

## Exercice 1

## Correction "Série groupe et sous groupe"

1. Hyp.  $\exists n \in \mathbb{N}^* \text{ tel que } a^n = e.$

On pose.  $H = \{k \in \mathbb{N}^* \text{ tq } a^k = e\}$

$\begin{cases} n \in H \Rightarrow H \neq \emptyset \\ H \subset \mathbb{N} \end{cases}$

$\hookrightarrow$  H est non vide par 0  
Alors H admet un plus petit élément noté

$p \in H \Rightarrow a^p = e$

$p = \min H \Rightarrow a^k \neq e, \forall 1 \leq k \leq p-1$

2. Soit  $m \in \mathbb{Z}^* \text{ tq } a^m = e.$

On effectue la division euclidienne de m par p, alors  $\exists q, r \in \mathbb{Z} \text{ tq } \begin{cases} m = q \cdot p + r \\ 0 \leq r < p \end{cases}$

alors  $a^m = a^{p \cdot q + r} = (a^p)^q \cdot a^r = a^r$

$\Rightarrow a^r = e$  vrai seulement si  $r = p$

Puisque si  $r \neq 0 \Rightarrow r < p = \min H \text{ tq } a^r = e$

D'où  $m = qp \Leftrightarrow p = \frac{m}{q}$

La réciproque est facile.

3. Soit  $x \in G$  avec  $o(x) = n \in \mathbb{N}^*$   
Soit  $H = \{x^k; 0 \leq k \leq n-1\}$

Montrons que  $\langle x \rangle = H$

On a  $\langle x \rangle = \{x^k, k \in \mathbb{Z}\}$

Alors  $H \subset \langle x \rangle$  ①

reciproquement.

Soit  $y \in \langle x \rangle \Rightarrow \exists p \in \mathbb{Z} \text{ tq } y = x^p$

division euclidienne de p par n

$\Rightarrow p = kn + r \text{ tq } 0 \leq r \leq n-1$

$\Rightarrow y = x^{kn+r} = (x^n)^k \cdot x^r = x^r$   
 $0 \leq r \leq n-1$

$\Rightarrow y \in H$

$\Leftrightarrow \langle x \rangle \subset H$  ②

① ②

$\langle x \rangle = H = \{x^k; 0 \leq k \leq n-1\}$   
D'où  $\text{Card}(\langle x \rangle) = \text{Card}(H)$

Vérifions que les éléments de H sont e.a.e.f.

Supposons qu'il existe  $0 \leq k \leq n-1$  et  $0 \leq p \leq n-1$

tq  $x^k = x^p \Leftrightarrow x^{k-p} = e$

d'après 1/ m divise k-p { ce ci n'est possible que si  $k-p=0$

$\Rightarrow k=p$   
Ainsi si  $k \neq p$ , alors  $x^k \neq x^p$

d'où  $\text{Card}(H) = n \Rightarrow \boxed{\text{Card}(\langle x \rangle) = n = o(x)}$

3) Soit  $G$  un groupe monogène.

$$\Leftrightarrow \exists a \in G \text{ tq } G = \langle a \rangle = \{a^k; k \in \mathbb{Z}\}$$

(Mentions que  $G$  est abélien.

$$\text{Soit } x \in G \Leftrightarrow \exists k \in \mathbb{Z} \text{ tq } x = a^k$$

$$y \in G \Leftrightarrow \exists p \in \mathbb{Z} \text{ tq } y = a^p$$

$$xy = a^k \cdot a^p = a^{k+p} = a^{p+k} = a^p \cdot a^k = yx$$

D'où  $G$  est abélien.

$$4) \omega_n = \{z \in \mathbb{C} \text{ tq } z^n = 1\}$$

$$= \{z \in \mathbb{C} \text{ tq } z = e^{\frac{2ik\pi}{n}}, 0 \leq k \leq n-1\}$$

$$= \{z \in \mathbb{C} \text{ tq } z = \left(e^{\frac{2i\pi}{n}}\right)^k; 0 \leq k \leq n-1\}$$

$$= \langle e^{\frac{2i\pi}{n}} \rangle$$

$\omega_n$  est engendré par  $e^{\frac{2i\pi}{n}}$   
de plus  $\omega_n$  est fini.

$\omega_n$  est cyclique.

$$5) f: (G, \circ) \longrightarrow (G', *) \text{ morphisme de groupes}$$

$$\Leftrightarrow f(x \circ y) = f(x) * f(y)$$

i) Pour  $x = y = e_G$ , on a.

$$f(e_G \circ e_G) = f(e_G) * f(e_G)$$

$$f(e_G)$$

$$\Rightarrow f(e_G) * f(e_G)^{-1} = f(e_G)$$

$$\Rightarrow f(e_G) = e_{G'}$$

ii) Pour  $y = x^{-1}$

$$f(x \circ x^{-1}) = f(x) * f(x^{-1})$$

$$f(e_G) = f(x^{-1}) * f(x)$$

$$f(x)^{-1} = f(x^{-1})$$

iii) Soit  $H$  un s.g de  $G$ , mg  $f(H)$  s.g de  $G'$ .

$$\text{On a } f(H) \subseteq G' \Rightarrow f(e_G) \in f(H) \text{ de } G'$$

$$\text{Or } f(e_G) = e_{G'} \Rightarrow e_{G'} \in f(H) \quad \textcircled{1}$$

$$\bullet \text{ Soit } y_1 \in f(H) \Leftrightarrow \exists x_1 \in H \text{ tq } y_1 = f(x_1)$$

$$y_2 \in f(H) \Leftrightarrow \exists x_2 \in H \text{ tq } y_2 = f(x_2)$$

$$y_1 * y_2 = f(x_1) * f(x_2) = f(x_1 \circ x_2) \in f(H)$$

$$\Rightarrow y_1 * y_2 \in f(H) \quad \textcircled{2}$$

②

Soit  $y_1 \in f(H) \Leftrightarrow y_1 = f(x_1), x_1 \in H$   
 $\Rightarrow (y_1)^{-1} = (f(x_1))^{-1} = f(x_1^{-1})$   
 Comme  $H$  s.g, alors  $x_1^{-1} \in H$   
 $\Rightarrow y_1^{-1} \in f(H)$  ②

$x_1 \in H \Rightarrow y_1 \in f(H)$  s.g de  $G$

iv)  $f^{-1}(K) \subseteq G', K$  s.g de  $G'$ , mg  $f^{-1}(K)$  s.g de  $G$

On a  $f(e_G) = e_{G'} \in K$   
 d'où  $e_G \in f^{-1}(K)$  ①

Soit  $x_1 \in f^{-1}(K) \Leftrightarrow f(x_1) \in K$

$x_2 \in f^{-1}(K) \Leftrightarrow f(x_2) \in K$

$\Rightarrow f(x_1) * f(x_2) \in K$  ( $K$  s.g de  $G'$ )

$f(x_1 * x_2) \in K$

$\Leftrightarrow x_1 * x_2 \in f^{-1}(K)$  ③

Soit  $x \in f^{-1}(K) \Leftrightarrow f(x) \in K$

$\Rightarrow (f(x))^{-1} \in K$  ( $K$  s.g de  $G'$ )

$f(x^{-1}) \in K \Leftrightarrow x^{-1} \in f^{-1}(K)$  ④

Alors d'après ①, ③ et ④

$f^{-1}(K)$  s.g de  $G$

v)  $\ker f \subseteq G$

$f(e_G) = e_{G'} \Rightarrow e_G \in \ker f$

Soient  $x, y \in \ker f \Leftrightarrow f(x) = e_{G'}$   
 $f(y) = e_{G'}$

$f(xy^{-1}) = f(x) * f(y^{-1})$   
 $= f(x) * (f(y))^{-1} = e_{G'} * e_{G'}^{-1} = e_{G'}$

$\Rightarrow xy^{-1} \in \ker f$

Ainsi  $\ker f$  est un s.g de  $G$ .

vi)  $\text{Im } f$  est un s.g de  $G'$

On a  $f(e_G) = e_{G'} \Rightarrow e_{G'} \in \text{Im } f$

Soit  $y_1 \in \text{Im } f \Leftrightarrow \exists x_1 \in G \text{ tq } y_1 = f(x_1)$   
 $y_2 \in \text{Im } f \Leftrightarrow \exists x_2 \in G \text{ tq } y_2 = f(x_2)$

$y_1 * y_2^{-1} = f(x_1) * (f(x_2))^{-1}$   
 $= f(x_1) * f(x_2^{-1})$   
 $= f(x_1 * x_2^{-1}) \in \text{Im } f$

$\Rightarrow y_1 * y_2^{-1} \in \text{Im } f$

D'où  $\text{Im } f$  s.g de  $G'$

ou bien  
 on a  $\text{Im } f = f(G)$ . or  $G$  s.g de  $G$ , d'où  
 $f(G)$  s.g de  $G'$

③

3) Soit  $A \dots$

### Exercice 2

1)  $S_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid {}^t A = A\}$

- $S_n(\mathbb{R}) \subset M_n(\mathbb{R})$  ①
- $0 \in S_n(\mathbb{R})$  ②

• Soit  $A, B \in S_n(\mathbb{R})$

${}^t(A-B) = {}^t A - {}^t B = A-B$ , alors

$(A-B) \in S_n(\mathbb{R})$  ③

1+2+3  $S_n(\mathbb{R})$  s.g. de  $M_n(\mathbb{R})$ .

2)  $O_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid {}^t A \cdot A = I_n\}$

• Si  $A \in O_n(\mathbb{R})$ , alors  $A$  est inversible.  
et  $A^{-1} = {}^t A$ .

D'où  $O_n(\mathbb{R}) \subset GL_n(\mathbb{R})$

- $I_n \in O_n(\mathbb{R})$
- Soient  $A, B \in O_n(\mathbb{R}) \Leftrightarrow \begin{cases} {}^t A A = I_n \\ {}^t B B = I_n \end{cases}$

${}^t(A \cdot B) \cdot AB = {}^t B \cdot \underbrace{{}^t A A}_{I_n} \cdot B = {}^t B \cdot B = I_n$

$\Rightarrow AB \in O_n(\mathbb{R})$

• Soit  $A \in O_n(\mathbb{R})$ , mg  $A^{-1} \in O_n(\mathbb{R})$

${}^t(A^{-1})A^{-1} = ({}^t A)^{-1}A^{-1} = ({}^t A^{-1}) \cdot {}^t A$   
 $= {}^t(A \cdot A^{-1}) = {}^t I_n = I_n$

$\Rightarrow A^{-1} \in O_n(\mathbb{R})$

D'où  $O_n(\mathbb{R})$  s.g. de  $(GL_n(\mathbb{R}), \times)$

3)  $O_n^+(\mathbb{R}) = \{A \in O_n(\mathbb{R}) \mid \det A = 1\}$

- $O_n^+(\mathbb{R}) \subset O_n(\mathbb{R})$
- $I_n \in O_n^+(\mathbb{R})$
- Soient  $A, B \in O_n^+(\mathbb{R})$

$\Rightarrow A \cdot B^{-1} \in O_n(\mathbb{R})$  d'après 2)

et  $\det(A \cdot B^{-1}) = \det A \cdot \det B^{-1}$   
 $= \frac{\det A}{\det B} = 1$

$\Rightarrow A \cdot B^{-1} \in O_n^+(\mathbb{R})$

$\Leftrightarrow O_n^+(\mathbb{R})$  est un s.g. de  $O_n(\mathbb{R})$ .

4)  $O_n^-(\mathbb{R}) = \{A \in O_n(\mathbb{R}) \mid \det A = -1\}$

$\det I_n = 1 \Rightarrow I_n \notin O_n^-(\mathbb{R})$ .

Alors  $O_n^-(\mathbb{R})$  n'est pas un sous groupe de  $O_n(\mathbb{R})$

### Exercice 3

1)  $\pi_1(B(G), o)$  est un groupe.

• Soient  $f \in B(G)$  et  $g \in B(G)$ , alors

$f \circ g$  est une bijection de  $G$   
 $\Rightarrow$  "o" L.C.I dans  $B(G)$ .

• Soient  $f, g, h \in B(G)$   
 $(f \circ g) \circ h = f \circ (g \circ h)$

④

(11)

La loi "o" est associative.

$\text{Id}_A \circ f = f \circ \text{Id}_B = f \Rightarrow \text{Id}_A = \text{l'élément neutre de } B(G)$   
 $\Rightarrow \text{Id}_A$  est l'élément neutre de  $B(G)$

$f$  bijective  $\Leftrightarrow f^{-1}$  bijective

$$f \circ f^{-1} = f^{-1} \circ f = \text{Id}_G$$

Alors  $f$  est invertible dans  $B(G)$   
 $\subseteq B(G, o)$  est un groupe.

$$\exists f_a: G \rightarrow G$$

$$x \mapsto axa^{-1}$$

soient  $x, y \in G$

$$f_a(x \cdot y) = axya^{-1} = axa^{-1}aya^{-1}$$

$$= f_a(x) \cdot f_a(y)$$

Alors  $f_a$  est un morphisme du groupe  $G$ .

soit  $y \in G \exists ! x \in G$  tq  $y = axa^{-1}$

$$\Rightarrow \exists ! x = a^{-1}ya$$

alors  $f_a$  est bijective et  $(f_a)^{-1} = f_{a^{-1}}$ .

Ainsi  $f$  est un automorphisme du groupe  $G$ .

$$\exists G' = \{f_a; a \in G\}$$

$\forall a \in G, f_a$  est bijective, d'où

$$\bullet G' \subseteq B(G) \quad \textcircled{1}$$

$$\bullet \text{Id}_G = f_e \Rightarrow \text{Id}_G \in G' \quad \textcircled{2}$$

$$\bullet \text{Si } f_a \in G' \Rightarrow (f_a)^{-1} = f_{a^{-1}} \in G' \quad \textcircled{3}$$

soient  $f_a, f_b \in G'$

$$f_a \circ f_b(x) = f_a(bxb^{-1}) = abxb^{-1}a^{-1}$$

$$= abx(ab)^{-1}$$

$$= f_{ab}(x)$$

$$\Leftrightarrow f_a \circ f_b = f_{ab}$$

$$\text{d'où } f_a \circ f_b \in G'$$

$\textcircled{1}, \textcircled{2}, \textcircled{3}$  et  $(G, o)$  sous groupe de  $B(G)$

$$\textcircled{4} \quad \varphi: (G, o) \rightarrow (G', o)$$

$$a \mapsto f_a$$

soient  $a, b \in G$

$$\varphi(a \cdot b) = f_{a \cdot b} = f_a \circ f_b = \varphi(a) \circ \varphi(b)$$

$\Rightarrow \varphi$  morphisme de groupes.

$$\textcircled{5} \quad x \in G.$$

$$C_x = \{y \in G \text{ tq } xy = yx\}$$

$$\text{a) } C_x \subseteq G.$$

$$e \cdot x = x \cdot e = x \Rightarrow e \in C_x$$

$$\text{soit } y \in C_x \text{ et } z \in C_x \Leftrightarrow xy = yx \text{ et } xz = zx$$

$$\Rightarrow x(yz) = yxz = yzx$$

$$\Rightarrow yz \in C_x$$

$$\bullet \text{soit } y \in C_x \Leftrightarrow xy = yx$$

$$\Leftrightarrow y^{-1}xy = x$$

$$\Leftrightarrow y^{-1}x = xy^{-1}$$

$$\textcircled{6} \Rightarrow y^{-1} \in C_x$$

Ce ci montre que  $C_x$  est un sous groupe de  $G$ .

$$b) \text{Ker } \varphi = \{ a \in G \mid \varphi(a) = \text{Id}_{G'} \} =: \text{Id}_G$$

$$\begin{aligned} \varphi(a) = \text{Id}_G &\Leftrightarrow f_a = \text{Id}_G \\ &\Leftrightarrow f_a(x) = x, \forall x \in G \\ &\Leftrightarrow ax = xa, \forall x \in G \\ &\Leftrightarrow a \in C_x, \forall x \in G \\ &\Leftrightarrow a \in \bigcap_{x \in G} C_x \end{aligned}$$

$$\text{D'où } \text{Ker } \varphi = \bigcap_{x \in G} C_x$$

On en déduit que  $\varphi$  est injective.ssi

$$\text{Ker } \varphi = \{ e \} \Leftrightarrow \bigcap_{x \in G} C_x = \{ e \}$$

c) soit  $h \in G'$ , alors  $\exists a \in G$  tq.

$$h = f_a = \varphi(a)$$

D'où  $\varphi$  est surjective.

#### Exercice 4

Card  $G = n$ . tq  $G = \langle a \rangle$ ,  $n \in \mathbb{N}^*$ .

$$\begin{aligned} f: G &\longrightarrow G \\ x &\longmapsto x^n \end{aligned}$$

$$\begin{aligned} f(xy) &= (xy)^n = x^n \cdot y^n \quad \left( \begin{array}{l} \text{car } G \\ \text{cyclique} \\ \text{Alors commutatif} \end{array} \right) \\ &= f(x) \cdot f(y) \end{aligned}$$

Alors  $f$  est un morphisme de groupes.

$$d) \text{ soit } x \in \text{Ker } f \Leftrightarrow f(x) = e$$

$$\Leftrightarrow \begin{cases} x^r = e \\ \exists k \text{ tq } x \in G \end{cases}$$

Comme  $G = \langle a \rangle$ , alors  $\exists k \in \mathbb{N}$  tq

$$x = a^k$$

D'où

$$a^{kr} = e$$

Puisque Card  $G = n$ , alors  $n \mid kr$ .

$$\begin{aligned} d = \text{pgcd}(n, r) &\Leftrightarrow n = dn' \\ r &= dr' \text{ avec } \text{pgcd}(n', r') = 1 \end{aligned}$$

$$n \mid kr \Leftrightarrow dn' \mid dk \cdot r'$$

$$\Rightarrow n' \mid kr'$$

Comme  $\text{pgcd}(n', r') = 1$ , alors d'après Gauss

$$n' \mid k \Leftrightarrow k = k' \cdot n' \Rightarrow x = a^{k' \cdot n'}$$

$$\Rightarrow x \in \langle a^{n'} \rangle.$$

reciproquement. si  $x \in \langle a^{n'} \rangle \Leftrightarrow x = a^{n' \cdot k'}$

$$\Rightarrow x^d = a^{dn'k'} = a^{n'k'} = e$$

$$\Rightarrow x^{dr'} = e \Leftrightarrow x^r = e \Rightarrow x \in \text{Ker } f.$$

$$\text{Ainsi } \text{Ker } f = \langle a^{n'} \rangle.$$

$\text{Ker } f = \langle a^d \rangle$ .  
 Soit  $y \in \langle a^d \rangle \Rightarrow \exists k \in \mathbb{N} \text{ tq } y = a^{dk}$   
 puisque  $d = \text{pgcd}(n, r) \xrightarrow{\text{Bezout}}$   
 $\exists u, v \in \mathbb{N} \text{ tq } d = nu + rv$   
 $\Rightarrow y = a^{(nu+rv)k} = a^{nuk} a^{rvk}$   
 $= (a^{rk})^n = x^n$  avec  $x = a^{rk}$

D'où  $y \in \text{Im } f \Rightarrow \langle a^d \rangle \subset \text{Im } f$ .

"⊃" Soit  $y \in \text{Im } f \Leftrightarrow \exists x \in G \text{ tq } y = x^n$   
 $y = x^n = x^{d \cdot r'} = a^{k \cdot dr'}$  avec  $x = a^k$   
 $= (a^d)^{kr'} \Rightarrow y \in \langle a^d \rangle$

Ainsi  $\text{Im } f = \langle a^d \rangle$ .

3) Soit  $y \in G$ .  
 1<sup>er</sup> cas si  $y \notin \text{Im } f \Rightarrow \nexists x \in G \text{ tq } y = x^n$

$\Rightarrow$  l'éq n'admet pas de solutions.

2<sup>e</sup> cas si  $y \in \text{Im } f$ , alors  $\exists x_0 \in G \text{ tq } y = x_0^n$ .

cherchons  $x$  tq  $y = x^n$   
 $\Rightarrow x_0^n = x^n \Leftrightarrow x_0^n (x^{-1})^n = e$

$\Leftrightarrow (x_0 x^{-1})^n = e \Leftrightarrow x_0 x^{-1} \in \text{Ker } f = \langle a^d \rangle$

comme  $\text{card}(\langle a^{n/d} \rangle) = d$  (car  $(a^{n/d})^d = e$ )  
 alors il y a d solutions.

## Exercice 5

$(G, \cdot)$  groupe fini: card  $G = n \in \mathbb{N}^*$

1) a)  $x, y \in G$ ;  $x R y \Leftrightarrow xy^{-1} \in H$

$\forall x \in G$ ;  $x \cdot x^{-1} = e \in H \Leftrightarrow x R x$

"R" est réflexive ①

soient  $x, y \in G$  tq  $x R y \Leftrightarrow$

$xy^{-1} \in H \Rightarrow (xy^{-1})^{-1} \in H$  ( $H$  s.g.)

$\Rightarrow yx^{-1} \in H$

$\Rightarrow y R x$ .

$\Rightarrow$  "R" est symétrique ②

soient  $x, y$  et  $z \in G$  tq

$x R y \Leftrightarrow xy^{-1} \in H$

$y R z \Leftrightarrow yz^{-1} \in H$

$\Rightarrow xy^{-1} \cdot yz^{-1} \in H$  ( $H$  s.g.)

$\Rightarrow xz^{-1} \in H \Leftrightarrow x R z$

D'où "R" est transitive ③

① + ② + ③  $\Rightarrow$  R est une relation d'équivalence

b)  $a \in G$   
 $\mathcal{C}_R(a) = \{x \in G \text{ tq } x R a\}$   
 $= \{x \in G \text{ tq } xa^{-1} \in H\}$

$xa^{-1} \in H \Leftrightarrow xa^{-1} = h \in H$

$\Leftrightarrow x = ha \in Ha$

D'où  $cl_R(a) = H \cdot a$

2) soit  $f: H \rightarrow cl_R(a)$   
 $x \mapsto x \cdot a$

soit  $y \in cl_R(a) = H \cdot a \Rightarrow \exists x \in H$  tq  
 $y = x \cdot a \leftarrow f_a(x)$

D'où  $f_a$  est surjective.

soit  $x, x' \in H$  tq  $f_a(x) = f_a(x')$

$\Leftrightarrow x \cdot a = x' \cdot a$

$\Leftrightarrow x \cdot a \cdot a^{-1} = x' \cdot a \cdot a^{-1}$

$\Leftrightarrow x = x' \Rightarrow f_a$  est injective

Alors  $f_a$  est bijective.

3) Puisque  $f_a$  est bijective, alors

$\text{Card}(H) = \text{Card}(cl_R(a))$

D'autre part on a l'ensemble des classes d'équivalence forment une partition de  $G$

$\Leftrightarrow G = \bigcup_{a \in G} cl_R(a)$  (union disjointe)

Alors  $\text{Card } G = \sum_{a \in G} \text{Card}(cl_R(a))$

$\Rightarrow \text{Card } G = p \cdot \text{Card } H$

D'où  $\text{Card } H \mid \text{Card } G$  (avec  $p = \text{nombre des classes d'équiv}$ )

4)  $(G, \cdot)$  groupe fini

$\text{Card}(G) = n$

soit  $a \in G$ , alors  $\exists k \in \mathbb{N}^* \text{ tq } a^k = e$

Cor. 11.10

$\forall k \in \mathbb{N}^*, a^k \neq e \Rightarrow a^k \neq a^{k'} \forall k, k' \in \mathbb{N}^*$

$\Rightarrow \{a^k, k \in \mathbb{N}^*\} = \text{un fini} \subset G$ . abstra  
Cor. 11.11

$\Rightarrow \exists k \in \mathbb{N}^* \text{ tq } a^k = e$

on pose  $p = \inf \{k \in \mathbb{N}^*; a^k = e\}$

$\Rightarrow a^p = e$  et on pose  $p = o(a)$

$\langle a \rangle = \{a^k; 0 \leq k \leq p-1\}$

$\Rightarrow \text{Card } H = p$  divise  $n$  (d'après 3)

$\Rightarrow$  l'ordre de  $a$  divise  $n$ .

on a aussi  $a^n = a^{k \cdot p} = (a^p)^k = e \Rightarrow \underline{a^n = e}$

5)  $n = \text{Card } G$

$n = ep + 1 \mid m \in \mathbb{N} \Rightarrow ep = mk$

a)  $f: G \rightarrow G$

$x \mapsto x^m$

soient  $x, y \in G$  tq  $f(x) = f(y) \Leftrightarrow$

$x^m = y^m \Rightarrow x^{mk} = y^{mk}$

$\Rightarrow x^{ep} = y^{ep} \Rightarrow x^{n-1} = y^{n-1}$

Comme  $x^n = e$  et  $y^n = e$ , alors  $x^{-1} = y^{-1}$

$\Rightarrow x = y$

$\Rightarrow f$  est injective.

soit  $y \in G \exists! x \in G$  tq  $f(x) = y$

$$f(x) = y \Leftrightarrow x^m = y$$

$$\Leftrightarrow x^{mk} = y^k$$

$$\Leftrightarrow x^p = y^k \Leftrightarrow x^{n-1} = y^k$$

$$\Leftrightarrow x^{-1} = y^k$$

$$\Leftrightarrow x = y^{-k}$$

$$\Rightarrow \exists x = y^{-k} \text{ tq } f(x) = y$$

D'où  $f$  est surjective.

$\underline{cl}$   $f$  est bijective.

b) On suppose que  $G$  est abélien.

On considère  $x, y \in G$ .

$$f(xy) = (xy)^m = x^m \cdot y^m \quad G \text{ commutatif}$$

$$= f(x) \cdot f(y)$$

$\Rightarrow f$  est un morphisme de groupes.  
Comme  $f$  est bijective, alors  $f$  est un automorphisme.

## Exercice 6

$$1) C(A) = \{x \in G \text{ tq } x \cdot a = ax, \forall a \in A\}$$

$$C(A) \subset A. \textcircled{1}$$

$$e \cdot a = a \cdot e = a, \forall a \in A \Rightarrow e \in C(A) \textcircled{2}$$

$$\bullet \text{ Soient } x, y \in C(A) \Leftrightarrow \begin{cases} xa = ax, \forall a \in A \\ ya = ay, \forall a \in A \end{cases}$$

alors  $\forall a \in A$

$$x \cdot ya = xay = axy$$

$$\Rightarrow xy \in C(A) \textcircled{3}$$

$$\bullet \text{ Soit } x \in C(A) \Leftrightarrow xa = ax, \forall a \in A$$

$$\Leftrightarrow x^{-1}xa = x^{-1}ax$$

$$\Leftrightarrow a = x^{-1}ax \Leftrightarrow ax^{-1} = x^{-1}a \cdot \underbrace{xx^{-1}}_e$$

$$\Rightarrow ax^{-1} = x^{-1}a \Rightarrow \underline{x^{-1} \in C(A)} \textcircled{4}$$

$$\xrightarrow{1+2+3+4} C(A) \text{ s.g. de } G.$$

$$\bullet N(A) = \{x \in G \text{ tq } xA = Ax\}$$

$$N(A) \subset A$$

$$\bullet e \cdot A = A \cdot e \Leftrightarrow e \in N(A)$$

$$\bullet \forall x, y \in N(A)$$

$$xyA = x \cdot Ay = Ax \cdot y$$

$$\Rightarrow xy \in N(A)$$

$$\bullet \text{ Soit } x \in N(A) \Leftrightarrow xA = Ax$$

$$\Rightarrow x^{-1}xA = x^{-1}Ax$$

$$\Leftrightarrow Ax^{-1} = x^{-1}A$$

D'où  $x^{-1} \in N(A)$

Ainsi  $N(A)$  est un sous-groupe de  $G$

2)  $\Pi q$   $A$  est un sous-groupe distingué de  $G$ .

On a  $A$  est distingué dans  $G \Leftrightarrow$

$$\forall h \in A, \forall x \in G, xhx^{-1} \in A$$

$$\Leftrightarrow xh \in Ax, \forall h \in A$$

$$\Leftrightarrow xA = Ax, \forall x \in G \Leftrightarrow x \in N(A)$$

$$\Leftrightarrow N(A) = G$$

3)  $\varphi: G \rightarrow G'$  morphisme de groupes

Soit  $h \in \ker \varphi$ , mg  $\forall x \in G$

$$xhx^{-1} \in \ker \varphi.$$

$$\begin{aligned} \varphi(xhx^{-1}) &= \varphi(x) \cdot \varphi(h) \cdot \varphi(x^{-1}) \\ &= \varphi(x) \cdot e_{G'} \cdot \varphi(x)^{-1} = e_{G'} \end{aligned}$$

Alors  $xhx^{-1} \in \ker \varphi, \forall x \in G$ .

$\Leftrightarrow \ker \varphi$  est un sous-groupe distingué de  $G$

$$4) HK = \{x.y; x \in H \text{ et } y \in K\}$$

On a  $e_G \in H$  et  $e_G \in K \Rightarrow$

$$e_G = e_G \cdot e_G \in H.K$$

Soient  $x \in H.K$  et  $y \in H.K$   
 $\Rightarrow \exists h, h' \in H, \exists k, k' \in K$   
 $x = h.k$  et  $y = h'.k'$

$$\begin{aligned} x.y^{-1} &= h.k.(h'.k')^{-1} \\ &= h.k.k'^{-1}.h'^{-1} \\ &= h.k.k'^{-1}.h'^{-1}.(k.k'^{-1})^{-1}.k.k'^{-1} \\ &\quad \underbrace{h.k.k'^{-1}.h'^{-1}}_{\in H} \cdot \underbrace{(k.k'^{-1})^{-1}.k.k'^{-1}}_{\in K} \end{aligned}$$

$$\Rightarrow h.(k.k'^{-1}.h'^{-1}.(k.k'^{-1})^{-1}) \in H.K$$

Ainsi  $xy^{-1} \in HK \Leftrightarrow HK$  s.g. de  $G$ .

## exercice 7

$\downarrow$   $G$  est un groupe cyclique.  $\Leftrightarrow$   
 $\exists a \in G$  tq  $\langle a \rangle = G$ .  
 $|G| = n = o(a)$ .

Soit  $H$  un s.g. de  $G$ .  
 on suppose que  $H \neq \{e\} \Leftrightarrow \exists y \in H, y \neq e$

$\Rightarrow \exists n_0 \in \mathbb{Z}^*$  tq  $y = a^{n_0}$   
 on pose  $I = \{k \in \mathbb{N}^* \text{ tq } a^k \in H\}$   
 $n_0 \in I \Rightarrow I \neq \emptyset$   
 et  $I \subset \mathbb{N}^*$   $\Rightarrow I$  admet un min.

on pose  $p = \min I \Rightarrow p \in I \Rightarrow a^p \in H$ .  
 $\Rightarrow \langle a^p \rangle \subset H$

reciproquement: soit  $x \in H \subset G$ .

$\Rightarrow \exists q \in \mathbb{Z}$  tq  $x = a^q$ .

on effectue la division euclidienne de  $q$  par  $p \Leftrightarrow \exists q' \in \mathbb{Z} \exists 0 \leq r \leq p-1$   
 tq  $q = pq' + r$

$$x = a^q = a^{pq' + r} = a^{pq'} \cdot a^r$$

$$\Rightarrow a^r = x \cdot a^{-pq'} = x \cdot (a^p)^{-q'}$$

$\in$

$$x \in H \text{ et } a^p \in H \Rightarrow (a^p)^{-q'} \in H$$

$$\Rightarrow x \cdot a^{-pq'} \in H \quad (H \cdot s.g.)$$

$$\Rightarrow a^r \in H.$$

Comme  $0 \leq r \leq p-1$  et  $p = \min I$

Alors ce ci n'est possible que si

$$r = 0$$

Ainsi  $x = (a^p)^{q'} \in \langle a^p \rangle$

$$\Leftrightarrow H \subset \langle a^p \rangle.$$

$$\underline{\underline{\subset}} \quad [H = \langle a^p \rangle]$$

$\Rightarrow$  Soit  $d$  un diviseur de  $|G| = n$

$$\Leftrightarrow \exists n' \in \mathbb{N} \text{ tq } n = dn'$$

$$\Leftrightarrow \frac{n}{d} \in \mathbb{N}.$$

Existence

on pose  $b = a^{\frac{n}{d}}$ .

Alors  $o(b) = d$ .

En effet

on a  $b^d = a^n = e \Rightarrow \underline{o(b) \mid d}$  ①

D'autre part on a  $b^{o(b)} = e$

$$\Leftrightarrow a^{\frac{n}{d} \cdot o(b)} = e \Rightarrow n \mid \frac{n}{d} \cdot o(b)$$

$$\Rightarrow \frac{o(b)}{d} \in \mathbb{N} \Rightarrow \underline{d \mid o(b)} \quad \textcircled{2}$$

①  $1 \leq d$   $[o(d) = d]$

On pose  $H = \langle a^{\frac{n}{d}} \rangle = \langle b \rangle$   
 $\Rightarrow H$  cyclique et  $|H| = o(b) = d$   
 ce qui montre l'existence

• Unicité :

soit  $H'$  un s.g de  $G$  tq  $|H'| = d$   
 On a déjà posé  $H = \langle a^{\frac{n}{d}} \rangle$ .

$$\Rightarrow x = a^p$$

$$= (a^{\frac{n}{d}})^k \in \langle a^{\frac{n}{d}} \rangle$$

$$\Rightarrow H' \subseteq \langle a^{\frac{n}{d}} \rangle = H$$

$$\text{Comme } \text{card } H' = \text{card } H = d$$

$$\Rightarrow H' = H$$

ce qui montre l'unicité.

$$\text{Soit } x \in H' \Rightarrow x \in G \Leftrightarrow \exists p \in \mathbb{Z}$$

$$\text{tq. } x = a^p.$$

$$\text{Or } |H'| = d \Rightarrow x^d = e \Leftrightarrow a^{p \cdot d} = e$$

$$\Rightarrow n \mid p \cdot d \Leftrightarrow p \cdot d = m \cdot n$$

$$\text{Or } d \mid n \Rightarrow n = n' \cdot d \Rightarrow p = k \cdot n'$$

$$\Leftrightarrow p = \frac{n}{d} \cdot k$$