quad$ $G \to (\mathbb{Z}/4\mathbb{Z}, +)$, $\; x \mapsto \bar{1}$

↑ isomorphe à

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 apparaissent 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

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

Donc en tout y'a $\boxed{2 \text{ groupes}}$.

Exercice 7

$n \in \mathbb{N}^*$

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

1) Mq $\mathcal{U}_n$ sous-groupe de $(\mathbb{C}^*, \times)$

<u>Vérifier:</u> ① $1 \in \mathcal{U}_n$ donc $\mathcal{U}_n \neq \emptyset$

② $x, y \in \mathcal{U}_n$ $\quad xy \in \mathcal{U}_n$ stabilité par le produit

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

① $1^n = 1$ donc $1 \in \mathcal{U}_n$

② $x, y \in \mathcal{U}_n$ $\quad (xy)^n = x^n y^n = 1 \times 1 = 1$

↑ car $x, y \in \mathcal{U}_n$

donc $xy \in \mathcal{U}_n$

③ $x \in \mathcal{U}_n$ $\quad (x^{-1})^n = (x^n)^{-1} = 1$

donc $x^{-1} \in \mathcal{U}_n$

2) Mq U_n cyclique d'ordre n.

$$U_n = \{\exp(2i\pi k/n),\ k = 0, 1, \dots, n-1\}$$
$$= \{\exp(\underbrace{2i\pi/n}_{\omega})^k, \dots\}$$
$$= \{1, \omega, \omega^2, \dots, \omega^{n-1}\}$$

Donc $U_n = \langle \omega \rangle \subset \mathbb{C}^*$ et $\mathrm{ord}(\omega) = n$.

3) Mq $U_m \subseteq U_n$ ssi $m | n$

$\boxed{\Leftarrow}$ On suppose $m | n \iff \exists k$ tq $mk = n$

Soit $z \in U_m$

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

donc $z \in U_n$

On a bien $U_m \in U_n$

$\boxed{\Rightarrow}$ On suppose $U_m \subseteq U_n$ donc $m \leq n$

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

$z \in U_m \subseteq U_n$ avec $\mathrm{ord}(z) = m$ (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 $\mathrm{ord}(z)$ divise r (si $r > 0$)

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

$\Rightarrow r = 0$

$\Rightarrow m | n$

Exercice 8

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

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

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

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

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

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

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

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

$= \{ \bar{1}, \bar{5}, \bar{7}, \bar{11} \}$

↳ groupe d'ordre 4

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

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

$ord(\bar{7}) = 2$ car $7^2 = 49 \equiv 1 \mod 12$

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

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

↳ pour la multiplication

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

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

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

30.03.2021

Exercice 9

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

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

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

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

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

donc $ord(x^{-1}) = m$ 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 $(xy)^{m \times n} = x^{mn} \times y^{mn} = (x^n)^m \times (y^m)^n = e^m \times e^n = e$ 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 $1 = e^{2i\pi . 0}$, $0 \in \mathbb{Q}$

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 ($\text{ord}(x) \leq q$)

- 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

$\mathcal{M}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, (a, b, c, d) \in \mathbb{Z}^4 \right\}$

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

$SL_2(\mathbb{Z}) \subset \underbrace{GL_2(\mathbb{R})}_{\text{c'est un groupe}} = \{ A \in \mathcal{M}_2(\mathbb{R}) \text{ tq } \det A \neq 0 \}$

0) Mq $(GL_2(\mathbb{R}), \times)$ 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) $A \in SL_2(\mathbb{R})$, $A' \in SL_2(\mathbb{Z})$

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

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

et $AA' = \begin{pmatrix} aa' + bc' & ab' + bd' \\ a'c + c'd & b'c + dd' \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z})$

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

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

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

• $\Big\{ \underbrace{\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}, k \in \mathbb{Z}}_{\text{infini}} \Big\} \subset SL_2(\mathbb{Z})$ donc $SL_2(\mathbb{Z})$ infini.

• $SL_2(\mathbb{Z})$ non abélien car

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

$\neq$

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

$A^2 = \dots$

$A^3 = \dots$

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

$B^2 = \dots$

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

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

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

Exercice 14

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

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

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

rattraper la suite

01/04/2021

Suite de l'exo

Calculer $\text{ord}(\bar{2})$ dans $\left(\left(\mathbb{Z}/13\mathbb{Z}\right)^*, \times\right)$ 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 $\left(\left(\mathbb{Z}/13\mathbb{Z}\right)^*, \times\right)$?

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

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) $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, +)$?

<u>Rappel</u>: G est un groupe cyclique si $\exists x \in G$ tq $\langle x \rangle = G$

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

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

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

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

$$\left.\begin{aligned} \left(\left(\mathbb{Z}/13\mathbb{Z}\right)^*, \cdot\right) &\to (\mathbb{Z}/12\mathbb{Z}, +) \\ \bar{2} &\mapsto \bar{1} \end{aligned}\right\} \text{On def un morphisme}$$

06. 04. 2021

Exercice 13

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

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

Mq $ord(xy) = ab$

$$(xy)^{ab} = x^{ab} y^{ab} \quad \text{car } x \text{ et } y \text{ commutent}$$
$$= (x^a)^b (y^b)^a$$
$$= e^b e^a = e$$

Donc l'ordre de xy divise ab.

Soit $k = ord(a, b)$

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

or $b = ord(y)$ donc b divise ak

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

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

Donc $a | k$ et $b | k$

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

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

Donc $k = ab = ord(xy)$

08.04.2021

Exercice 11

$|G| = 35$

① Si G est cyclique
Alors $G = \langle x \rangle$, $x^{35} = e$, $x \in G$

$y = x^5$, $z = x^7$ $\quad ord(y) = 7$, $ord(z) = 5$

② Si G n'est pas cyclique

a) On suppose par l'absurde que G n'a que des éléments d'ordre 5 (et donc aucun d'ordre 7)

Si $x \in G$, $ord(x) = 5$ alors $H_1 = \langle x \rangle = \{e, x, x^2, x^3, x^4\}$ $\quad ord(x^2) = 5$ car $x^2 \in H_1 = \langle x \rangle$ et $|H| = 5$
$ord(x^3) = 5$ — x^3 ———

On a supposé que tous les éléments de G sont d'ordre 5.

Donc $\exists y \in G \setminus H_1$ tq $\text{ord}(y) = 5$

$$H_2 = \langle y \rangle = \{e, y, y^2, y^3, y^4\}$$

Alors $H_1 \cap H_2 = \{e\}$ donc $\text{card}(H_1 \cup H_2) = 9$ $\quad (H_1 \cup H_2 = \{e, x, x^2, x^3, x^4, y, y^2, y^3, y^4\})$

On voit que $\text{car}(G) = 4k+1$ (on pourrait refaire la même avec un $z \in G$, et en regardant $H_1 \cup H_2 \cup H_3$ ...)

CONTRADICTION car $35 \not\equiv 1 \, [4]$

b) De même comme $35 \not\equiv 1 \, [6]$, G ne peut pas contenir que des éléments d'ordre 7.

CONCLUSION de a) et b) $\quad |G| = 35$, G a au moins 1 elt d'ordre 5 et un elt d'ordre 7.