Exo 14 planche TD2

1 la table de $\mathbb{Z}_{10}^*$

$$\mathbb{Z}_{10}^* = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}$$

$\cdot$	$[1]$	$[3]$	$[7]$	$[9]$
$[1]$	$[1]$	$[3]$	$[7]$	$[9]$
$[3]$	$[3]$	$[9]$	$[1]$	$[7]$
$[7]$	$[7]$	$[1]$	$[9]$	$[3]$
$[9]$	$[9]$	$[7]$	$[3]$	$[1]$

2. M.Q. $\mathbb{Z}_{10}^*$ est un groupe cyclique

$$\langle [3]_{10} \rangle = \{[1], [3], [9], [7]\} = \mathbb{Z}_{10}^*$$

donc $\mathbb{Z}_{10}^*$ est cyclique engendré par $[3]$

Rappel Soit $x \in G$ d'ordre fini, soit $n = ord(x)$

Alors $\langle x \rangle = \{e, x \dots x^{n-1}\}$

Preuser un isomorphisme $(\mathbb{Z}_4, +) \longrightarrow (\mathbb{Z}_{10}^*, \cdot)$

Rappel Soit $x \in G$ d'ordre fini n. Alors la formule

$g_x([k]_n) = x^k$ définit un isomorphisme

$g_x : (\mathbb{Z}_n, +) \longrightarrow \langle x \rangle$

Dans notre cas $x = [3]_{10}$

On obtient un isomorphisme

$\varphi = g_{[3]}$ $\quad \varphi : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_{10}^{\times}$, $\quad \varphi([k]_4) = [3]_{10}^{k} = [3^k]_{10}$

Est-ce que $\mathbb{Z}_{30}^{\times}$ est un groupe cyclique ?

$\mathbb{Z}_{30}^{\times} = \{[1], [7], [11], [13], [17], [19], [23], [29]\}$

$\mathrm{ord}(\mathbb{Z}_{30}^{*}) = 8$

Par calcul direct on obtient :

$\forall \xi \in \mathbb{Z}_{30}^{\times}$, $\mathrm{ord}(\xi) \in \{1, 2, 4\}$, donc aucun élément de $\mathbb{Z}_{30}^{\times}$ n'est générateur de ce groupe.

$\mathbb{Z}_{30}^{\times}$ n'est pas cyclique.

Exo 13 Soit $(G, \cdot)$ un groupe, e son élément neutre

Supposons $x^2 = e$ pour tout $x \in G$ (i.e. $\forall x \in G,\ x' = x$)

1. M.q $(G, \cdot)$ est abélien

Soient $x, y \in G$

$$xy = (xy)' = y'x' = yx$$

règles de calcul dans un groupe

Autre démonstration :

$$(xy)^2 = e$$

x / $xyxy = e$ \ y

$$\underbrace{x(x}_{x^2}\, y x \,\underbrace{y)}_{y^2} y = xy$$

2.

Soit $H \subset G$ sous-groupe

$H \neq G$ et soit $a \in G \setminus H$

(a) M.q. $H \cap aH = \phi$

$$aH := \{ax \mid x \in H\}$$

Soit $x \in H \cap aH$

$\Updownarrow$

$x \in H$ et $x \in aH$

$\Downarrow$

$\exists x \in H,\ x = ax$

Donc $\exists x \in H$, $a = x x'$
$x \in H$
$x \in H$
$\Rightarrow a \in H$ (contradiction)

Conclusion : l'existence d'un élément $x \in H \cap aH$ nous donne une contradiction

(6) M.q. $H \cup aH$ est un sous-groupe de G et ce sous-groupe est isomorphe à $H \times \mathbb{Z}_2$, en particulier (si H est fini) $|H \cup aH| = 2|H|$

M.q. $H \cup aH$ est un sous-groupe de G :

1. Mq $e \in H \cup aH$. évident car $e \in H$.

2. Mq pour tous $x, y \in H \cup aH$, on a $x.y = H \cup aH$.

i) Soit $x \in H$, $y \in H$. On a $xy \in H \subset H \cup aH$.

Donc $xy \in H \cup aH$.

ii) Soit $x \in H$, $y \in aH$.

$\Downarrow$

$\exists h \in H$ tq $y = ah$.

On obtient $xy = xah = a\underbrace{xh}_{\in H} \in aH \subset H \cup aH$.

Donc $xy \in H \cup aH$.

iii) Soit $x \in aH$, $y \in H$. On a $xy = yx$ (d'après 1),
et $yx \in H \cup aH$ (d'après ii).

iv) Soient $x, y \in aH$. Alors $\exists h_1 \in H$ tq $x = ah_1$

$\exists h_2 \in H$ tq $y = ah_2$

On a $xy = ah_1 a h_2 \overset{(1)}{=} a^2 h_1 h_2 = h_1 h_2 \in H \subset H \cup aH$.

$$a^2 = e$$

Donc $xy \in H \cup aH$.

3. Mq $x \in H \cup aH \Rightarrow x^{-1} \in H \cup aH$.

Mais $x = x^{-1}$ donc évident.

À définir : un isomorphisme de groupes

$$f : H \times \mathbb{Z}_2 \longrightarrow H \cup aH.$$

On définit f par : $\begin{cases} f(h, [0]_2) = h \\ f(h, [1]_2) = ah \end{cases}$, $\forall h \in H$.

Pour justifier que f est bijective, on utilise $g : H \cup aH \to H \times \mathbb{Z}_2$ par :

$$\begin{cases} g(h) = (h, \overline{0}) \\ g(ah) = (h, \overline{1}) \end{cases}$$

On vérifie facilement que $g \circ f = Id_{H \times \mathbb{Z}_2}$, $f \circ g = I_{H \cup aH}$.

Par exemple pour vérifier que $g \circ f = Id_{H \times \mathbb{Z}_2}$:

Soit $\xi \in H \times \mathbb{Z}_2$, $\xi = (h, \overline{0})$ ou $\xi = (h, \overline{1})$, avec $h \in H$.

Dans le premier cas on calcule $g \circ f(\xi) = g(f(h, \overline{0})) = g(h) = (h, \overline{0}) = \xi$.

$$\begin{cases} g \circ f = Id_{H \times \mathbb{Z}_2} \\ f \circ g = Id_{H \cup aH} \end{cases} \Rightarrow \begin{cases} f \text{ est bijective.} \\ f^{-1} = g. \end{cases}$$

Mq f est un morphisme de groupes;

i.e $f((h,\alpha)*(x,\beta)) = f(h,\alpha)\cdot f(x,\beta)$, $\forall h,x \in H$, $\forall \alpha,\beta \in \mathbb{Z}_2$

i) $\alpha = \beta = [0]_2$.

$$f((h,[0]_2)*(x,[0]_2)) = f(\langle hx, \overbrace{[0]_2+[0]_2}^{[0]_2}\rangle) = hx.$$

$$f(h,[0]_2)\cdot f(x,[0]_2) = h\cdot x.$$

ii) $\alpha = [0]_2$, $\beta = [1]_2$.

$$f((h,[0]_2)*(x,[1]_2)) = f((hx, \overbrace{[0]_2+[1]_2}^{[1]_2})) = ahx.$$

$$f(h,[0]_2)\cdot f(x,[1]_2) = h\,a\,x = a\,h\,x.$$

iii) $\alpha = [1]_2$, $\beta = [0]_2$, iv) $\alpha = \beta = [1]_2$. (Calculs similaires)

3 Supposons de G est fini

À montrer : $\exists k \in \mathbb{N}$, t.q $G \simeq \mathbb{Z}_2^k$

↑ le produit itéré (k fois) du groupe $(\mathbb{Z}_2, +)$

On va démontrer la propriété demandée par récurrence par rapport à $n = \#G$

Initialisation : $n = 1$ évident $G = \{e\}$

$\mathbb{Z}_2^0$ un groupe trivial

donc on a bien un isomorphisme $G \simeq \mathbb{Z}_2^0$

$n = 2$ D'après le 3ème corolaire au thm. de Lagrange, G est un groupe cyclique d'ordre 2 donc isomorphe à $\mathbb{Z}_2 = \mathbb{Z}_2^1$

Hérédité : l'hypothèse de récurrence

On va démontrer que, si l'affirmation à démontrer est vraie pour tout $k < n$, alors elle sera vraie pour n.

On suppose $n > 1$. Soit m l'ordre maximal d'un sous-groupe $H \subset G$ de G.
$H \neq G$

$$m = \max \{ k \in \mathbb{N}^* \mid \exists H \subsetneq G \text{ sous-groupe}, k = |H| \}$$

$\checkmark$ sous-ensemble non-vide et majoré de $\mathbb{N}$

Soit $H \subsetneq G$ sous-groupe de G t.q. $|H| = m$

$H \subsetneq G \Rightarrow \exists a \in G \setminus H$. Remarque $H \cup aH = G$

En effet, d'après (2) $H \cup aH$ est un sous-groupe de G et $|H \cup aH| = 2|H| = 2m > m$

Si, par l'absurde, $H \cup aH \subsetneq G$, alors G admettra un sous-groupe $H' = H \cup aH \subsetneq G$ d'ordre $2m > m$, ce qui contredit la définition de m.

Conclusion : On a bien $H \cup aH = G$

$|H| = m < n$. D'après l'hypothèse de récurrence, l'affirmation à démontrer est vraie pour H, donc $\exists \ell \in \mathbb{N}$, t.q $H \simeq \mathbb{Z}_2^{\ell}$

D'après 2b) $\underbrace{H \cup aH}_{\text{"}G} \simeq H \times \mathbb{Z}_2 \simeq \mathbb{Z}_2^{\ell} \times \mathbb{Z}_2 \simeq \mathbb{Z}_2^{\ell+1}$

$\simeq \mathbb{Z}_2^{k}$ où $k = \ell+1$

Exo 15 Soit $f : G \to \tilde{G}$ morphisme de groupes.

1 Soit $\tilde{H} \subset \tilde{G}$ sous-groupe. À démontrer $f^{-1}(\tilde{H})$ est un sous-groupe de G, qui est normal si $\tilde{H}$ est normal

$$f^{-1}(\tilde{H}) := \{x \in G \mid f(x) \in \tilde{H}\}$$

(1) Pq $e \in f^{-1}(\tilde{H})$

propriété de cours — $f(e) = \tilde{e} \in \tilde{H}$ car $\tilde{H}$ est un sous groupe.

donc $e \in f^{-1}(\tilde{H})$.

(2) Pq : Si $x, y \in f^{-1}(\tilde{H})$ alors $xy \in f^{-1}(\tilde{H})$.

Soient $x, y \in f^{-1}(\tilde{H})$ i.e $f(x) \in \tilde{H}$ et $f(y) \in \tilde{H}$.

$f(xy) = f(x) f(y) \in \tilde{H}$ car $f(x), f(y) \in \tilde{H}$ et $\tilde{H}$ est un sous groupe.

(3) Soit $x \in f^{-1}(\tilde{H})$ Mq $x' \in f^{-1}(\tilde{H})$.

$f(x') = (f(x))'$

↑ propriété de cours.

$x \in f^{-1}(\tilde{H}) \iff f(x) \in \tilde{H} \Rightarrow (f(x))' \in \tilde{H}$

↑ Car $\tilde{H}$ un sous groupe.

donc $f(x') \in \tilde{H}$ donc $x' \in f^{-1}(\tilde{H})$.

Mq $f^{-1}(\tilde{H})$ est normal si $\tilde{H}$ est normal.

supposons $\tilde{H} \subset \tilde{G}$ est un sous groupe normal.

Mq $f^{-1}(\tilde{H})$ est normal.

Soit $x \in G$ et $h \in f^{-1}(\tilde{H})$. Mq $xhx' \in f^{-1}(\tilde{H})$.

$f(xhx') = f(x) f(h) f(x') = f(x) f(h) (f(x))' \in \tilde{H}$ car $f(h) \in \tilde{H}$ et $\tilde{H}$ est normal.

Donc $x h x' \in f^{-1}(\tilde{H})$.

2) Soit $H \subset G$ un sous-groupe. Mq $f(H)$ est un sous groupe de $\tilde{G}$.

$$f(H) = \{ y \in \tilde{G} \mid \exists\, x \in H,\ y = f(x) \} = \{ f(x) \mid x \in H \}$$

(1) Mq $\tilde{e} \in f(H)$.

$$\left.\begin{array}{l} \tilde{e} = f(e) \\ e \in H \end{array}\right\} \Rightarrow \tilde{e} \in f(H).$$

(2) Mq pour tous $y_1, y_2 \in f(H)$, $y_1 y_2 \in f(H)$.

$$\left.\begin{array}{l} y_1 \in f(H) \Rightarrow \exists\, x_1 \in H,\ y_1 = f(x_1) \\ y_2 \in f(H) \Rightarrow \exists\, x_2 \in H,\ y_2 = f(x_2) \end{array}\right\} \Rightarrow y_1 y_2 = f(x_1) f(x_2) = f(x_1 x_2)$$

Donc $\left.\begin{array}{l} y_1 y_2 = f(x_1 x_2) \\ x_1 x_2 \in H \end{array}\right\} \Rightarrow y_1 y_2 \in f(H)$.

($x_1, x_2 \in H$ et H est un sous-groupe)