I - Exercice 0

Soit $(G,)$ un groupe fini de cardinal n, et soit $x \in G$, on a le sous-groupe $H = \langle x \rangle$ est un sous-groupe de G.
D'après le théorème de Lagrange, on a $card(H)|card(G)$. En notant $d = o(x)$ l'ordre de x, on a $d = card(H)$, donc $d|n$. D'après le deuxième caractérisation de l'ordre, on a donc $x^n = e$.
Finalement, on a $\boxed{\forall x \in G, x^n = e}$

II - Exercice 1

II.A -

Soient $x \in G, y \in H$, on note $p = o(x)$, $q = o(y)$, $d = ppcm(p,q)$. On a donc $p|d$, $q|d$. Alors il existe $(m,n) \in \mathbb{Z}^2$ tel que $d = m * p = n * q$

- On a $\forall n \in \mathbb{N}, (x,y)^n = (x^n, y^n)$(on peut le montrer par récurrence sur n).
  On a donc $(x,y)^d = (x^d, y^d) = ((x^p)^m, (y^q)^n) = (e_G^m, e_H^n) = (e_G, e_H)$ l'élément neutre du groupe produit.
- Soit $k \in \mathbb{Z}$ tel que $(x,y)^k = (e_G, e_H)$, on a donc $(x^k, y^k) = (e_G, e_H)$.
  Alors $x^k = e_G$, $y^k = e_H$. D'après le deuxième caractérisation de l'ordre, on a donc $p|k$, $q|k$, donc $d|k$

D'après le deuxième caractérisation de l'ordre, on a donc $\boxed{d = ppcm(o(x), o(y)) = o(x,y)}$

II.B -

Soient $g \in G$ un générateur de G, $h \in H$ un générateur de H. On note $a = o(g)$, $b = o(h)$, les ordres respectivement de g et de h.

- sens indirect : Soit a et b sont premiers entre eux, soit $(m,n) \in G \times H$. alors il existe $M \in \mathbb{Z}$ tel que $m = g^M$, donc pour tout $x \in \mathbb{Z}$ tel que $[x]_a = [M]_a$, on a toujours $g^x = m$ car $g^a = e_G$.
  De même, il existe $N \in \mathbb{Z}$ tel que $n = h^N$, donc pour tout $y \in \mathbb{Z}$ tel que $[y]_b = [N]_b$, on a toujours $h^y = n$ car $h^b = e_H$.
  Puisque a et b sont premiers entre eux, par le théorème chinois, il existe $X \in \mathbb{Z}$ tel que $\psi([X]_{ab}) = ([X]_a, [X]_b) = ([M]_a, [N]_b)$ (car ψ est un isomorphisme).
  On a donc $(g,h)^X = (g^X, h^X) = (g^M, h^N) = (m,n)$. $G \times H$ est donc monogène. Car G et H sont finis, $G \times H$ aussi, et il est donc $\boxed{\text{cyclique}}$
- sens direct : On va le montrer par l'absurde
  Soit $d = pgcd(a,b) > 1$ et supposons que $G \times H$ est cyclique. Alors $\exists (a_1, b_1) \in \mathbb{Z}^2$, $a = a_1 d, b = b_1 d$, avec a_1, b_1 premiers entre eux. On suppose que $(g,h) \in G \times H$ est un générateur.
  Car $(e_G, h) \in G \times H$, alors il existe $X \in \mathbb{Z}$, tel que $(g,h)^X = (e_G, h)$. Donc $e_G = g^X, h = h^X$. Car G est $\mathbb{Z}/a\mathbb{Z}$ sont isomorphes(G est fini), alors $[X]_a = [0]_a$, c'est-à-dire il exists $m \in \mathbb{Z}$ tel que $X = ma$.
  De même, $[X]_b = [1]_b$, donc il existes $n \in \mathbb{Z}$ tel que $X = nb + 1$. On a donc $1 + nb = ma$, d'où $1 = ma - nb = d(ma_1 - nb_1) \in d\mathbb{Z}$. Mais c'est impossible car $d > 1$. C'est donc l'absurde.

Finalement, on a donc

$\boxed{G \times H \text{ est cyclique si et seulement si les entiers } card(G) \text{ et } card(H) \text{ sont premiers entre eux}}$

III - Exercice 2

III.A -

Car $d = pgcd(k, n)$, il existe $(k_1, n_1) \in \mathbb{Z}^2$, tel que $k = dk_1$, $n = dn_1$, avec k_1, n_1 premiers entre eux.
Pour $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$

- $\overline{k}^{n_1} = \overline{k}n_1 = \overline{kn_1} = \overline{\frac{kn}{d}} = \overline{nk_1} = \overline{0}$, l'élément neutre de $\mathbb{Z}/n\mathbb{Z}$
- Soit $x \in \mathbb{Z}$ tel que $\overline{k}^x = \overline{0}$, donc $\overline{0} = \overline{k}x = \overline{kx}$, donc $n|kx$. Alors $\exists m \in \mathbb{Z}, mn = kx$, c'est-à-dire $\exists m \in \mathbb{Z}, mn_1 = xk_1$, c'est-à-dire $n_1|xk_1$. Car k_1, n_1 sont premiers entre eux, par le théorème de Gauss, on a $n_1|x$

Finalement, on a $\boxed{o(\overline{k}) = n_1 = \frac{n}{d}}$

III.B -

- soit $x \in \langle\overline{k}\rangle$, alors il existe $a \in \mathbb{Z}$ tel que $x = \overline{k}^a$. Donc $x = \overline{ka} = \overline{dk_1a} = \overline{d}^{k_1a} \subset \langle\overline{d}\rangle$. Donc $\langle\overline{k}\rangle \subset \langle\overline{d}\rangle$
- soit $x \in \langle\overline{d}\rangle$, alors il existe $b \in \mathbb{Z}$ tel que $x = \overline{d}^b$. Car k_1, n_1 sont premiers entre eux, par le théorème de Bezout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $un_1 + vk_1 = 1$
  - analyse : Soit $x \in \langle\overline{k}\rangle$, alors il faut qu'il existe $c \in \mathbb{Z}$ tel que $x = \overline{db} = \overline{k}^c = \overline{kc}$, alors il existe $a \in \mathbb{Z}$ tel que $db+an = kc$, donc $b+an_1 = ck_1$. Donc $b(un_1+vk_1)+an_1 = ck_1$, on a alors $k_1|(bu + a)n_1$. On peut donc prendre $a = k_1 - bu \in \mathbb{Z}$
  - synthèse : on a $x = \overline{db} = \overline{db + (k_1 - bu)n} = \overline{db + (k_1 - bu)dn_1} = \overline{db + k_1dn_1 - bdun_1} = \overline{db + k_1dn_1 - bd(1 - vk_1)} = \overline{k_1d(n_1 + bv)} = \overline{k(n_1 + bv)} = \overline{k}^{n_1+bv} \subset \langle\overline{k}\rangle$
    On a donc $\langle\overline{d}\rangle \subset \langle\overline{k}\rangle$

Finalement, on en déduit $\boxed{\langle\overline{d}\rangle = \langle\overline{k}\rangle}$, ils donc engendrent le même sous-groupe de $\mathbb{Z}/n\mathbb{Z}$

III.C -

Par les résultat précédents, on considère l'ensemble $S = \bigcup_{e\in E}\{\langle\overline{e}\rangle\}$, avec $E = \{e|e \in [\![1, n]\!], e|n\}$, l'ensemble de diviseurs de n.

- pout tout sous ensemble $\langle\overline{k}\rangle$ avec $k \in [\![1, n]\!]$, on note $d = pgcd(k, n)$, on a $d|n$, donc $d \in E$. Par les résultat précédents, on a $\langle\overline{k}\rangle = \langle\overline{d}\rangle \in S$
  l'ensemble de sous groupes de $\mathbb{Z}/n\mathbb{Z}$ est donc inclus dans S
- pour tous $s \in S$, il exise $e \in E \in [\![1, n]\!]$, tel que $s = \langle\overline{e}\rangle$. s est bien un sous groupe de $\mathbb{Z}/n\mathbb{Z}$.
  S est donc inclus dans l'ensemble de sous groupes de $\mathbb{Z}/n\mathbb{Z}$

Finalement, l'ensemble de sous groupes de $\mathbb{Z}/n\mathbb{Z}$ est donnée par $\boxed{S = \bigcup_{e\in E}\{\langle\overline{e}\rangle\}}$