or $u(\psi(h)(k_1)) = (u \circ \psi(h_1))(k_1) =$

$= (\varphi(h) \circ u)(k_1) = \varphi(h)(u(k_1))$,

donc g est un isomorphisme de groupes.

i) * Soit $G = \mathbb{Z}/n\mathbb{Z} \times_\varphi \mathbb{Z}/2\mathbb{Z}$, donc

G est le produit (ensembliste) $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

muni de la loi :

$$(\bar{x}, \dot{y}).(\bar{x_1}, \dot{y_1}) = (\bar{x} + (\varphi(\dot{y})(\bar{x_1})), \dot{y+y_1})$$

L'élément neutre est $(\bar{0}, \dot{0})$.

$$(\bar{1}, \dot{0}).(\bar{1}, \dot{0}) = (\bar{1} + (\varphi(\dot{0})(\bar{1}), \dot{0}) =$$

$$= (\bar{1} + \bar{1}, \dot{0}) = (\bar{2}, \dot{0}), \text{ donc}$$

$\forall (\bar{x}, \dot{0})$, avec $0 \leq x < n-1$,

$$(\bar{x}, \dot{0}) = \underbrace{(\bar{1}, \dot{0}).(\bar{1}, \dot{0}).\ldots.(\bar{1}, \dot{0})}_{x \text{ fois}}$$

$\forall (\bar{x}, \dot{0}), (\bar{0}, \dot{y})$ dans G, on a :

$$(\bar{x}, \dot{0}).(\bar{0}, \dot{y}) = (\bar{x} + (\varphi(\dot{0})(\bar{0}), \dot{0+y}) =$$

$= (\bar{x}, \dot{y})$

$\forall (\bar{o}, \dot{y}) \in G$ avec $0 \leq y \leq 1$,

$(\bar{o}, \dot{1}).(\bar{o}, \dot{1}) = (\bar{o} + \varphi(\dot{1})(\bar{o}), \dot{\overline{1+1}})$

$= (\bar{o} - \bar{o}, \dot{2}) = (\bar{o}, \dot{o})$.

Donc G est engendré par

$\{a = (\bar{1}, \dot{o}) ; b = (\bar{o}, \dot{1})\}$ et on a :

$\underbrace{a.a.\ldots a}_{n \text{ fois}} = (\bar{o}, \dot{o}) = O_G$,

$b.b = (\bar{o}, \dot{o}) = O_G$ et $b \neq (\bar{o}, \dot{o})$ donc

$o(b) = 2$.

Si $k \in \{1, \ldots, n-1\}$, $\underbrace{a.\ldots.a}_{k \text{ fois}} =$

$= (\bar{k}, \dot{o}) \neq (\bar{o}, \dot{o})$ donc $o(a) = n$,

$ab = (\bar{1}, \dot{o}).(\bar{o}, \dot{1}) = (\bar{1}, \dot{1})$

$a.b.a.b = (\bar{1}, \dot{1}).(\bar{1}, \dot{1}) =$

$= (\bar{1} + (\varphi(\dot{1})(\bar{1})), \dot{1} + \dot{1}) =$

$= (\bar{1} + f(\bar{1}), \dot{0}) = (\bar{1} - \bar{1}, \dot{0}) =$

$= (\bar{0}, \dot{0})$, et comme $a.b \neq 0_G$ alors

$o(ab) = 2$.

Conclusion: G est un groupe engendré par $\{a, b\}$ tel que $o(a) = n$, $o(b) = 2$ et $o(ab) = 2$.

Inversement, Soit G un groupe engendré par $\{a, b\}$ tel que $o(a) = n$, $o(b) = 2$ et $o(ab) = 2$.

$\forall z \in G$, z s'écrit de la forme

$z = a^{k_1} b^{l_1} a^{k_2} b^{l_2} \dots a^{k_m} b^{l_m}$ où $m \in \mathbb{N}^*$,

$k_i \in \{\pm 1, \dots, \pm n\}$ et $l_i \in \{0, 1\}$.

or $abab = e$ (ie) $aba = b^{-1} = b$,

$ab = b^{-1}a^{-1} = ba^{-1}$, $\forall k \in \mathbb{Z}$: $a^k b = ba^{-k}$

(car $a^k b = a^{k-1}(ab) = a^{k-1} b a^{-1}$

$= a^{k-2} b a^{-2} = \dots = a^{k-(k-1)} b a^{-(k-1)}$

(ie) $a^k b = a b a^{-(k-1)} = b a^{-k}$)

ainsi $z = b^{l_1+\dots+l_m} a^{-k_1-\dots-k_m}$

donc $\forall z \in G, \exists k \in \{0,1\}$ et $\exists \alpha \in \{1,\dots,n\}$ tels que $z = b^k a^\alpha$.

Montrons que cette écriture est unique :

si $z = b^{k_1} a^{\alpha_1} = b^{k_2} a^{\alpha_2}$ alors

$b^{k_1-k_2} = a^{\alpha_2-\alpha_1}$, si $b^{k_1-k_2} = e$

et comme $k_i \in \{0,1\}$ alors forcément

$k_1 - k_2 = 0$ (ie) $k_1 = k_2$ (car $k_1 - k_2 \in \{0,-1,+1\}$ et $b^{-1} = b \neq e$), ainsi

$a^{\alpha_2-\alpha_1} = e$, or $-n < \alpha_2 - \alpha_1 < n$

donc forcément $\alpha_1 = \alpha_2$.

Si $b^{k_1-k_2} \neq e$ alors $b^{k_1-k_2} = b$

$= a^{\alpha_2-\alpha_1}$, donc $o(b) = o(a^{\alpha_2-\alpha_1})$

$= \dfrac{o(a)}{pgcd(o(a), \alpha_2-\alpha_1)} = \dfrac{n}{pgcd(n, \alpha_2-\alpha_1)}$, donc

$pgcd(n, \alpha_2-\alpha_1) = \frac{n}{2}$, d'où $\alpha_2-\alpha_1$ est de la forme $\beta \cdot \frac{n}{2}$ avec $\beta \in \mathbb{N}^*$, si $\beta \geq 2$ alors $\alpha_2-\alpha_1 = \beta \cdot \frac{n}{2} \geq n$, absurde donc $\beta = 1$ (i.e) $|\alpha_2-\alpha_1| = \frac{n}{2}$ et alors $b = a^{\alpha_2-\alpha_1} = a^{\frac{n}{2}}$, donc

$ab = a a^{\frac{n}{2}} = a^{\frac{n+2}{2}}$, $2 = o(ab) =$

$= o(a^{\frac{n+2}{2}}) = \frac{n}{pgcd(n, \frac{n+2}{2})}$ (i.e)

$pgcd(n, \frac{n+2}{2}) = 2^{-1} \cdot n = \frac{n}{2}$, donc

$\frac{n}{2}$ divise $\frac{n}{2}+1$, absurde (sauf si $n=2$ et alors $b=a$, donc $ab=e$, absurde)

Ainsi l'écriture $z = b^k a^\alpha$ est unique et $gr(b) \cap gr(a) = \{e\}$. De plus $|G| = 2n$ car $G = \{\underbrace{e, a, \dots, a^{n-1}}_{n \text{ éléments}}, \underbrace{b, ba, \dots, b^{n-1}a}_{n \text{ éléments}}\}$

Soit $\Psi : G \longmapsto \mathbb{Z}/n\mathbb{Z} \times_\varphi \mathbb{Z}/2\mathbb{Z}$

$$b^k a^\alpha \longmapsto (\bar{0}, \dot{1})^k . (\bar{1}, \dot{0})^\alpha$$

Ψ est alors une application bien définie, homomorphisme de groupes et surjectif, et comme $|G| = |\mathbb{Z}/n\mathbb{Z} \times_\varphi \mathbb{Z}/2\mathbb{Z}| = 2n$ alors Ψ est un isomorphisme de groupes et G est un groupe diédral de degré n.

Conclusion:

Soit $n \geq 2$ et G un groupe. G est diédral de degré n si G est engendré par $\{a, b\}$ tel que $o(a) = n$, $o(b) = 2$ et $o(ab) = 2$.

* Soit $G = \mathbb{Z} \times_\varphi \mathbb{Z}/2\mathbb{Z}$, dans G est le produit (ensembliste) $\mathbb{Z} \times_\varphi \mathbb{Z}/2\mathbb{Z}$ muni de la loi : $(x, \dot{y}) . (x', \dot{y}') = (x + (\varphi(\dot{y}))(x'),$

$\dot{\overline{y+y_2}}$)

L'élément neutre est $(0,\dot{0})$

$(1,\dot{0}).(1,\dot{0}) = (1+\varphi(\dot{0})(1),\dot{0}) =$

$= (1+1,\dot{0}) = (2,\dot{0})$ et il est facile de vérifier que, $\forall n \in \mathbb{N}^*$,

$\underbrace{(1,\dot{0}).(1,\dot{0})\ldots\ldots(1,\dot{0})}_{n \text{ fois}} = (n,\dot{0})$ et

$(-n,\dot{0}) = \underbrace{(-1,\dot{0})\ldots(-1,\dot{0})}_{n \text{ fois}}$, et

$\forall n \in \mathbb{Z}, \forall \dot{y} \in \mathbb{Z}/2\mathbb{Z}$:

$(n,\dot{0}).(0,\dot{y}) = (n+\varphi(\dot{0})(0), \dot{0}+\dot{y}) = (n,\dot{y})$.

$\forall \dot{y} \in \mathbb{Z}/2\mathbb{Z}$ avec $y \in \{0,1\}$, $(0,\dot{1}).(0,\dot{1}) =$

$= (0,\dot{2}) = (0,\dot{0})$, donc $\mathbb{Z} \times_\varphi \mathbb{Z}/2\mathbb{Z}$ est engendré

par $\{a = (1,\dot{0}); b = (0,\dot{1})\}$, on a

$o(a)$ est infini, $o(b) = 2$ et $ab = (1,\dot{1})$ et

D'où $\mathbb{Z}$ (car $a.b.a.b = (1,\dot{1}).(1,\dot{1}) =$

$= (1 + \varphi(\dot{1})(1), \dot{1} + \dot{1}) = (1 + (-1), \dot{2}) =$

$= (0, \dot{0})$). Ainsi un groupe diédral de degré ∞ est un groupe engendré par deux éléments a et b tels que $o(a)$ est infini, $o(b) = o(ab) = 2$.

Inversement; Soit G un groupe engendré par deux éléments a et b tels que $o(a) = \infty$, $o(b) = o(ab) = 2$. Montrons que $G \simeq \mathbb{Z} \times_\varphi \mathbb{Z}/2\mathbb{Z}$.

On a, $\forall z \in G$, $\exists!\,(k,l) \in \mathbb{Z} \times \{0,1\}$ tel que $z = b^l a^k$ (l'écriture vient du fait que $aba = b$ et alors $ab = ba^{-1}$, et l'unicité vient du fait que $gr(b) \cap gr(a) = \{e\}$ puisque si $b = a^\alpha$ alors $o(b) = o(a^\alpha) = 2$, absurde).

Soit $\Psi : G \longrightarrow \mathbb{Z} \times_\varphi \mathbb{Z}/2\mathbb{Z}$

$$b^t a^k \longmapsto (1,\dot{0})^k . (0,\dot{1})^\ell$$

Il est facile de prouver que Ψ est un isomorphisme de groupes. Ainsi un groupe est diédral de degré l'infini si et seulement s'il est engendré par deux éléments a et b tels que a est d'ordre infini et $o(b) = o(ab) = 2$.

j) * si $\forall (a,b) \in G^2$ tel que $(ab)^2 = a^2 b^2$, alors $abab = aabb$, donc $ba = ab$. Ainsi G est abélien.

* Remarquons que si $|G| = 9$ et $\varphi : G \longrightarrow Aut(\mathbb{Z}/32)$ un homomorphisme de groupes. Comme $Aut(\mathbb{Z}/32) = \{ id_{\mathbb{Z}/32}, f$ avec $f(x) = -x \}$ (car si $f : \mathbb{Z}/32 \longrightarrow \mathbb{Z}/32$ automorphisme avec

$f \neq id$, alors $\bar{0} \longmapsto \bar{0}$

$\bar{1} \longmapsto \bar{2} = -\bar{1}$

$\bar{2} \longmapsto \bar{1} = -\bar{2}$)

alors si φ est non trivial il est

surjectif, donc $G/\ker\varphi \simeq Aut(\mathbb{Z}/32)$,

d'où $9 = |G| = 2.|\ker\varphi|$, absurde.

* Si $\varphi : \mathbb{Z}/32 \longmapsto Aut(G)$ un

homomorphisme de groupes où $G = \mathbb{Z}/92$

Si $G_1 = \mathbb{Z}/92 \times_\varphi \mathbb{Z}/32$ alors

$(\bar{1}, \dot{0})^3 = (\bar{1} + \varphi(\dot{0})(\bar{1}), \dot{0}).(\bar{1}, \dot{0}) =$

$= (1 + \underbrace{\varphi(\dot{0})}_{id_G}(\bar{1}) + \underbrace{\varphi(\dot{0})}_{id_G}(\bar{1}), \dot{0}) =$

$= (\bar{1} + \bar{1} + \bar{1}, \dot{0}) = (\bar{3}, \dot{0}) \neq e_{G_1}$,

donc ce n'est pas le bon exemple.

* Comme $G \simeq \mathbb{Z}/32 \times \mathbb{Z}/32$ ou $G \simeq \mathbb{Z}/92$,

l'unique cas qui reste est de prendre

$G_1 = (\mathbb{Z}/32 \times \mathbb{Z}/32) \rtimes_\varphi \mathbb{Z}/32$, avec

$\varphi : \mathbb{Z}/32 \longmapsto Aut(\mathbb{Z}/32 \times \mathbb{Z}/32)$ un homomorphisme de groupes.

$$\varphi : \mathbb{Z}/32 \longmapsto Aut(\mathbb{Z}/32 \times \mathbb{Z}/32)$$

$$\bar{0} \longmapsto id_{\mathbb{Z}/32 \times \mathbb{Z}/32}$$

$$\bar{1} \longmapsto g$$

$$\bar{2} \longmapsto g^2$$

$$\vdots$$

$$g$$

Pour que G_1 soit non abélien il faut et il suffit que φ soit non trivial (ie) $g \neq id_{\mathbb{Z}/32 \times \mathbb{Z}/32}$ et comme $\varphi(\bar{1}+\bar{2}) =$

$= \varphi(\bar{1}) \circ \varphi(\bar{2}) = g \circ g^2 = g^3$ alors $g^3 = id_{\mathbb{Z}/32 \times \mathbb{Z}/32}$, $\varphi(\bar{2}+\bar{2} = \bar{4} = \bar{1}) =$

$= g = g^2 \circ g^2$, donc $g^2 \neq id_{\mathbb{Z}/32 \times \mathbb{Z}/32}$,

d'où $o(g) = 3$. On doit avoir

$\forall (x,\dot{y}) \in G_1, (x,\dot{y})^3 =$

$= (x + \varphi(\dot{y})(x), 2\dot{y}).(x,\dot{y}) =$

$= (x + \varphi(\dot{y})(x) + \varphi(2\dot{y})(x), 3\dot{y}) =$

$= (x + \varphi(\dot{y})(x) + \varphi(\dot{y})^2(x), \dot{0}) = (0, \dot{0})$

(ie) $\forall x \in \mathbb{Z}/32 \times \mathbb{Z}/32 : x + g(x) + g^2(x) = 0.$

Soit alors $g : \mathbb{Z}/32 \times \mathbb{Z}/32 \longmapsto \mathbb{Z}/32 \times \mathbb{Z}/32$

définie par :

$(\bar{0},\bar{0}) \longmapsto (\bar{0},\bar{0})$

$(\bar{1},\bar{0}) \longmapsto (\bar{1},\bar{1})$

$(\bar{2},\bar{0}) \longmapsto (\bar{2},\bar{2})$

$(\bar{0},\bar{1}) \longmapsto (\bar{0},\bar{1})$

$(\bar{0},\bar{2}) \longmapsto (\bar{0},\bar{2})$

$(\bar{1},\bar{1}) \longmapsto (\bar{1},\bar{2})$

$(\bar{1},\bar{2}) \longmapsto (\bar{1},\bar{0})$

$(\bar{2},\bar{1}) \longmapsto (\bar{2},\bar{0})$

$(\bar{2},\bar{2}) \longmapsto (\bar{2},\bar{1})$

(Les images à choisir sont celles de $(\bar{1},\bar{0})$ et $(\bar{0},\bar{1})$, les autres découlent (cf graphique) Les images doivent respecter les 2 conditions:

$o(g)=3, \forall x \in \mathbb{Z}/32 \times \mathbb{Z}/32, x+g(x)+g^2(x)=0$)

Sinon : $(\bar{1},\bar{0})+(\bar{1},\bar{1})+(\bar{1},\bar{2})=(\bar{0},\bar{0})$

$(\bar{2},\bar{0})+(\bar{2},\bar{2})+(\bar{2},\bar{1})=(\bar{0},\bar{0})$

$(\bar{0},\bar{1})+(\bar{0},\bar{1})+(\bar{0},\bar{1})=(\bar{0},\bar{0})$

$(\bar{0},\bar{2})+(\bar{0},\bar{2})+(\bar{0},\bar{2})=(\bar{0},\bar{0})$

$(\bar{1},\bar{1})+(\bar{1},\bar{2})+(\bar{1},\bar{0})=(\bar{0},\bar{0})$

$(\bar{1},\bar{2})+(\bar{1},\bar{0})+(\bar{1},\bar{1})=(\bar{0},\bar{0})$

$(\bar{2},\bar{1})+(\bar{2},\bar{0})+(\bar{2},\bar{2})=(\bar{0},\bar{0})$,

ainsi $\forall x \in \mathbb{Z}/32 \times \mathbb{Z}/32 : x+g(x)+g^2(x)=$

$= 0_{\mathbb{Z}/32 \times \mathbb{Z}/32}$.

$g^3 = id_G$ et $g^2 \neq id_G$

(car $g^2(\bar{1},\bar{0}) = g(\bar{1},\bar{1}) = (\bar{1},\bar{2})$))

Montrons que si $G_1 = (\mathbb{Z}/32 \times \mathbb{Z}/32) \times_\varphi \mathbb{Z}/32$

où $\varphi : \mathbb{Z}/32 \longmapsto Aut(\mathbb{Z}/32 \times \mathbb{Z}/32)$

$\bar{0} \longmapsto id_G$

$$\overline{1} \longmapsto g$$
$$\overline{2} \longmapsto g^2$$

alors φ est un homomorphisme de groupes non trivial, et alors G_1 non abélien,

en effet $\forall z = (x, y) \in G_1$:

$$z^3 = z^2 \cdot z = [(x,y)\cdot(x,y)]\cdot(x,y)$$

$$= (x + \varphi(y)(x), 2y)\cdot(x,y) =$$

$$= (x + \varphi(y)(x) + \varphi(2y)(x), 3y)$$

$$= (x + \varphi(y)(x) + \varphi(y)^2(x), 0) = (0,0)$$

car $x + \varphi(y)(x) + \varphi(y)^2(x) =$

$$= \begin{cases} x + x + x = 3x = 0 & \text{si } \varphi(y) = id_G \\ x + g(x) + g^2(x) = 0 & \text{si } \varphi(y) = g \\ x + g^2(x) + g^4(x) = x + g^2(x) + g(x) = 0 & \text{si } \varphi(y) = g^2 \end{cases}$$

D'où, $\forall (a,b) \in G_1^2$, $a^3 b^3 = (ab)^3 \ (= 0_{G_1})$

et G_1 est non abélien.