Groupe cyclique-Ordre d'un groupe/d'un élément

I. Sous-groupe engendré par un élément (groupe cyclique)

Théorème et définition (sous-groupe engendré par un élément)
Soit $(G,*)$ un groupe et $a \in G$.
L'ensemble noté $\langle a \rangle = \{a^n \ / \ n \in \mathbf{Z}\}$ est un sous-groupe de $(G,*)$.
$\langle a \rangle = \{a^n \ / \ n \in \mathbf{Z}\}$ s'appelle le groupe engendré par l'élément a.

Preuve. $e_G = a^0 \in \langle a \rangle$, reste à vérifier que $\forall x, y \in \langle a \rangle$ on a : $x * y^{-1} \in \langle a \rangle$
en utilisant les propriétés : $\forall (n,m) \in \mathbf{Z}^2$, $(a^m)^{-1} = a^{-m}$ et $a^n * a^m = a^{n+m}$

Remarque
Si $(G,+)$ est un groupe et $a \in G$ alors le groupe engendré par a est $\langle a \rangle = \{n\,a \ / \ n \in \mathbf{Z}\}$

Définition (groupe cyclique)
Un groupe $(G,*)$ est cyclique $\Leftrightarrow$ Il existe $a \in G$ tel que $G = \langle a \rangle = \{a^n \ / \ n \in \mathbf{Z}\}$
Dans ce cas on dit que $(G,*)$ est engendré par a ou on dit que a est un générateur du groupe $(G,*)$.

Remarque
Un groupe $(G,+)$ est cyclique $\Leftrightarrow$ Il existe $a \in G$ tel que $G = \langle a \rangle = \{n\,a \ / \ n \in \mathbf{Z}\}$

Exemples
1) Pour $n \in \mathbf{N}$, $(n\mathbf{Z},+)$ est un groupe cyclique engendré par n en particulier $(\mathbf{Z},+)$ est un groupe cyclique engendré par 1
2) Pour $n \in \mathbf{N}^*$, $(Z/nZ,+)$ est un groupe cyclique engendré par $\bar{1}$. On montrera dans le prochain cours que si $a \in \mathbf{N}^*$ et $p\gcd(a,n) = 1$ alors $\bar{a}$ est un générateur de $(Z/nZ,+)$.
3) Pour $n \in \mathbf{N}^*$, $(\Omega_n,.)$ est un groupe cyclique où Ω_n désigne l'ensemble des racines $n^{ième}$ de l'unité : $\Omega_n = \{z \in \mathbf{C} \ / \ z^n = 1\} = \left\{ e^{\frac{2ik\pi}{n}} \ / \ k \in \mathbf{Z} \right\} = \left\{ \left(e^{\frac{2i\pi}{n}} \right)^k \ / \ k \in \mathbf{Z} \right\} = \left\langle e^{\frac{2i\pi}{n}} \right\rangle$
et donc $(\Omega_n,.)$ est engendré par $e^{\frac{2i\pi}{n}}$

4) $(\mathbf{R},+)$ n'est pas un groupe cyclique (**à prouver**)

II. Ordre d'un groupe et théorème de Lagrange

Définition (ordre d'un groupe)
Soit $(G,*)$ un groupe
On appelle ordre de G et on note $ord(G)$, le cardinal de l'ensemble G.
Ainsi, $ord(G) = card(G) =$ le nombre d'éléments de G.

Exemples

1) Pour $n \in \mathbf{N}^*$, $ord(\Omega_n) = n$ où $\Omega_n) = \{z \in \mathbf{C} \ / \ z^n = 1\}$

2) Pour $n \in \mathbf{N}^*$, $ord(Z/nZ) = n$

3) le groupe $(\mathbf{Z},+)$ est d'ordre infini car $\mathbf{Z}$ est un ensemble infini

Théorème de Lagrange

Si $(G,*)$ est un groupe **fini** et H est un sous-groupe de $(G,*)$, alors $ord(H)$ divise $ord(G)$.

Preuve.

On définit une relation binaire R sur G par : pour $(x,y) \in G^2$, $xRy \Leftrightarrow (x * y^{-1}) \in H$

On vérifie que R est une relation d'équivalence sur G.

Pour $x \in G$, la classe d'équivalence de x est : $\bar{x} = \{y \in G / yRx\} = \{y \in G / y * x^{-1} \in H\}$

Donc, pour tout $y \in G$, $y \in \bar{x} \Leftrightarrow y * x^{-1} \in H \Leftrightarrow \exists h \in H,\ y = h * x$

Par conséquent, $\bar{x} = \{h * x / h \in H\}$ que l'on note H_x

Si $x \in G$, alors l'application $\begin{array}{rcl} f : H & \to & H_x \\ h & \mapsto & h * x \end{array}$ est bijective

Ainsi, pour tout $x \in G$ on a : $card(H_x) = card(H) = ord(H)$

Comme les classes d'équivalence modulo R forment une partition de G, il vient :

$$ord(G) = \sum_{\bar{x} \in (G/R)} card(H_x) = card(G/R).ord(H) \text{ où } G/R = \{\bar{x} / x \in G\}$$

Donc, $ord(H)$ divise $ord(G)$

III. Ordre d'un élément dans un groupe

Définition (ordre d'un élément d'un groupe)

Soient $(G,*)$ un groupe et $a \in G$.

On appelle ordre de a et on note $ord(a)$, l'ordre du sous–groupe engendré par a.

Ainsi, $ord(a) = ord(\langle a \rangle)$

Remarque : Si l'ordre de a est fini, alors $ord(a) \in IN^*$ car $\langle a \rangle$ est non vide

Théorème 1. Soient $(G,*)$ un groupe et $a \in G$

Si $ord(a) = d \in IN^*$ **est fini**, alors le sous-groupe engendré par a est :

$$\langle a \rangle = \{a^k / k \in \mathbf{N},\ 0 \le k \le d-1\}$$

et $\quad d = \min\{\ k \in \mathbf{N}^* / a^k = e_G\ \}$

Résultats pratiques

- Dans $(G,\cdot)$, $a \in G$ et $ord(a)$ **est fini** , on a :
  - $ord(a) = d$ où d est **le plus petit** $k \in \mathbf{N}^*$ vérifiant $a^k = 1_G$
  - Si $d \in IN^*$ et pour tout $k \in \mathbf{N}^*$, $1 \le k < d$ on a $a^k \neq 1_G$ et $a^d = 1_G$, alors $ord(a) = d$
  - Si $q \in \mathbf{N}^*$, alors on a : $\quad a^q = 1_G \Leftrightarrow ord(a) \mid q$

- Dans $(G,+)$, $a \in G$ et $ord(a)$ **est fini** , on a :

  - $ord(a) = d$ où d est **le plus petit** $k \in \mathbf{N}^*$ tel que $k.a = 0_G$
  - Si $d \in IN^*$ et pour tout $k \in \mathbf{N}^*$, $1 \le k < d$ on a : $k\,a \neq 0_G$ et $d\,a = 0_G$ alors, $ord(a) = d$
  - Si $q \in \mathbf{N}^*$, alors on a : $q.a = 0_G \Leftrightarrow ord(a) \mid q$

Exemples :

1) Si $(G,*)$ est un groupe, alors $ord(e_G) = 1$, de plus pour $a \in G$, $ord(a) = 1 \Leftrightarrow a = e_G$

2) Dans le groupe $(\mathbf{Z},+)$, $ord(0) = 1$ et pour $a \in \mathbf{Z}^*$ on a $ord(a)$ **est infini** car $\langle a \rangle = a.Z$ est infini 3) Dans le groupe $(\Omega_3,\times)$ où $\Omega_3 = \{1,\ j,\ j^2\}$ avec $j = e^{\frac{2i\pi}{3}}$ on a :

$ord(1) = 1$ et $ord(j) = 3$ car $j^1 \neq 1,\ j^2 \neq 1$ et $j^3 = 1$ idem $ord(j^2) = 3$

4) Dans le groupe $(Z/8Z,+)$ on a :

$ord(\bar{0}) = 1$ et $ord(\bar{2}) = 4$ car $1.\bar{2} \neq \bar{0},\ 2.\bar{2} \neq \bar{0}, 3.\bar{2} \neq \bar{0}$ et $4.\bar{2} = \bar{0}$

Théorème 2. Soit $(G,*)$ un **groupe fini**. On a :

Pour tout $a \in G$, $ord(a)$ divise $ord(G)$

En particulier, pour tout $a \in G$, $a^{ord(G)} = e_G$

- Dans $(G,.)$, si on note $ord(G) = n$ alors $\forall x \in G$ on a : $x^n = 1_G$
- Dans $(G,+)$, si on note $ord(G) = n$ alors $\forall x \in G$ on a : $n\,x = 0_G$

Exemples : (autres méthodes pour le calcul de l'ordre d'un élément**)**

1) Dans le groupe $(\Omega_4,\times)$ où $\Omega_4 = \{-i,-1,1,i\}$, calculons $ord(i)$ on a :

$ord(i) \mid 4$ car $ord(\Omega_4) = 4$ d'où $ord(i) \in \{1,2,4\}$ de plus $i^1 \neq 1,\ i^2 \neq 1$ donc $ord(i) = 4$

2) Dans le groupe $(Z/8Z,+)$ calculons $ord(\bar{2})$

- **<u>Méthode 1.</u>** On a : $ord(\bar{2}) \mid 8$ car $ord(Z/8Z) = 8$ d'où $ord(\bar{2}) \in \{1,2,4,8\}$, de plus $1.\bar{2} \neq \bar{0},\ 2.\bar{2} \neq \bar{0}$ et $4.\bar{2} = \bar{0}$ d'où $ord(\bar{2}) = 4$
- **<u>Méthode 2.</u>** Cherchons le plus petit $k \in \mathbf{N}^*$ tel que $k\bar{2} = \bar{0}$ dans $Z/8Z$ on a :

  Dans $Z/8Z$, $k\bar{2} = \bar{0} \Leftrightarrow 2k \equiv 0[8] \Leftrightarrow k \equiv 0[4] \Leftrightarrow \exists m \in \mathbf{Z},\ k = 4m$

  d'où le plus petit $k \in \mathbf{N}^*$ tel que $k\bar{2} = \bar{0}$ dans $Z/8Z$ est $k = 4$ c-à-d $ord(\bar{2}) = 4$

Méthode pratique pour calculer l'ordre d'un élément dans le groupe $(Z/nZ,+)$

Pour déterminer l'ordre de $\bar{a}$ dans le groupe $(Z/nZ,+)$, on cherche **le plus petit** $k \in \mathbf{N}^*$ tel que $k\bar{a} = \bar{0}$, en résolvant l'équation $a\,k \equiv 0[n]$

Proposition

Soient $(G,.)$ un **groupe fini** et $a \in G$. On a:

- $ord(a) = ord(a^{-1})$
- Pour $k \in \mathbf{N}^*$, $ord(a^k) = \dfrac{ord(a)}{ord(a) \wedge k}$

  En particulier, si $k \wedge ord(a) = 1$ alors $ord(a^k) = ord(a)$ et $\langle a \rangle = \langle a^k \rangle$

Version additive : Soient $(G,+)$ un **groupe fini** et $a \in G$. On a:

- $ord(a) = ord(-a)$
- Pour $k \in \mathbf{N}^*$, $ord(k\,a) = \dfrac{ord(a)}{ord(a) \wedge k}$

  En particulier, si $k \wedge ord(a) = 1$ alors $ord(k\,a) = ord(a)$ et $\langle a \rangle = \langle k.a \rangle$

Preuve

Posons $ord(a) = d$ on a $a^d = 1_G$ d'où $\left(a^d\right)^{-1} = (1_G)^{-1}$ c-à-d $\left(a^{-1}\right)^d = 1_G$ donc $\boxed{ord(a^{-1}) \mid ord(a)}$

Idem en remplaçant a par a^{-1} on a $\boxed{ord(a) \mid ord(a^{-1})}$ par suite $ord(a) = ord(a^{-1})$ car $ord(a) \in \mathbf{N}^*$ et $ord(a^{-1}) \in \mathbf{N}^*$

Posons $ord(a) = m$ et $d = k \wedge m$ d'où $m' \wedge k' = 1$ où $m' = \dfrac{m}{d}$ et $k' = \dfrac{k}{d}$

Si $r = ord(a^k)$ alors $\left(a^k\right)^r = a^{kr} = 1_G$ d'où $m \mid (k\,r)$ c-à-d $(d\,m') \mid (d\,k'r)$ donc $m' \mid (k'r)$

or $m' \wedge k' = 1$ d'où $\boxed{m' \mid r}$ (1) d'après le théorème de Gauss

Montrons que $r \mid m'$. On a : $\left(a^k\right)^{m'} = a^{k\,m'} = a^{d\,k'm'} = a^{mk'} = \left(a^m\right)^{k'} = (1_G)^{k'} = 1_G$ car $ord(a) = m$

d'où $ord(a^k) \mid m'$ c-à-d $\boxed{r \mid m'}$ (2) donc $r = m'$ (cf. (1) et (2)) c'est-à-dire $ord(a^k) = \dfrac{ord(a)}{ord(a) \wedge k}$

Exemples

1) Dans le groupe $(\Omega_{24},\times)$ des racines 24èmes de l'unité, on a $a = e^{\frac{i\pi}{3}} \in \Omega_{24}$ car $a^{24} = e^{8i\pi} = 1$ de plus $ord(a) = 6$ car $a^6 = 1$, $a \neq 1$, $a^2 \neq 1$, $a^3 \neq 1$, $a^4 \neq 1$ et $ord(a)$ divise $ord(\Omega_{24}) = 24$.

d'où $ord(a^2) = \dfrac{6}{2 \wedge 6} = 3$ c'est-à-dire $ord(e^{\frac{2i\pi}{3}}) = 3$ idem $ord(e^{\frac{5i\pi}{3}}) = ord(a^5) = \dfrac{6}{5 \wedge 6} = 6$

Remarque : $ord(e^{\frac{2i\pi}{24}}) = 24$ car $e^{\frac{2i\pi}{24}}$ est un générateur du groupe cyclique $(\Omega_{24},\times)$ et $ord(\Omega_{24}) = 24$ d'où $ord(a) = ord\left(\left(e^{\frac{2i\pi}{24}}\right)^4\right) = \dfrac{24}{4 \wedge 24} = \dfrac{24}{4} = 6$

2) Dans le groupe $(Z/16Z,+)$ on a $ord(\bar{1}) = 16$ car $\bar{1}$ est un générateur du groupe cyclique $(Z/16Z,+)$ et $ord(Z/16Z) = 16$ d'où $ord(\bar{8}) = ord(8 \times \bar{1}) = \dfrac{ord(\bar{1})}{8 \wedge ord(\bar{1})} = \dfrac{16}{8 \wedge 16} = 2$

Idem $ord(\overline{12}) = \dfrac{ord(\bar{1})}{12 \wedge ord(\bar{1})} = \dfrac{16}{12 \wedge 16} = \dfrac{16}{4} = 4$

En général, dans $(Z/nZ,+)$, $ord(\bar{a}) = ord(a \times \bar{1}) = \dfrac{ord(\bar{1})}{a \wedge ord(\bar{1})} = \dfrac{n}{a \wedge n}$

IV. Sous-groupes d'un groupe cyclique

Théorème

Si $(G,*)$ est un groupe cyclique et H est un sous-groupe de $(G,*)$, alors $(H,*)$ est un groupe cyclique

Preuve : $(G,*)$ est un groupe cyclique. il existe $a \in G$ tel que $G = \{a^n \ / \ n \in \mathbf{Z}\}$

Pour tout $x \in H$, il existe $d \in \mathbf{Z}$ tel que $x = a^d$

Soit $A = \{n \in \mathbf{N}^* / a^n \in H\}$.

On distingue 2 cas.

1er cas : A est vide.

Dans ce cas, $H = \{e_G\} = \langle e_G \rangle$

2ème cas : A est une partie non vide de $\mathbf{N}^*$

d'après l'axiome de Péano, A admet un plus petit élément noté p.

Montrons que $H = \langle a^p \rangle = \{(a^p)^n \ / \ n \in \mathbf{Z}\}$,

D'après la définition de p , on a : $a^p \in H$ d'où $\langle a^p \rangle \subset H$ car $(H,*)$ est un groupe

Reste à montrer que $H \subset \langle a^p \rangle$

soit $x \in H$. Il existe $d \in \mathbf{Z}$, $x = a^d$ et d'après la division euclidienne de d par p, il existe un unique $(q,r) \in \mathbf{Z} \times \mathbf{N}$, $d = pq + r$ avec $0 \leq r < p$

Et donc $a^d = a^{(pq)} * a^r$. D'où $a^r = a^{-(pq)} * a^d \in H$ car $(H,*)$ est un groupe

Comme $r \in \mathbf{N}$ et $r < p$, $r = 0$ d'après la définition de p.

Par suite $r = 0$ et $x = a^d = a^{pq} = (a^p)^q$. Soit $x \in \langle a^p \rangle$ d'où $H \subset \langle a^p \rangle$

Conclusion : $H = \langle a^p \rangle$ et $(H,*)$ est groupe cyclique

Théorème

Si $(G,*)$ est un groupe **cyclique d'ordre fini** n, alors pour tout $d \in \mathbf{N}^*$ tel que $d \mid n$, **il existe un unique** sous-groupe H de $(G,*)$ tel que $ord(H) = d$

Preuve.

Existence : On a $G = \langle a \rangle$ avec $ord(G) = ord(a) = n$ de plus $d \mid n \Leftrightarrow \exists q \in \mathbf{N}^*, n = dq$

d'où $H = \langle a^q \rangle$ est un sous-groupe de $(G,*)$ et $ord(H) = d$ car

$$ord(H) = ord(a^q) = \frac{ord(a)}{q \wedge ord(a)} = \frac{n}{q \wedge n} = \frac{n}{q} = d$$

Unicité : Soit H' un sous-groupe de $(G,*)$ tel que $ord(H') = d$, alors il existe $q' \in \mathbf{N}^*$ tel que $H' = \langle a^{q'} \rangle$ d'après le théorème précédent

De plus $(a^{q'})^d = a^{q'd} = e_G$ d'où $ord(a) | q'd$ c-à-d $n = dq | q'd$. Ainsi $q \mid q'$

Donc : $\exists d' \in \mathbf{N}^*, q' = d'q$ et $a^{q'} = (a^q)^{d'}$ et $H' = \langle a^{q'} \rangle \subset H = \langle a^q \rangle$

Comme $ord(H) = d = ord(H')$, $H = H'$

V. Exercices d'application

Exercice 1. Donnez un élément $\bar{a}$ du groupe $(Z/140Z,+)$ tel que $ord(\bar{a}) = 70$.

Solution : il suffit de choisir $a = 2$.

En effet : dans $(Z/140Z,+)$, $ord(\bar{2}) = \frac{140}{2 \wedge 140} = 70$

Exercice 2. Montrez que si $(G,*)$ est un groupe fini tel que $ord(G) = p$ où p est premier, alors $(G,*)$ est un groupe cyclique engendré par un élément quelconque différent de e_G.

Solution : $ord(G)=p$ et $p\geq 2$ car p est premier. Soit $a\in G$ et $a\neq e_G$ on a $ord(a)\,|\,p$ donc $ord(a)=1$ ou $ord(a)=p$ car p est premier or $a\neq e_G$ d'où $ord(a)\neq 1$

par suite $ord(a)=p=ord(G)$ donc $G=\langle a\rangle$

Conclusion: $(G,*)$ est un groupe cyclique engendré par tout élément $a\in G$, $a\neq e_G$.

Exercice 3. Montrez que si $(G,*)$ est un groupe **cyclique fini** tel que $ord(G)=p$ où p est un entier premier**,** alors les seuls sous-groupes de $(G,*)$ sont $\{e_G\}$ et G.

Solution : Soit H un sous-groupe du groupe cyclique $(G,*)$

$(H,*)$ est un groupe cyclique. Donc, il existe $a\in G$ tel que $H=\langle a\rangle$

de plus $ord(H)=ord(a)$ et $ord(a)\,|\,p$, donc $ord(a)=1$ ou $ord(a)=p$ car p est premier

d'où $a=e_G$ et $H=\{e_G\}$ ou $ord(a)=p=ord(G)$ et $H=\langle a\rangle=G$

Exercice 4. Montrez que $(Z/12Z,+)$ admet exactement six sous-groupes.

Solution : Si H est un sous-groupe de $(Z/12Z,+)$ alors $ord(H)\,|\,12$ de plus $(Z/12Z,+)$ est un groupe cyclique d'ordre 12 donc pour chaque diviseur $d\in\mathbf{N}^*$ de 12, il existe un unique sous-groupe de $(Z/12Z,+)$ d'orde d

Par conséquent, le nombre de sous-groupes de $(Z/12Z,+)$ est égal au nombre des diviseurs positifs de 12 or 12 admet 6 diviseurs positifs 1, 2, 3, 4, 6 et 12.

Conclusion: $(Z/12Z,+)$ admet exactement six sous-groupes.

Exercice 5. Déterminez les sous-groupes de $(Z/9Z,+)$

Solution : Si H est un sous-groupe de $(Z/9Z,+)$ alors $ord(H)\,|\,9$

De plus $(Z/9Z,+)$ est un groupe cyclique d'ordre 9, donc pour chaque diviseur $d\in\mathbf{N}^*$ de 9, il existe un unique sous-groupe de $(Z/9Z,+)$ d'orde d or les diviseurs positifs de 9 sont les éléments de l'ensemble $\{1,3,9\}$.

par conséquent $(Z/9Z,+)$ admet un unique sous-groupe d'ordre 1, 3 ou 9

$(Z/9Z,+)$ est engendré par $\bar{1}$. Donc,

$ord(H)=1$ si $H=\langle\bar{0}\rangle=\{\bar{0}\}$

$ord(H)=3$ si $H=\langle 3.\bar{1}\rangle=\langle\bar{3}\rangle=\{\bar{0},\bar{3},\bar{6}\}$ car $3=9/3$

et $ord(H)=9$ si $H=Z/9Z$

Conclusion: Les sous-groupes de $(Z/9Z,+)$ sont $\{\bar{0}\}$, $\langle\bar{3}\rangle=\{\bar{0},\bar{3},\bar{6}\}$ et $Z/9Z$

Remarque :

Si $(G,*)$ est un groupe **cyclique d'ordre fini** n et de générateur a, alors pour tout diviseur $d\in\mathbf{N}^*$ de n, l'**unique** sous-groupe de $(G,*)$ d'ordre d est $H=\left\langle a^{\frac{n}{d}}\right\rangle$.

Exercice 6. Déterminez les sous-groupes de $(Z/40Z,+)$ qui contiennent $\overline{12}$

Solution : Soit H un sous-groupe de $(Z/40Z,+)$ tel que $\overline{12}\in H$

alors $ord(H)\,|\,40$ et $ord(\overline{12})\,|\,ord(H)$. Or $ord(\overline{12})=\dfrac{40}{12\wedge 40}=10$

d'où $ord(H)\,|\,40$ et $10\,|\,ord(H)$

Par suite $ord(H)=10$ ou $ord(H)=20$ ou $ord(H)=40$.

De plus $(Z/40Z,+)$ est un groupe cyclique d'ordre 40 donc pour chaque diviseur $d \in \mathbf{N}^*$ de 40, il existe un unique sous-groupe de $(Z/40Z,+)$ d'orde d d'où il existe respectivement un unique sous-groupe d'ordre 10, 20 et 40.

1er cas : $ord(H)=10$

Comme $(Z/40Z,+)$ est engendré par $\bar{1}$ et $40/10=4$,

$$H=\langle 4.\bar{1}\rangle=\langle\bar{4}\rangle=\{\bar{0},\bar{4},\bar{8},\overline{12},\overline{16},\overline{20},\overline{24},\overline{28},\overline{32},\overline{36}\}$$

On a aussi $H=\langle\overline{12}\rangle$ car $ord(\overline{12})=10$

2ème cas : $ord(H)=20$

Comme dans le cas précèdent, on a : $H=\langle\bar{2}\rangle=\{k\bar{2}/k\in\mathbf{N},0\le k\le 19\}=\{\bar{0},\bar{2},\bar{4},\bar{6},\ldots,\overline{36},\overline{38}\}$

3ème cas : $ord(H)=40$ donc $H=Z/40Z$

Conclusion: Les sous-groupes de $(Z/40Z,+)$ qui ont pour élément $\overline{12}$ sont $\langle\bar{4}\rangle$, $\langle\bar{2}\rangle$ et $Z/40Z$

Exercice 7. Déterminez les sous-groupes de $(Z/140Z,+)$ qui contiennent $\overline{42}$ et $\overline{96}$ (indication : Pour $(a,b,c)\in\mathbf{N}^*\times\mathbf{N}^*\times\mathbf{N}^*$, si $a\,|\,c$ et $b\,|\,c$ alors $ppcm(a,b)\,|\,c$)

Solution : Soit H un sous-groupe de $(Z/140Z,+)$ tel que $\overline{42}\in H$ et $\overline{92}\in H$

alors $ord(H)\,|\,140$, $ord(\overline{42})\,|\,ord(H)$ et $ord(\overline{92})\,|\,ord(H)$. Or $ord(\overline{42})=\dfrac{140}{42\wedge 140}=10$ et $ord(\overline{92})=\dfrac{140}{92\wedge 140}=35$ d'où $ppcm(10,35)\,|\,ord(H)$ c'est-à-dire $70\,|\,ord(H)$.

Donc $ord(H)=70$ ou $ord(H)=140$ de plus $ord(\bar{2})=\dfrac{140}{2\wedge 140}=70$ et $(Z/140Z,+)$ est un groupe cyclique d'ordre 140 d'où il existe un unique sous-groupe d'ordre respectivement 70 et 140.

Conclusion: Les sous-groupes de $(Z/140Z,+)$ qui ont pour élément $\overline{42}$ et $\overline{96}$ sont $\langle\bar{2}\rangle=\{k\bar{2}/k\in\mathbf{N},0\le k\le 69\}=\{\bar{0},\bar{2},\bar{4},\bar{6},\ldots,\overline{136},\overline{138}\}$ et $Z/140Z$