Proyecciones Journal of Mathematics
Vol. 25, N^o 2, pp. 121-150, August 2006.
Universidad Católica del Norte
Antofagasta - Chile

UN ETUDE CLASSIQUE DES DUPLICATIONS D'UN GROUPE CYCLIQUE

ALFONSO RIDER-MOYANO
and
RAFAEL RUBIO-RUIZ
UNIVERSIDAD DE CORDOBA, ESPAÑA

Received : May 2005. Accepted : April 2006

Abstract

Pour chaque entier n, nous allons à établir la quantité, sauf isomorphism, des groupes G d'ordre $2n$ et de façon qu'ils aient au moins un élément d'ordre n. C'est-à-dire, nous donnerons le nombre des groupes (sauf isomorphism) d'ordre $2n$, qui aient un sous-groupe isomorphic au groupe cyclique d'ordre n, $\mathcal{C}_n$.

En plus , nous étudierons aussi la structure de ces groupes.

AMS Subject Class : *(2000):20E34, 20F05, 20F22.*

1. Introduction

Il est considérable la quantité des groupes finis qui apparaissent comment la duplication d'un groupe cyclique d'ordre $n \in \mathbb{N}^*$. C'est-à-dire, des groupes d'ordre $2n$, qui ont au moins un élément d'ordre n, donc ils contenissent un sous-groupe cyclique isomorph à $\mathcal{C}_n$.

De ça façon, en plus du groupe produit $\mathcal{C}_2 \times \mathcal{C}_n$ et le groupe cyclique $\mathcal{C}_{2n}$ nous pouvons remarquer, le groupe diedrique à degré n $\mathcal{D}_n$, le groupe dicyclique à degré n $\mathcal{DC}_n$, le groupe semi-diedrique à degré n $\mathcal{SD}_n$, le groupe semi-cyclique à degré n $\mathcal{DC}_n$, etc,.. Touts ces groupes sont definis de maniére simple grâce à leurs presentations (generateurs et relations).

Dans ce travail, nous étudierons de manière classique, les duplications des groupes cycliques. C'est-à-dire, nous allons établir la quantité -sauf ismorphismes- des groupes G d'ordre $2n$, qui contenissent au moins , un élément d'ordre n. En plus, nous étudierons aussi, la structure de ces groupes et nous caractérisons leurs presentations, en donnant la description de quelques modèles classiques.

Définition 1. *On dira que le groupe G d'ordre $2n$ est une duplication du groupe cyclique $\mathcal{C}_n$, s'il a un élément g d'ordre n.*

Pour $n = 1, 2$, la réponse est immédiate :

Si $n = 1$, alors $g = e$ et $G = \{e, s\}$ avec $e \neq s$, c'est-à-dire $G \sim \mathcal{C}_2$.

Si $n = 2$, alors $G = \{e, g, s, sg\}$ avec $s \notin < g >$ et il y a deux cas: pour le $ord(s) = 2$, nous aurions $G = \mathcal{C}_2 \times \mathcal{C}_2$, tandis que pour le $ord(s) = 4$ on aura $G \sim \mathcal{C}_4$

En général, soit G un groupe d'ordre $2n$ et soit $g \in G$ un élément d'ordre n. Il est claire que le sous-groupe $< g >$ a index 2 et en conséquence, il est posible d'écrire $G =< g > \cup s < g >= \{e, g, g^2, \ldots, s, sg, \ldots, sg^{n-1}\}$. C'est-à-dire, le groupe est génère par un élément d'ordre n et un autre élément qui n'appartient a le sous-groupe $< g >$.

2. Sur la table du groupe

La table du groupe aura quatre quarts:

Dans le quart supérieur à gauche, ils seraient les produits $g^x g^y$, dont loi sera fermée dans ce quart, c'est-à-dire, cette operation on fera dans $\mathcal{C}_n$, $g^x g^y = g^{x+y}$.

Dans le quart inférieur à gauche seront les produits d'éléments de $s < g >$ par les éléments de $< g >$. Le résultat sera dans $s < g >$, $sg^x g^y = s(g^x g^y) = sg^{x+y}$.

Dans le supérieur a droite seront les produits $g^x(sg^y)$, qui appartiendront à la classe $s < g >$. Le résultat de ces produits, dépendra d'un entier μ tel que $gs = sg^\mu$, ou d'autre façon, d'un entier μ tel que $i_s(g) = s^{-1}gs = g^\mu$. En effet, $i_s(g^x) = s^{-1}g^x s = (i_s(g))^x = (g^\mu)^x = g^{\mu x} \Rightarrow g^x s = sg^\mu$. Et pour finir, $g^x(sg^y) = (g^x s)g^y = (sg^{\mu x})g^y = sg^{\mu x+y}$.

Dans la quart inférieur à droite nous aurons les produits de la façon $(sg^x)(sg^y)$, qui appartenirant à la classe $< g >$ et ils dependrant, d'un entier β, tel que $s^2 = g^\beta$, puisque, si nous connaisons l'exposant β, alors $(sg^x)(sg^y) = s(g^x sg^y) = s(sg^{\mu x+y}) = g^\beta g^{\mu x+y} = g^{\beta+\mu x+y}$.

Ainsi, la table du groupe sera en fonction des entiers μ y β tels que $s^{-1}gs = g^\mu$ et $s^2 = g^\beta$.

Observons que $(sg^y)^{-1}g^x(sg^y) = g^{-y}(s^{-1}g^x s)g^y = g^{\mu x} = (g^x)^\mu$ et que $(sg^y)^2 = g^{\beta+(\mu+1)y}$. En consequence, l'entier μ ne change pas pour chaque élément du sous-groupe $< g >$ et non plus, si nous changeons s, par un autre élément de leur classe $s < g >$. Pourtant, si nous prenons l'élément sg^y au lieu de s, il est posible qu'il change le valeur de β.

Définition 2. *Si on a determiné les entiers μ y β, on dira que le groupe G est une duplication de type (n, μ, β).*

La loi interne que nous avons donné pour chaque quart dans la table, on pourra écrire de façon global: $(s^u g^x)(s^v g^y) = s^{u+v} g^{uv\beta+\mu^v x+y}$, $\mu, u, v \in \mathbf{Z/2Z}$ et $x, y \in \mathbf{Z/nZ}$.

Les éléments inverses s'écriront $(s^u g^x)^{-1} = s^u g^{-\mu\beta-\mu^u x}$.

2.1. Des conditions nécesaires et suffisantes pour les entiers μ et β

Proposition 1. *Soit $s \notin < g >$, alors $s^2 \in < g >$ et $s^2 \in \mathcal{Z}(G)$. En plus, si $s^{-1}gs = g^\mu$, alors on a que $\mu^2 \equiv 1 \,(mod\, n)$.*

Démonstration

Supposons que $s^2 \notin < g >$, il existe x tel que $s^2 = sg^x$, donc $s = g^x$, ce qui est contradictoire. Il est claire que s^2 commutera avec les élément du sous-groupe $< g >$ et comme $s^2(sg^x) = (s^2 s)g^x = s(s^2 g^x) = s(g^x s^2) = (sg^x)s^2$, nous avons que $s^2 \in \mathcal{Z}(G)$.

Si nous faisons deux fois l'automorphism interne i_s sur g, on a que $s^{-2}gs^2 = s^{-1}(s^{-1}gs)s = s^{-1}g^{\mu}s = g^{\mu^2}$, mais comme $s^2 \in \mathcal{Z}(G)$, nous avons que $g = g^{\mu^2}$, donc $\mu^2 \equiv 1\,(mod\, n)$. □

D'autre part, observez que si $s^2 = g^{\beta}$, *alors* $(\mu - 1)\beta \equiv 0\,(mod\, n)$, *puisque* $g^{\beta} \in \mathcal{Z}(G)$, $s^{-1}g^{\beta}s = g^{\beta}$ *et* $s^{-1}g^{\beta}s = g^{\mu\beta}$. *En consequence,* $g^{\beta} = g^{\mu\beta} \Leftrightarrow e = g^{(\mu-1)\beta} \Leftrightarrow (\mu - 1)\beta \equiv 0\,(mod\, n)$

Remarquez que μ est un élément d'ordre 2 (ou involutif) dans le groupe multiplicatif des unités du anneaux $\mathbf{Z/nZ}$. Ils existent toujours de ces élément (par example $\mu = 1$ et $\mu = n - 1$). Dans l'appendice de ce travail, nous donnerons des méthodes pour trouver ces éléments et donnerons aussi, une formule qui exprimera la quantité d'eux.

Si on a donne un valeur pour μ, il faut que l'entier β soit une solution pour l'equation en congruences $(\mu - 1)x \equiv 0\,(mod\, n)$. Cette équation est linéaire et homogène, donc elle sera toujours compatible et l'ensemble $\mathcal{B}$, qui est formé par toutes ses solutions, il est un sous-groupe de $(\mathbf{Z/nZ}, +)$, dont ordre est $d = pgcd\,\{n, \mu - 1\}$ (où, pgcd note le plus grand commun diviseur). Un générateur de ce sous-groupe est la classe du entier n/d, module n. Comme $(\mu - 1)(\mu + 1) = \mu^2 - 1 = 0\,(mod\, n)$, on aura que $\mu + 1 \in \mathcal{B}$. Cette solution n'est pas nulle, sauf que $d \geq 2$. Encore, si on aurait $\mu = n - 1$ et en étant n pair, on a que $d = pgcd\,\{n, n - 2\} = 2$ et $\mathcal{B} = \{0, n/2\}$. C'est-a-dire, le groupe $\mathcal{B}$ est trivial si et seulement si $\mu = n - 1$ et n est impair.

Voyons maintenant, la suffisance des conditions précédentes.

D'abort, nous prenons l'ensemble support $G = \mathbf{Z/2Z} \times \mathbf{Z/nZ}$, dont cardinal est $2n$ et nous définissons la loi interne suivante:

$$(u, x)(v, y) = (u + v, uv\beta + \mu^v x + y)$$

Cette opération donne sur G une structure de groupe et en plus G sera une duplication de type (n, μ, β). En effet:

1) La opération est associative

$((u, x)(v, y))(w, z) = (u + v, uv\beta + \mu^v x + y)(w, z) = ((u + v) + w, (u + v)w\beta + \mu^w(uv\beta + \mu^v x + y) + z)$,

$(u, x)((v, y)(w, z)) = (u, x)(v + w, vw\beta\mu^w y + z) = (u + (v + w), u(v + w)\beta + \mu^{v+w}x + vw\beta + \mu^w y + z)$,

il reste à voir si $(u+v)w\beta+\mu^w(uv\beta+\mu^v x+y)+z) \equiv u(v+w)\beta+\mu^{v+w}x+vw\beta+\mu^w y+z) \Leftrightarrow \mu^w uv\beta \equiv uv\beta$.

Si $w = 0$, cette question est triviale. D'autre part, si $w = 1$, la dernière expression est équivalent à $uv(\mu-1)\beta \equiv 0$, qui est vraie n'importe pas pour quoi valeurs de u et v.

2) Il est claire, que le couple (0,0) est l'element neutre

3) Le couple $(u, -u\beta - \mu^u x)$ est l'inverse de (u, x). Il suffit de voir, que $u\beta - u\beta\mu^u - \mu^{2u}x + x \equiv -u(\mu^u - 1)\beta - (\mu^2)^u x + x \equiv -u(\mu^u - 1)\beta - x + x = -u(\mu^u - 1)\beta \equiv 0$, et pour finir, il suffit de raisonner de la même façon que dans 1.

4) Remarquons les éléments $g = (0, 1)$ et $s = (1, 0)$.

N'est pas difficile de voir par induction que $g^x = (0, x)$ et en consequence g aura ordre n. Comme $s \notin < g >$ on a que $G =< g, s >$.

D'autre part, $s^{-1} = (1, 0) = (1, -\beta)$ et $s^{-1}gs = (1, -\beta)(0, 1)(1, 0) = (1, -\beta)(1, \mu) = (0, \beta - \mu\beta + \mu) = (0, \mu) = g^\mu$ et finalement $s^2 = (1, 0)(1, 0) = (0, \beta) = g^\beta$.

2.2. Le centre d'une duplication

D'abort, si $\mu = 1$ le groupe G est commutatif et $G = \mathcal{Z}(G)$.

Si $\mu \neq 1$ il n'y a aucun élément dans la classe $s < g >$ qu'il soit commutatif avec g et en consequence $\mathcal{Z}(G) \subset < g >$. De ça façon $g^x \in \mathcal{Z}(G)$ si et seulement s'il commute avec chaque élément $sg^y \in s < g >$. Ainsi, $g^x sg^y = sg^y g^x \Leftrightarrow sg^{\mu x + y} = sg^{y+x} \Leftrightarrow g^{\mu x} = g^x \Leftrightarrow \mu x \equiv x \,(mod\, n) \Leftrightarrow (\mu - 1)x \equiv 0 (mod\, n)$. Donc, $\mathcal{Z}(G)$ sera isomorph au sous-groupe $\mathcal{B} \leq (\mathbf{Z}/\mathbf{nZ}, +)$ (rappelons que $\mathcal{B}$ est le sous-groupe des solutions de la écuation $(\mu - 1)x \equiv 0 \,(mod\, n)$) et l'ordre de $\mathcal{Z}(G)$ sera $d = pgcd\,\{n, \mu - 1\}$, en étant $\mathcal{Z}(G) =< g^{\frac{n}{d}} >$.

Remarquons que $\mathcal{Z}(G) = e$ si et seulement si $\mu = n - 1$ et n est impair.

3. Sur l'indicateur d'involution

3.1. Indice d'un élément involutif

Proposition 2. *Soit μ un élément involutif, module n, et soit $\mathcal{B}$ le groupe des solutions pour l'écuation $(\mu - 1)\xi \equiv 0 \,(mod\, n)$.*

Alors, l'indice du sous-groupe $< \mu + 1 >$ dans $\mathcal{B}$ est au plus 2.

Démonstration

Comme $\mu+1$ est un élément involutif du groupe $\mathcal{B}$, il existe un entier c tel que $\mu+1 = c(n/d)$ et ainsi, on aura que $ord\,(\mu+1) = \frac{d}{pgcd\,\{d,c\}}$, $Ind\,(<\mu+1>) = pgcd\,\{d,c\}$.

D'autre part, comme l'entier $\mathcal{I} = pgcd\,\{d,c\}$ divise au entier c, $\mathcal{I}$ divisera aussi a $\mu+1$ et comme il divise à d, il divisera aussi à $\mu-1$. Donc

$$\mathcal{I} \mid pgcd\,\{\mu+1,\mu-1\} = pgcd\,\{\mu-1,2\} = \begin{cases} 1 & \text{si } \mu \text{ est pair} \\ 2 & \text{si } \mu \text{ est impair} \end{cases}$$

En consequence, nous aurions que $\mathcal{I}=1$, ou bien $\mathcal{I}=2$. □

À l'avenir, l'indice de $\mu+1$ dans $\mathcal{B}$, on appellera indice de μ et on notera $Ind\,(\mu)$. De ça façon on a la égalité, $Ind\,(\mu)\,ord\,(\mu+1) = pgcd\,\{n,\mu-1\}$

Pour tout élḿent involutif module n μ, on vérifie que

$Ind\,(\mu)n = pgcd\,\{n,\mu-1\}\,pgcd\,\{n,\mu+1\}$. En effet, l'ordre de $\mu+1$ dans le groupe $\mathbf{Z/nZ}$ est $ord\,(\mu+1) = \frac{n}{pgcd\,\{n,\mu+1\}}$.

D'autre par, nous avons obtenu que $ord\,(\mu+1) = \frac{pgcd\,\{n,\mu-1\}}{Ind\,(\mu)}$.

Proposition 3. *Si μ est involutif module n, on vérifie que $Ind\,(n-\mu) = Ind\,(\mu)$.*

Démonstration

a) Tout diviseur commun pour n et $(n-\mu)-1$, est un diviseur commun pour n et $(n-((n-\mu)-1) = \mu+1$.

Au contraire, un diviseur commun pour n et $\mu+1$, est aussi diviseur commun pour n et $n-(\mu+1)$. Donc, si nous notons par $[m]$ l'ensemble formé par les multiples d'un entier m, on a que $[n]\cap[(n-\mu)-1] = [n]\cap[\mu+1]$. Ce qui est equivalent à $pgcd\,\{n,(n-\mu)-1\} = pgcd\,\{n,\mu+1\}$.

b) Tout le diviseur commun pour n et $(n-\mu)+1$ est un diviseur commun pour n et $(n-(n-\mu)+1) = \mu-1$. Au contraire, un diviseur commun pour n et $\mu-1$ est aussi diviseur commun pour n et $n-(\mu-1)$. Donc $[n]\cap[(n-\mu)+1] = [n]\cap[\mu-1]$. Ce qui est equivalent à $pgcd\,\{n,(n-\mu)+1\} = pgcd\,\{n,\mu-1\}$.

Maintenant, nous utilisons l'observation d'avant, et pouvons écrire, $Ind\,(n-\mu)\,n = pgcd\,\{n,(n-\mu)-1\}\,pgcd\,\{n,(n-\mu)+1\} = pgcd\,\{n,\mu+1\}\,pgcd\{n,\mu-1\} = Ind\,(\mu)n \Rightarrow Ind(n-\mu) = Ind\,(\mu)$. □

3.2. Indice des élément involutif $\mu = 1$ et $\mu = n - 1$

Proposition 4. *Pour chaque entier $n \geq 3$, on a:*

$$Ind\,(1) = Ind\,(n-1) = \begin{cases} 1 & \textit{si } n \textit{ est impair} \\ 2 & \textit{si } n \textit{ est pair} \end{cases}$$

Démonstration

Comme nous savons que $Ind\,(1) = Ind\,(n-1)$, il suffit de calculer l'indice de 1. Puisque $pgcd\,\{n, \mu-1\} = pgcd\,\{n, 0\} = n$ et $pgcd\,\{n, \mu+1\} = pgcd\,\{n, 2\} = \begin{cases} 1 & \text{si } n \text{ est impair} \\ 2 & \text{si } n \text{ est pair} \end{cases}$
en utilisant la formule $Ind\,(\mu)\, n = pgcd\,\{n, \mu-1\}\, pgcd\,\{n, \mu+1\}$, on aura

$$Ind\,(1)\; n = \begin{cases} n & \text{si } n \text{ est impair} \\ 2n & \text{si } n \text{ est pair} \end{cases} \Rightarrow Ind\,(1) = \begin{cases} 1 & \text{si } n \text{ est impair} \\ 2 & \text{si } n \text{ est pair} \end{cases}$$

Remarquons que si n$\geq$ 3 est un entier impair, pour tout élément involutif μ, module n, comme $Ind\,(\mu) \mid n$, on vérifie que $Ind\,(\mu) = 1$. □

3.3. Sur les indices pour n pair

Après le dernier résultat, le cas $Ind\,(\mu) = 2$, n'est pas possible que pour modules pairs. Dans ces cas, on pourra écrire $n = 2^m p$, $m \geq 1$, p impair.

D'abort, supposons $p = 1$. Si $m = 1$ $(n = 2)$, il y a seulement un élément involutif (μ) avec indice 2.

D'autre part, si $m = 2$ $(n = 4)$, il y aura deux élément involutif: 1 et 3, tout les deux, avec indice 2.

Proposition 5. *Dans le cas $n = 2^m$, avec $m \geq 3$ on vérifie:*
$Ind\,(1) = Ind\,(2^m - 1) = 2$ *et* $Ind\,(2^{m-1}) = Ind\,(2^{m-1} + 1) = 1$.

Démonstration

Nous savons (n pair) que $Ind\,(1) = Ind\,(2^m - 1) = 2$. Les autres deux élément involutif (voir appendice) seront opposés l'un du autre. Donc, il suffit de étudier le cas $\mu = 2^{m-1} - 1$. De ça façon:
$Ind(\mu)\, 2^m = Ind\,(\mu)\, n = pgcd\,\{n, \mu-1\}\, pgcd\,\{n, \mu+1\} =$
$pgcd\,\{2^m, 2^{m-1}-2\}\, pgcd\,\{2^m, 2^n\} = 2\, pgcd\,\{2^{m-1}, 2^{m-2}-1\}\, 2^{m-1}\, pgcd\,\{2, 1\} =$
$2^m \Rightarrow Ind\,(\mu) = 1$. □

Remarquez que nous avons utilisé que $pgcd\,\{2^{m-1\}, 22m-2} - 1\} = 1$, puisque si $m \geq 3$, l'entier 2^{m-2} est impair.

3.4. Sur les indices pour $n = 2^m p$, ou $m \geq 1$ et l'entier $p \geq 3$ est impaire

Si μ est involutif, module $n = 2p$, avec l'entier impair $p \geq 3$, alors $Ind\,(\mu) = 2$. En effet:

$Ind\,(\mu)\,2p = Ind\,(\mu)\,n = pgcd\,\{n, \mu - 1\}\,pgcd\,\{n, \mu + 1\} =$

$pgcd\,\{2p, \mu - 1\}\,pgcd\,\{2p, \mu + 1\} = 2pgcd\,\{p, \frac{(\mu-1)}{2}\}\,2pgcd\,\{p, \frac{(\mu+1)}{2}\} \Rightarrow$ $Ind\,(\mu)\,p = 2pgcd\,\{p, \frac{(\mu-1)}{2}\}\,pgcd\,\{p, \frac{(\mu+1)}{2}\}$. Comme le deuxième côté de la égalité est pair et p est impair, alors $Ind\,(\mu) = 2$.

D'autre part, si μ est involutif, module $n = 4p$, ou $p \geq 3$ est un entier impair, on aura que $Ind\,(\mu) = 2$. Puisque, tout l'élément involutif, module $n = 4p$ est dans la classe de congruence module 4, des entiers 1 ou 3. Alors:

a) $\mu \equiv 1\,(mod\ 4) \Rightarrow \mu - 1 \equiv 0\,(mod\ 4)$. Donc, $Ind\,(\mu)\,4p = Ind\,(\mu)\,n =$ $pgcd\,\{n, \mu - 1\}\,pgcd\,\{n, \mu + 1\} =$

$pgcd\,\{4p, \mu - 1\}\,pgcd\,\{4p, \mu + 1\} = 4pgcd\,\{p, \frac{(\mu-1)}{4}\}\,2pgcd\,\{2p, \frac{(\mu+1)}{2}\} \Rightarrow$ $Ind\,(\mu)\,p = 2pgcd\,\{p, \frac{(\mu-1)}{4}\}\,pgcd\,\{2p, \frac{(\mu+1)}{2}\}$.

Comme le deuxième côté est pair et l'entier p est impair, on a que $Ind\,(\mu) = 2$.

b) $\mu \equiv 3\,(mod\ 4) \Rightarrow n - \mu \equiv -3 \equiv 1\,(mod\ 4)$. Donc, $Ind\,(n - \mu) = 2$ et $ind\,(\mu) = Ind\,(n - \mu)$.

Proposition 6. *Si $n = 2^m p$, ou $m \geq 3$, l'entier $p \geq 3$ est impair et μ est involutif module n, on vérifie:*

$$Ind\,(\mu) = \begin{cases} 2 & si\ \mu \equiv \begin{cases} 1 & (mod\ 2^m) \\ 2^m - 1 & (mod\ 2^m) \end{cases} \\ 1 & si\ \mu \equiv \begin{cases} 2^{m-1} - 1 & (mod\ 2^m) \\ 2^{m-1} + 1 & (mod\ 2^m) \end{cases} \end{cases}$$

Démonstration

Comme μ est involutif module $2^m p$, il sera aussi involutif module 2^m. Donc il appartiendra à une des classes des entiers $1, 2^{m-1}, 2^{m-1} + 1, 2^m - 1$.

a)$\mu \equiv 1\,(mod\ 2^m) \Leftrightarrow \mu - 1 \in 2^m \mathbf{Z}$. Alors:

$$Ind\,(\mu)\,2^m p = Ind\,(\mu)\,n = pgcd\,\{n, \mu - 1\} = pgcd\,\{n, \mu + 1\} =$$

$$pgcd\,\{2^m p, \mu - 1\}\,pgcd\,\{2^m p, \mu + 1\}$$

$$= 2^m pgcd\{p, \frac{(\mu-1)}{2^m}\}\, 2\, m\, pgcd\{2^{m-1}p, \frac{(\mu+1)}{2}\} \Rightarrow$$

$$Ind\,(\mu)\, p = 2\, pgcd\{p, \frac{(\mu-1)}{2^m}\}\, pgcd\{2^{m-1}p, \frac{(\mu+1)}{2}\}$$

Le deuxième côté de la égalité est pair et l'entier p est impair, en consequence $Ind(\mu) = 2$.

b) $\mu \equiv 2^{m-1} - 1\,(mod\ 2^m)$. Il existe un entier c tel que
$\mu = 2^m c + 2^{m-1} - 1$. De ça façon,
$Ind\,(\mu)\, 2^m p = ind\,(\mu)\, n = pgcd\{n, \mu - 1\}\, pgcd\{n, \mu + 1\} =$
$pgcd\{2^m p, 2^m c + 2^{m-1} - 2\}\, pgcd\{2^m p, 2^m c + 2^{m-1}\} =$
$2\, pgcd\{2^{m-1}p, 2^{m-1}c + 2^{m-2} - 1\}\, 2^{m-1}\, pgcd\{2p, 2c+1\} \Rightarrow$
$Ind\,(\mu)\, p = pgcd\{2^{m-1}p, 2^{m-1}c + 2^{m-2} - 1\}\, pgcd\{2p, 2c+1\}$
Comme $m \geq 3$, alors l'entier $2^{m-1}c + 2m - 2 - 1$ es impair. D'autre part, l'entier $2c + 1$ est aussi impair et le deuxième côté de la égalité précédente ne contiendra pas le facteur 2. Ainsi, il n'est pas possible que $Ind\,(\mu) = 2$.

c) $\mu \equiv 2^{m-1} + 1\,(mod\ 2^m)$. Il existe un entier c tel que $\mu = 2^m c + 2^{m-1} + 1$. De ça façon,
$n - \mu = 2^m p - 2^c - 2^{m-1} - 1 = -2^{m-1} - 1 \equiv 2^{m-1} - 1\,(mod\ 2^m)$
D'après b), $Ind\,(n - \mu) = 1$ et rappelez que $ind\,(\mu) = Ind\,(n - \mu)$.

d) $\mu \equiv 2^m - 1\,(mod\ 2^m)$. Il existe un entier c, tel que $\mu = 2^m c + 2^m - 1$. De ça façon,
$n - \mu = 2^m p - 2^m c - 2^m + 1 \equiv 1\,(mod\ 2^m)$. D'après a) $Ind\,(n - \mu) = 2 = Ind\,(\mu)$. □

3.5. Le premier théorème d'isomorphism pour duplications

Proposition 7. *Supposons que* $ind\,(\mu) = 2$, *et soit* $d = pgcd\{n, \mu - 1\}$. *Alors, les duplications* $(n, \mu, 0)$ *et* $(n, \mu, \frac{n}{d})$ *ne sont pas isomorphes.*

Démonstration

Comme n sera pair, dans la premiere duplication aura au moins deux élément d'ordre deux: $g^{\frac{n}{2}}$ (c'est l'unique dans $< g >$) et s. Dans la deuxième duplication il sera seulement l'élément $g^{\frac{n}{2}}$, puisque:
$(sg^x)^2 = g^{\frac{n}{d}+(\mu+1)x} = e \Rightarrow \frac{n}{d} + (\mu+1)x \equiv 0\,(mod\ n) \Rightarrow \frac{n}{d} \equiv -x\,(\mu + 1)\,(mod\ n) \Rightarrow Ind\,(\mu) = 1$ □

Proposition 8. *Soit μ une solution de la écuation $\xi^2 \equiv 1\,(mod\ n)$ et soient β_1, β_2 deux solutions de l'écuation*
$(\mu-1)\xi \equiv 0\,(mod\ n)$. Alors les duplications de types (n, μ, β_1) et (n, μ, β_2) sont isomorphes si et seulement si
$\beta_1 \equiv \beta_2\,(mod\ < \mu+1 >)$.

Démonstration

Considérons un groupe G d'ordre $2n$, avec génératuers g et s, tels que: $ord\,(g) = n$, $s \notin < g >$, $s^{-1}gs = g^{\mu}$ et $s^2 = g^{\beta_1}$.

Et soit H un autre groupe d'ordre $2n$ et générateurs h, t tels que: $ord\,(h) = n$, $t \notin < h >$, $t^{-1}ht = h^{\mu}$ et $t^2 = h^{\beta_2}$.

Comme $\beta_1 \equiv \beta_2\,(mod\ < \mu+1 >)$, il existera un élément c tel que $\beta_1 - \beta_2 \equiv c\,(\mu+1)\,(mod\ n)$.

La application $f : G \to H$ définie par la loi $f(s^{\mu}g^x) = t^{\mu}h^{x+cu}$ est un morphism de groupes. En effet,

1) $f(g^x g^y) = f(g^{x+y}) = h^{x+y} = h^x h^y = f(g^x)f(g^y)$
2) $f(sg^x g^y) = f(sg^{x+y}) = th^{x+y+c} = th^{x+c}h^y = f(sg^x)f(g^y)$
3) $f(g^x sg^y) = f(sg^{\mu x+y}) = th^{\mu x+y+c} = h^x th^{y+c} = f(g^x)f(sg^y)$
4) $f(sg^x sg^y) = f(g^{\beta_1+\mu x+y}) = h^{\beta_1+\mu x+y} = h^{\beta_2+c(\mu+1)+\mu x+y}$

$=\mathrm{h}^{\beta_2+\mu(x+c)+(y+c)} = th^{x+c}th^{y+c} = f(sg^x)f(sg^y)$.

Cette application est injective parce que $f(s^u g^x) = t^u h^{x+cu} = e \Rightarrow u = 0$, $x = 0 \Rightarrow s^u g^x = e$. En plus, elle est surjectif, puisque si on donne $t^v h^y \in H$, $f(s^v g^{y-cv}) = t^v h^{(y-cv)+cv} = t^v h^y$.

b) Supposons maintenant que les duplications soient isomorphes. Il y aura deux possibilités:

1) Si $Ind\,(\mu) = 1$, il n'existe pas que une classe, donc
$\beta_1 \equiv \beta_2\,(mod\ < \mu+1 >)$.

2) Si $Ind\,(\mu) = 2$, μ est pair et on vérifie que $\frac{n}{d} \notin < \mu+1 >$, avec $d = pgcd\,\{n, \mu+1\}$.

Maintenant, si les duplications sont dans différentes classes, l'une sera isomorphe a la duplication $(n, \mu, 0)$ et l'autre sera isomorphe à $(n, \mu, \frac{n}{d})$. De ça façon, on arriverait à que $(n, \mu, 0) \simeq (n, \mu, \frac{n}{d})$ et $Ind\,(\mu) = 2$, ce qui est contradictoire. □

Depuis ce théorème, chaque élément involutif peut induire une ou deux duplications, sauf isomorphisme, d'acord avec le valeur de sa indice.

3.6. Sur le plus grand ordre dans la classe $s < g >$

Proposition 9. *Dans le groupe* $G = (n, \mu, \beta) =< s, g >$, *on vérifie:* $ord\,(sg^x) = 2\,ord\,((sg)^2) = \frac{2n}{pgcd\,\{n, \beta+(\mu+1)x\}}$

Démonstration

L'indice du sous groupe $< g >$ dans G est 2. Donc, l'image de chaque élément sg^x par le homomorphism canonique $\pi : G \to G/ < g >$ sera la classe $s < g >$, qui a ordre 2 dans le groupe quotient. En consequence $2 \mid ord\,(sg^x)$. Ainsi, $ord\,((sg)^2) = \frac{ord\,(sg^x)}{pgcd\,\{ord\,(sg^x),2\}} = \frac{ord\,(sg^x)}{2} \Rightarrow ord\,(sg^x) = 2\,ord\,((sg^x)^2)$.

Maintenant, il suffit d'observer que $(sg^x)^2 = g^{\beta+(\mu+1)x}$ □

Proposition 10. *Soit* $d = pgcd\,\{n, \mu - 1\}$, *alors* $ord\,(sg^x) \mid 2d$. *En plus, si* $Ind\,(\mu) = 2$ *y* $\beta = 0$, *on a que* $ord(sg^x) \mid d$.

Démonstration

Puisque $(sg^x)^2 \in \mathcal{Z}(G)$, dont ordre est d, on vérifie que $ord\,((sg^x))^2 \mid d$. Alors $ord\,(sg^x) = 2\,ord((sg^x))^2 \mid 2d$.

D'autre part, si $Ind\,(\mu) = 2$ nous savons que $2n = d\,pgcd\{n, \mu + 1\}$. Si en plus, $\beta = 0$, $ord\,(sg^x) = 2\,ord\,((sg^x)^2) = 2\,ord\,(g^{(\mu+1)x}) \mid 2\,ord\,(g^{\mu+1}) = \frac{2n}{pgcd\,\{n,\mu+1\}} = d$.

De ça manière, $2d$ sera une cote supérieur des ordres des éléments qui appartient à la classe $s < g >$. Remarquez que cette cote se réduit à d, lorsque $\beta = 0$ et l'indice est 2. □

Si $Ind\,(\mu) = 1$, dans la classe $s < g >$, ils existent éléments à plus grand ordre égal $2d$. En effet, comme dans ce cas, nous pouvons prendre $\beta = 0$. Alors, il suffit de voir que sg vérifie:

$ord\,(sg) = 2\,ord\,((sg)^2) = 2\,ord\,(g^{\mu+1}) = \frac{2n}{pgcd\,\{n,\mu+1\}} = \frac{2d\,pgcd\,\{n,\mu+1\}}{\{pgcd\,\{n,\mu+1\}} = 2d$.

D'autre part, si $Ind\,(\mu) = 2$ et $G = (n, \mu, 0)$, ils existent éléments appartient à la classe $s < g >$, à plus grand ordre égal d. Il suffit de voir que sg vérifie:

$ord\,(sg) = \frac{2n}{pdcd\,\{n,\mu+1\}} = \frac{d\,pdcd\,\{n,\mu+1\}}{pdcd\,\{n,\mu+1\}} = d$

Finalement, si $Ind\,(\mu) = 2$ y $G = (n, \mu, \frac{n}{d})$, ils existent élément appartient à la classe $s < g >$, à plus grand ordre égal $2d$. En effet:

Il existe un entier c tel que $\mu + 1 = c\,(\frac{n}{d})$. Alors, en prenant l'élément sg^d, on a:

$ord\,(sg^d) = \frac{2n}{pgcd\,\{n,\beta+(\mu+1)d\}} = \frac{2n}{pgcd\,\{n,(\frac{n}{d})+(\frac{n}{d})\,cd\}} = \frac{2n}{(\frac{n}{d})\,pgcd\,\{d,1+cd\}} = \frac{2d}{pgcd\,\{d,1+cd\}} = \frac{2d}{pgcd\,\{d,1\}} = 2d$

3.7. Les élément d'ordre n dans la classe $s < g >$

Soit G une duplication de Type (n, μ, β). Nous voulons chercher les conditions pour n, μ et β, de faćcon qu'ils existent éléments sg^x, avec $0 \leq x \leq n-1$, tels que leurs ordres dans G soient égals n.

Il y a une caractérisation inmmédiate:
Si $ord\,(sg^x) = \frac{2n}{pgcd\,\{n,\beta+(\mu+1)x\}}$ on aura, $ord\,(sg^x) = n \Leftrightarrow$
$pgcd\,\{n, \beta + (\mu+1)\,x\}) = 2$.

Proposition 11. *Si dans* $G =< s, g >= (n, \mu, \beta)$ *il existe un élément* sg^x *avec ordre* n*, alors* n *est pair et* μ *prend les valeurs* 1 *ou* $(\frac{n}{2}) + 1$.

Démonstration

D'après la denière condition, on conclut que l'entier n est pair. Alors μ, qui doit être prime avec n, il sera impaire et aussi $\mu+1$ et $(\mu+1)x$ seront pairs. En consequence, β aussi sera pair. Si nous posons $\beta + (\mu+1)x = y$, la condition d'avant, se tournera à $pgcd\,\{\frac{n}{2}, y\} = 1$.

Comme β et $\mu+1$ sont solutions de l'écuation $(\mu-1)\xi \equiv 0\,(mod\ n)$, $2y$ aussi sera solutions.

Maintenant, $(\mu-1)(2y) \equiv 0\,(mod\ n) \Rightarrow (\mu-1)y \equiv 0\,(mod\ \frac{n}{2}) \Rightarrow \mu-1 \equiv 0\,(mod\ \frac{n}{2})$, puisque $pgcd\,\{y, \frac{n}{2}\} = 1$. Cette condition est verifiée seulement par les valeurs $\mu = 1$ et $\mu = \frac{n}{2} + 1$. □

Le valeur 1 est toujours involutif et on a le résultat suivant:

Proposition 12. *Si* n *est pair dans le groupe* $(n, 1, 1) \cong \mathcal{C}_2 \times \mathcal{C}_n$ *on a que* $ord\,(sg^x) = n \Leftrightarrow pgcd\,\{\frac{n}{2}, x\} = 1$.

Au contraire, dans le groupe $(n, 1, 1) \cong \mathcal{C}_{2n}$*, la classe* $s < g >$ *n'a pas des éléments d'ordre* n.

Démonstration

Si n est par, nous savons que $Ind\,(1) = 2$ et dans touts les deux groupes on a que $d = pgcd\,\{n, 0\} = n$.

1) Dans le cas $(n, 1, 0)$, le plus grand ordre possible des élément appartenant à la classe $s < g >$ est $d = n$ et on a:
$ord\,(sg^x) = n \Leftrightarrow pcgd\,\{n, \beta+(\mu+1)x\} = 2 \Leftrightarrow pgcd\,\{n, 2x\} = 2\,pgcd\,\{\frac{n}{2}, x\} = 1$

2) Dans le cas $(1,1,1)$, le plus grand ordre est $2d = 2n$ en ayant cet ordre l'élément $sg^d = sg^n = s$. Alors, les éléments du groupe avec ordre n sont touts dans le sous-groupe $< s^2 > \subset < g >$ et de ça façon, il n'y a aucunne dans la classe $s < g >$. □

Le valeur $\mu = \frac{n}{2} + 1$ sera ou non involutif, d'accord à le suivant proposition.

Proposition 13. *Soit n un entier pair. Le nombre $\mu = \frac{n}{2} + 1$ est involutif, module n, si et seulement s'il est multiple de 4.*

Démonstration

a) Si $n = 4q$, il est claire que $(\frac{n}{2} + 1)^2 - 1 = 4q^2 + 4q = 4q(q+1) \equiv 0\,(mod\ 4q) = n$

b) Soit $n = 2c$ et supposons que $\frac{n}{2}$ est involutif, module n. Alors $(\frac{n}{2})^2 - 1 = c^2 + 2c \equiv c^2 \equiv 0\,(mod\ 2c) = n$, ce qui n'est pas possible avec c impair. Comme n est pair, alors il est multiple de 4. □

Pour trouver les possibles élément d'ordre n, nous distinguerons deus cas:

Proposition 14. *Si $n = 4p$ avec p un nombre impair alors, dans le groupe $(4p, 2p+1, 0)$ la classe $s < g >$ n'a pas d'éléments d'ordre n. Au contraire, dans le groupe $(4p, 2p+1, 2)$ on a, $ord\,(sg^x) = n \Leftrightarrow pgcd\,\{\frac{n}{4}, 1+x\} = 1$.*

Démonstration

1) Dans le cas $(4p, 2p+1, 0)$, le plus grand ordre possible pour un élément appartenant à la classe $s < g >$ est $d = 2p$. Donc, il n'existeront pas d'élément d'ordre $n = 4p$ dans $s < g >$.

2) Pour le cas $(4p, 2p+1, 2)$, le plus grand ordre est $2d = n$ et l'élément $sg^d = sg^{2p}$ a cet ordre. De maniére plus generale on aura, $ord\,(sg^x) = n \Leftrightarrow pgcd\,\{n, \beta + (\mu+1)x\} = 2 \Leftrightarrow pgcd\,\{4p, 2 + (2p+2)x\} = 2 \Leftrightarrow$
$pgcd\,\{2, 1 + (p+1)x\} = 1$, cette condition est equivalent à $pgcd\,\{p, 1 + (p+1)x\} = 1$.

D'autre part, $1 + (p+1)x = px + (1+x) \equiv 1 + x\,(mod\ p)$, donc
$pgcd\,\{p, 1 + (p+1)x\} = pgcd\,\{p, 1+x\}$. Ainsi, nous pouvons concluire que $ord\,(sg^x) = n \Leftrightarrow pgcd\,\{p, 1+x\} = 1$.

□

Proposition 15. *Si $n = 2^m p$, avec $m \geq 3$ et p un entier impair, alors dans le groupe $(2^m p, 2^{m-1}p + 1, 0)$ on vérifie, $ord\,(sg^x) = n \Leftrightarrow pgcd\,\{\frac{n}{2}, x\} = 1$.*

Démonstration

Maintenant $Ind\left(\left(\frac{n}{2}\right)+1\right)=1$, donc nous pouvons prendre $\beta=0$ et on aura $d=pgcd\left\{n,\frac{n}{2}\right\}=\frac{n}{2}=2^{m-1}p$. Le plus grand ordre sera $2d=n$ et cet ordre l'aura l'élément sg. De maniére plus generale,
$ord\left(sg^x\right)=n \Leftrightarrow pgcd\left\{n,\beta+(\mu+1)x\right\}=2 \Leftrightarrow pgcd\left\{2^m p,(2^{m-1}p+2)x\right\}=2 \Leftrightarrow pgcd\left\{2^{m-1},(2^{m-2}p+1)x\right\}=1$.

Comme $pgcd\left\{2^{m-1}p,2^{m-2}p+1\right\}=pgcd\left\{2^{m-2}p+1,2^{m-2}p-1\right\}=pgcd\left\{2^{m-2}p,2\right\}=1$, finalement on aura que
$ord\left(sg^x\right)=n \Leftrightarrow pgcd\left\{2^{m-1}p,x\right\}=1$ □

3.8. Duplications isomorphes

Proposition 16. *Considérons un entier $n\geq 3$ et soient:*
μ_1 et μ_2 deux solutions pour l'écuation $\xi^2\equiv 0\,(mod\ n)$
β_1 une solution pour l'écuation $(\mu_1-1)\,\xi\equiv 0\,(mod\ n)$
β_2 une solution pour l'écuation $(\mu_2-1)\,\xi\equiv 0\,(mod\ n)$
Alors, $(n,\mu_1,\beta_1)\simeq(n,\mu_2,\beta_2)\Rightarrow\mu_1=\mu_2$.

Démonstration

Considérons les groupes d'ordre $2n$,
$G=<s,g>$, $ord\,(g)=n$, $s\notin<g>$, $s^{-1}gs=g^{\mu_1}$, $s^2=g^{\beta_1}$
$H=<t,h>$, $ord\,(h)=n$, $t\notin<h>$, $t^{-1}ht=h^{\mu_2}$, $t^2=h^{\beta_2}$
et supposons qu'il existe un isomorphism $\varphi:G\to H$.
Nous distinguerons deux possibilités:
a) Si $\varphi(g)\in<h>$, c'est-à-dire $\varphi(g)=h^x$
Dans ce cas, $\varphi(s)\in t<h>$, puisque au contraire $\varphi(G)\subset<h>\leq H$, ce qui est contradictoire.
Comme l'ordre de $\varphi(g)$ doit être n, alors le $pgcd\left\{x,n\right\}=1$.
Si nous supposons $\mu_1\geq\mu_2$, on a:
$\varphi(s^{-1}gs)=\varphi(g^{\mu_1})=\varphi(g)^{\mu_1}=(h^x)^{\mu_1}=h^{x\mu_1}=\varphi(s^{-1})\varphi(g)\varphi(s)=\varphi(s)^{-1}h^x\varphi(s)=h^{x\mu_2}\Rightarrow h^{x\mu_1}=h^{x\mu_2}\Rightarrow h^{x(\mu_1-\mu_2)}=e\Rightarrow x(\mu_1-\mu_2)\equiv 0\,(mod\ n)\Rightarrow$
$\Rightarrow(\mu_1-\mu_2)\equiv 0\,(mod\ n)\Rightarrow\mu_1-\mu_2=0$, puisque l'élément x a inverse dans $\mathbf{Z}/n\mathbf{Z}$ et $0\leq\mu_1-\mu_2<n$.

b) Si $\varphi(g)\in t<h>$, c'est-à-dire $\varphi(g)=th^x$.
Soit $\varphi(s)=t^v h^y$, ou $v=0,1$. Comme $\varphi(g)\in t<h>$, nous avons que n est pair et nous pouvons êcrire $n=2^m p$ ou $n\geq 1$ et p impair, avec une des deux suivants possibilites:
1) $\mu_2=1$.

Dans ce cas, le groupe H est abelienne, donc G est aussi abelienne. En consequence $\mu_1 = \mu_2$

2) $\mu_2 = \frac{n}{2} + 1 = 2^{m-1}p + 1$

Dans ce cas, il faut que $m \geq 2$. En étant $q = \frac{(\mu-1)}{2}$, nous aurons:

2a) Si $m = 2$, on peut prendre $\beta_2 = 2$ et il faut que $pgcd\{p, x+1\} = 1$. Alors, $\varphi(s^{-1}gs) = \varphi(g^{\mu_1}) = \varphi(g)^{\mu_1} = th^x((th^x)^2)^q = th^x(h^{\beta_2+(\mu_2+1)x})^q = \varphi(s^{-1})\varphi(g)\varphi(s) = \varphi(s^{-1})th^x\varphi(s) = (t^v h^y)^{-1}th^x(t^v h^y) = h^{-y}t^{-v}th^x t^v h^y =$

$$= \begin{cases} h^{-y}th^x h^y & \text{si } v = 0 \\ h^{-y}h^x th^y & \text{si } v = 1 \end{cases} = \begin{cases} th^{-y\mu_2}h^x h^y & \text{si } v = 0 \\ th^{(-y+x)\mu_2}h^y & \text{si } v = 1 \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} (h^{\beta_2+(\mu_2+1)x})^q = h^{-y\mu_2}h^y & \text{si } v = 0 \\ (h^{\beta_2+(\mu_2+1)x})^q = h^{(-y+x)\mu_2}h^y & \text{si } v = 1 \end{cases} \Rightarrow$$

$$\Rightarrow (h^{\beta_2+(\mu_2+1)x})^q = \begin{cases} h^{-y(\mu_2-1)} & \text{si } v = 0 \\ h^{(x-y)(\mu_2-1)} & \text{si } v = 1 \end{cases} \Rightarrow$$

$$\Rightarrow (\beta_2 + (\mu_2+1)x)q = (\beta_2 + (\tfrac{n}{2}+2)x)q \equiv$$

$$\equiv \begin{cases} -y(\mu_2-1) = -y\frac{n}{2} & \text{si } v = 0 \\ (x-y)(\mu_2-1) = (x-y)\frac{n}{2} & \text{si } v = 1 \end{cases} \Rightarrow (\beta_2 + 2x)q \equiv 0 \ (mod \tfrac{n}{2}).$$

2a) Si $m = 2$, on peut prendre β_2 et il faut que $pgcd\{p, x+1\} = 1$. Alors, $(2+2x)q = 2(1+x)q = (1+x)(\mu_1 - 1) \equiv 0\,(mod\ 2p) \Rightarrow$

$\Rightarrow (1+x)(\mu_1 - 1) \equiv 0\,(mod\ p) \Rightarrow \mu_1 - 1 \equiv 0\,(mod\ p) \Rightarrow$

$\Rightarrow \mu_1 = 1, p+1, 2p+1, 3p+1.$

De ces valeurs, nous éliminons l'entier 1, parce que nous sommes dans le cas non commutatif et aussi les entiers $p+1$ et $3p+1$, parce que μ_1 est impair. Ainsi, $\mu_1 = 2p + 1 = \mu_2$.

2b) Si $m \geq 3$, alors on peut prendre $\beta_2 = 0$ et il faut que $pgcd\{2^{m-1}p, x\} = 1$. Alors, $2xq = x(\mu_1 - 1) \equiv 0\,(mod\ 2^{m-1}p) \Rightarrow (\mu_1 - 1) \equiv 0\,(mod\ 2^{m-1}p) \Rightarrow \mu_1 = 1, 2^{m-1}p + 1$.

Nous éliminons le cas 1, donc $\mu_1 = 2^{m-1}p + 1 = \mu_2$. □

D'après la derniére proposition et la proposition 8, nous pouvons êcrire.

Proposition 17. *Considérons un entier $n \geq 3$ et soient:*
μ_1 et μ_2 deux solutions pour l'écuation $\xi^2 \equiv 0\,(mod\ n)$
β_1 une solution pour l'écuation $(\mu_1 - 1)\,\xi \equiv 0\,(mod\ n)$
β_2 une solution pour l'écuation $(\mu_2 - 1)\,\xi \equiv 0\,(mod\ n)$
Alors, $(n\mu_1, \beta_1) \simeq (n\mu_2, \beta_2) \Leftrightarrow \mu_1 = \mu_2, \quad \beta_1 \equiv \beta_2\,(mod\ < \mu_1 + 1 >)$.

3.9. Une formule pour l'indicateur de duplication$\mathcal{D}p\,(n)$

Pour chaque entier prime p nous définisson leur longueur prime impair ($lpi\,(p)$), comme la quantité des facteurs primes impairs qu'il y a dans la déscomposition du nombre p.

D'autre part, nous noterons i(n), comme le quantité d'élément involutif dans $\mathbf{Z}/n\mathbf{Z}$ (voir apendice)

Proposition 18. *Si $n = 2^m p$, avec $m \geq 0$ et p un entier impair, on vérifie:*

$$\mathcal{D}p\,(2^m p) = \begin{cases} 1 \cdot 2^{lpi\,(p)} & si\ m = 0 \\ 2 \cdot 2^{lpi\,(p)} & si\ m = 1 \\ 4 \cdot 2^{lpi\,(p)} & si\ m = 2 \\ 6 \cdot 2^{lpi\,(p)} & si\ m \geq 3 \end{cases}$$

Démonstration

1) Si $m = 0$, nous avons un entier impair. Si $p = 1$, le sujet est trivial, $\mathcal{D}p\,(1) = 1$. Si $p \geq 3$, touts les éléments involutifs auront indice 1, donc $\mathcal{D}p\,(p) = i(p) = 1 \cdot 2^{lpi\,(p)}$.

2) Si $m = 1$, les élément involutifs auront indice 2, donc $\mathcal{D}p\,(2p) = 2\,i(2p) = 2 \cdot 2^{lpi\,(p)}$.

3) Si $m = 2$, les élément involutifs auront indice 2, donc $\mathcal{D}p\,(4p) = 2\,i(4p) = 4 \cdot 2^{lpi\,(p)}$.

4) Pour le cas generale $m \geq 3$, nous savons que une moitié des élément ivolutifs ont indice 2, et l'autre moitié, ils ont indice 1. En consequence, $\mathcal{D}p\,(2^m p) = 2\,\frac{i(2^m p)}{2} + \frac{i(2^m p)}{2} = 3\,\frac{i(2^m p)}{2} = 6 \cdot 2^{lpi\,(p)}$ □

4. Modèles pour quelques duplications

4.1. Des Groupes qui s'expriment de Façon naturel comment duplications

Nous donnons en ce qu'il suit, six familles de groupes classiques, qui s'expriment comment duplications. En le suivant écarté, nous utiliserons ces modèles classiques, pour conaître la structure d'autres duplications plus générales, dans lesquelles, elles seront facteurs directes ou semi-directes.

4.2. Groupe produit $\mathcal{C}_2 \times \mathcal{C}_n$

Ils sont les groupes $G = \{e, g, g^2, ..., g^{n-1}; s, sg, sg^2, .., sg^{n-1}\}$ d'ordre $2n$ généres par les élément s y g tels que $ord\,(g) = n$, $s \notin < g >$, $s^2 = e$, $s^{-1}gs = g$.

C'est-à-dire, il s'agit de duplications du type $(n, 1, 0)$. Ces duplications peuvent apparaître pour n pair ou impair.

4.3. Groupes cycliques $\mathcal{C}_{2n}$ d'ordre pair

Si dans un groupe cyclique $G =< a >$ d'ordre $2n$, nous faisons remarquer, les élément $s = a$ et $g = a^2$, nous avons que $ord\,(g) = n$, $s \notin < g >$, $s^2 = g$, $s^{-1}gs = g$, ce qui interpréte les duplications du type $(n, 1, 1)$, valables seulement pour n pair.

Si n est puissance de deux, ces groupes ne peuvent pas se décomposer comment produits ni directes ni semi-directes de sous-groupes propres.

4.4. Groupes diedriques

Soit $n \geq 1$ un entier. On définit le groupe diedrique de degré n et on note $\mathcal{D}_n$, au groupe $G = \{e, g, g^2, ..., g^{n-1}; s, sg, sg^2, ..., sg^{n-1}\}$ d'ordre $2n$, généré par les élément s y g tels que $ord\,(g) = n$, $s \notin < g >$, $s^2 = e$, $s^{-1}gs = g^{n-1}$.

Il s'agit d'une duplication de type $(n, n-1, 0)$, valables pour toute n.

Pour les valeurs $n = 1, 2$ nous avons les groupes commutatifs $\mathcal{D}_1 = \{e, s\} \simeq \mathcal{C}_2$, $\mathcal{D}_2 = (2, 1, 0) \simeq \mathcal{C}_2 \times \mathcal{C}_2$.

Touts les autres ne seront pas commutatifs, puisque si $n \geq 3$ $(n-1 \neq 1)$ on a:

$$d = pgcd\,\{n, n-2\} = \begin{cases} 1 & \text{si } n \text{ est impair} \\ 2 & \text{si } n \text{ est pair} \end{cases}$$

$$\Rightarrow \mathcal{Z}(\mathcal{D}_n) = \begin{cases} < e > & \text{si } n \text{ est impair} \\ < g^{\frac{n}{2}} > & \text{si } n \text{ est pair} \end{cases}$$

En tel cas $(n \geq 3)$, il s'agit du classique groupe de mouvement du polygone régulier de n côtés.

4.5. Groupes dicycliques

Soit $n \geq 1$ un entier. On définit le groupe dyclique de degré n et on note $\mathcal{DC}_n$, au groupe $G = \{e, g, g^2, ..., g^{2n-1}; s, sg, sg^2, ..., sg^{2n-1}\}$ d'ordre $4n$, généré par les élément s y g tels que $ord\,(g) = 2n$, $s \notin < g >$, $s^2 = g^n$, $s^{-1}gs = g^{2n-1}$.

Il s'agit d'une duplication de type $(2n, 2n-1, n)$, valables seulement pour modules pairs.

Lorsque $n = 1$ il s'agit de la duplication commutative $\mathcal{DC}_1 = (2, 1, 1) \simeq \mathcal{C}_4$. Il n'y a plus. Pour $n \geq 2$ $(2n-1 \neq 1)$, on a que $d = pgcd\{2n, 2n-2\} = 2\,pgcd\{n, n-1\} = 2 \Rightarrow \mathcal{Z}(G) =< g^n >$.

Le nom ciclyque est pris de Ledermann. Lorsque $n = 2$, nous avons le groupe quaternio de Hamilton. Quelques auteurs (Gorestein, Robinson, Suzuki, etc,..) parlent de groupes de quaternions généralises pour les groupes dicycliques de degré $n = 2^m$, c'est-à- dire, pour les groupes dicycliques qui soient 2-groupes. De la mème façon que avec les groupes cycliques d'ordre puisance de 2, le groupe $\mathcal{DC}_n$ $(n = 2^m\ m \geq 1)$ ne peut pas se decomposer, ni directe ni semi-directement en sous-groupes propres. En effet:

Comme $\mu = 2n-1$ et $\beta = n$, pour tout $x \in [0, n-1]$ on vérifie que $(sg^x)^2 = g^{\beta+(\mu+1)x} = g^n \Rightarrow g^n = g^{2^m} \in < sg^x >$.

Le groupe $< g >$ a ordre 2^{m+1} et la relation completète de ses sous-groupes est la suivante:

$\{e\} \subset < g^{2^m} > \subset < g^{2m-1} > \subset \ldots \subset < g^2 > \subset < g >$.

Maintenant, il est claire que $g^{2^m} \in < g^x >$, $\forall x \in [1, n-1]$. De ça façon, l'élément g^{2^m} est dans tout sous-groupe non trivial et si M et N sont deux sous-groupes propres, alors $M \cap N \neq \{e\}$, et en consequence, il n'est pas possible des décompositions directes ou semi-directes.

4.6. Groupes semi-diedriques

Soit $n \geq 3$ un entier. On définit le groupe semi-diedrique de degré n et on note $\mathcal{SD}_n$, au groupe $G = \{e, g, g^2, ..., g^{2^{n-1}-1}; s, sg, sg^2, ..., sg^{2^{n-1}-1}\}$ d'ordre 2^n, généré par les élément s y g tels que $ord\,(g) = 2^{n-1}$, $s \notin < g >$, $ord\,(s) = 2$, $s^{-1}gs = g^{2n-1-1}$.

Il s'agit d'une duplication de type $(2^{n-1}, 2^{n-2}-1, 0)$.

Pour le valeur $n = 3$ on a le groupe commutatif $\mathcal{SD}_3 = (4, 1, 0) \simeq \mathcal{C}_2 \times \mathcal{C}_4$.

Il n'y a plus, puisque si $n \geq 4$ $(2^{n-2}-1 \neq 1)$, nous avons que

$d = pgcd\{2^{n-2}-2, 2^{n-1}) = 2\,pgcd\{2^{n-3}-1, 2^{n-2}\} = 2 \Rightarrow \mathcal{Z}(g) =< g^{2^{n-2}} >$.

Ces groupes sont aussi 2-groupes.

4.7. Groupes semi-cycliques

Soit $n \geq 2$ un entier. On définit le groupe semi-cyclique de degré n et on note $\mathcal{SC}_n$, au groupe $G = \{e, g, g^2, ..., g^{2^{n-1}-1}; s, sg, sg^2, ..., sg^{2^{n-1}-1}\}$

d'ordre 2^n, généré par les élément s y g tels que $ord\,(g) = 2^{n-1}$, $s \notin < g >$, $ord\,(s) = 2$, $s^{-1}gs = g^{2^{n-2}+1}$.

Il s'agit d'une duplication de type $(2^{n-1}, 2^{n-2} + 1, 0)$.

Pour le valeur $n = 2$ on a le groupe commutatif $\mathcal{SC}_2 = (2, 1, 0) \simeq \mathcal{C}_2 \times \mathcal{C}_2$.

Il n'y a plus, puisque si $n \geq 3$ $(2^{n-2} + 1 \neq 1)$, nous avons que $d = pgcd\,\{2^{n-1}, 2^{n-2}\} = 2^{n-2} pgcd\,\{2, 1\} = 2^{n-2} \Rightarrow \mathcal{Z}(G) =< g^2 >$.

Remarquez que pour $n = 3$ on a $\mathcal{SC}_3 = (4, 3, 0) \simeq \mathcal{D}_4$. Autre foi, ces groupes seront 2-groupes.

4.8. Modèles pour les duplications avec $n = 2^m$

Nous montrerons que toute duplications de type $(2^m, \mu, \beta)$ est une de les précedéntes:

1) $m = 0$

Il n'y a pas d'élément involutifs, mais si aura une duplications, le groupe $\mathcal{C}_2$

2) $m = 1$

Le nombre $\mu = 1$ est involutif avec indice 2. Les duplications seront: $(2, 1, 0) \simeq \mathcal{C}_2 \times \mathcal{C}_2$ et $(2, 1, 1) \simeq \mathcal{C}_4$.

3) $m = 2$

Il y a deux élément involutif $\mu = 1, 3$, tout les deux avec indice 2 et duplications: $(4, 1, 0) \simeq \mathcal{C}_2 \times \mathcal{C}_4$, $(4, 1, 1) \simeq \mathcal{C}_8$, $(4, 3, 0) \simeq \mathcal{D}_4$ et $(4, 3, 2) \simeq \mathcal{DC}_2$.

4) $m \geq 3$

Les entiers $\mu = 1, 2^m - 1$ sont involutifs avec indice 2 et duplications: $(2^m, 1, 0) \simeq \mathcal{C}_2 \times \mathcal{C}_{2^m}$, $(2^m, 1, 1) \simeq \mathcal{C}_{2^{m+1}}$, $(2^m, 2^m - 1, 0) \simeq \mathcal{D}_{2^m}$,
$(2^m, 2^m - 1, 2^{m-1}) \simeq \mathcal{DC}_{2^{m-1}}$,
et les nombres $\mu = 2^{m-1} - 1, 2^{m-1} + 1$ sont involutif, avec indice 1 et duplications: $(2^m, 2^{m-1} - 1, 0) \simeq \mathcal{SD}_{m+1}$ et $(2^m, 2^{m-1} + 1, 0) \simeq \mathcal{SC}_{m+1}$.

5. Sur la structure d'une duplication

5.1. Décomposition semi-directe d'une duplication

Pour toute duplication $g = (n, \mu, \beta)$, on a que $G =< g >< s >= \{g^x s^y : x, y \in \mathbf{Z}\}$, ou $< g >$ est normal dans G. Si $\beta \in < \mu + 1 >$, en changant s , par un autre élément adéquat de la classe $s < g >$, nous pouvons

supposer $\beta = 0$ et alors $< s > \cap < g >= \{e\}$. De ça façon nous avons la decomposition:

$$G =< s > \Big[< g >\Big] \simeq \mathcal{C}_2 \times \mathcal{C}_n$$

Où, $< s > \Big[< g >\Big]$ note le produit semi-direct de les sous-groupes.

Il y a une autre décomposition valable pour toute β. Nous utiliseront la décomposition du nombre n en ses facteurs pairs et impairs.

Proposition 19. *Supposons que $n = 2^m p$, avec $m \geq 0$ et p impair.*

Donnée une duplication $G =< s, g >= (2^m p, \mu, \beta)$, soient $\gamma \equiv \mu \, (mod \; 2^m)$ et $\rho \equiv \beta \, (mod \; 2^m)$. Alors on a une décomposition semi-directe

$(2^m p, \mu, \beta) = H\Big[K\Big]$, ou $H =< s^p g^p >= (2^m, \gamma, p)$, $K =< g^{2^m} > \simeq \mathcal{C}_p$

La décomposition est directe si et seulement si $\mu \equiv 1 \, (mod \; p)$.

Démonstration

Soient les élément $t = s^p$, $h = g^p$, $k = g^{2^m}$

Les sous-groupes cycliques $< h >$ et $< k >$ sont normals dans G. En plus,

$ord\,(h) = ord\,(g^p) = \frac{n}{p} = 2^m$ et $ord\,(k) = ord(g^{2^m}) = \frac{n}{2^m} = p$

1) Soit $H =< t >< h >$. Comme $< h >$ est normal, l'ensemble h sera un sous-groupe de G. En plus comme p est impair, on a

$t = s^p \in s < g >\Rightarrow t \notin< g >\Rightarrow t \notin< h >$

Pendant que, $t^2 = (s^p)^2 = (s^2)^p = (g^\beta)^p = (g^p)^\beta = h^\beta = h^\rho \in< h >$.

En consequence, les puissances impairs de t, ne sont pas dans $< h >$, mais les pair si les sont. Ainsi, l'entier t sera pair et on vérifie:

$$ord\,(H) = ord\,(< t >< h >) = \frac{ord\,(< t >)\, ord\,(< h >)}{ord\,(< t > \cap < h >)}$$

$$= 2\, ord\,(< h >) = 2^{m+1}.$$

Finalement, comme $t \in< g >$ et $h \in< g >$, on a que $t^{-1}ht = h^\mu = h^\gamma$ et en consequence $H =< t, h >= (2^m, \gamma, p)$.

2) Nous savons que $K =< k >$ est normal, en plus comme son ordre est p, on aura que $K \simeq \mathcal{C}_p$.

Comme les ordres respectifs 2^{m+1} et p de H et K sont primes, on aura que $H \cap K = \{e\}$

4) Par tout ça d'avant, on peut écrire que $ord\,(H\,K) = ord\,(H)\, ord\,(K) = 2^{m+1}p = ord\,(G) \Rightarrow G = H\,K$.

Ainsi, nous avons que $G = H\Big[K\Big]$.

D'autre part, cette décomposition sera directe si et seulement si h et K commutent élément par élément. Comme $h, k \in < g >$, l'affirmation d'avant est equivalent à que $tk = kt$ ou que $k \in \mathcal{Z}(G)$. Alors:

a) Si $\mu = 1\,(mod\ p)$, il existe c tel que $\mu = pc + 1$ et on a, $(\mu - 1)2^m = (pc)\,2^m = (2^m p)\,c = nc \equiv 0\,(mod\ n)$.

Donc, $k = g^{2^m} \in \mathcal{Z}(g)$

b) Si $k \in \mathcal{Z}(g)$, alors $(\mu - 1)\,2^m \equiv 0\,(mod\ 2^m p) \Rightarrow (\mu - 1) \equiv 0\,(mod\ p) \Rightarrow \mu \equiv 1\,(mod\ p)$.

Notons que nous avons exclu la possibilité $p = 1$, puisque $\mathcal{C}_p = \{e\}$ et la décomposition $G = H$ serait trivial. □

Par rapport à les facteurs d'une duplications, le facteur normal K est un groupe cyclique d'ordre impair et en consequence il pourra s'ècrire comment produit de groupes cycliques d'ordres puisances de primes impairs.

D'autre part, le facteur H, il sera un 2-sous-groupe de Sylow dans G, dont structure nous établiront dans les trois suivantes propositions.

Proposition 20. *Pour toute duplication* $G =< s, g >= (2^m p, \mu, 0)$ $m \geq 1$, *le sous-groupe* $H =< s^p, g^p >= (2^m, \gamma, 0)$ *vérifie:*

$H =< S > \left[< g^p >\right]$, *avec* $< s > \simeq \mathcal{C}_2$, $< g^p > \simeq \mathcal{C}_{2^m}$

Cette décomposition sera directe si et seulement si $\mu \equiv 1\,(mod\ 2^m)$.

Démonstration

Comme p est impair et $s^2 = e$, on a que $t = s^p = s$ et on vérifie que $< s > \cap < g^p >= \{e\}$.

Nous savons que $H =< s >< g^p >$ et que $< g^p >$ est normal, donc $H =< s > \left[< g^p >\right]$. Cette décomposition sera directe si et seulement si $sh = hs$ (h soit central). Alors:

a) Si $\mu = 2^m c + 1$ ou $c \in \mathbf{Z}$, on a que $(\mu - 1)p = (2^m c)p = (2^m p)c = nc \equiv 0\,(mod\ n)$. D'ou $h = g^p$ est central.

b) Si h est central on vérifie que $(\mu - 1)p \equiv 0\,(mod\ 2^m p) \Rightarrow \mu - 1 \equiv 0\,(mod\ 2^m) \Rightarrow \mu \equiv 1\,(mod\ 2^m$.

Nous avons exclu, la possibilité $m = 0$, puisque $\mathcal{C}_{2^m} = \{e\}$ implique que la décomposition $H =< s >$ soit trivial.

D'autre part, si $\mu \equiv 2^m - 1\,(mod\ 2^m)$, alors H est le groupe diedrique $\mathcal{D}_{2^m}$. □

Proposition 21. *Soit* $n = 2^m p$ *avec* $m \geq 1$. *Soit* μ *un élément involutif module* n, *et soit* $d = pgcd\,\{n, \mu - 1\}$. *Supposons que* $ind\,(\mu) = 2$ *et que* $\mu \equiv 1\,(mod\ 2^m)$. *Alors, dans* $G =< s, g >= (2^m p, \mu, 2^m \frac{p}{d})$ *on vérifie:*

$H =< s^p, s^p >=< s^p >\simeq \mathcal{C}_{2^{m+1}} \simeq (2^m, 1, 1)$

Démonstration

Comme $\mu = 2^m a + 1$, on a que $d = pgcd\{2^m p, 2^m a\} = 2^m\, pgcd\{p, a\}$. Alors, le nombre $\frac{n}{d} = \frac{p}{m}\, pgcd\{p, a\}$ est impair et en consequence sera prime avec 2^m. Ainsi, en prenant $t = s^p$ et $h = g^p$ on a que $ord\,(t) = 2\, ord\,(h^{\frac{n}{d}}) = 2\, ord\,(h) = 2^{m+1} \Rightarrow H =< t >\simeq \mathcal{C}_{2^{m+1}}$. Comme $h \in H$, cet élément sera une puissance de t, dont exposant sera pair, puisque les puissances impairs de t seront dans $s < g >$. C'est-à-dire, il existera un entier b tel que $t^{2b} = h$. Alors,

$2^m = ord\,(h) = ord\,(t^{2b}) = \frac{2^{m+1}}{pgcd\{2^{m+1}, 2b\}} = \frac{2^m}{pgcd\{2^m, b\}} \Rightarrow pgcd\{2^{m+1}, b\} = 1 \Rightarrow < t^b >=< t >$

Si nous changeons t par t^b, comme $(t^b)^2 = h$, alors le sous-groupe H est représenté par la duplication canonique $(2^m, 1, 1)$. □

Proposition 22. *Soient $n = 2^m p$, $m \geq 1$, μ un élément involutif module n, et*
$d = pgcd\{n, \mu - 1\}$.

Supposons que $Ind\,(\mu) = 2$, et que $\mu \equiv 2^m - 1\,(mod\ 2^m)$. Alors, dans le groupe $g =< s, g >= (2^m p, \mu, 2^m \frac{p}{d})$ on vérifie:

$$H =< s^p, g^p >\simeq \mathcal{DC}_{2^{m-1}} \simeq (2^m, 2^m - 1, 2^{m-1})$$

Démonstration

Par hypothèse, il existera un entier a tel que $\mu = 2^m a + 2^m - 1$. De ça façon, $d = pgcd\{2^m p, 2^m a + 2^m - 2\} = 2\, pgcd\{2^{m-1} p, 2^{m-1} a + 2^{m-1} - 1\}$. Alors, $\frac{n}{d} = \frac{2^{m-1} p}{pgcd\{2^{m-1} p, 2^{m-1} a + 2^{m-1} - 1\}}$, òu $pgcd\{2^{m-1} p, 2^{m-1} a + 2^{m-1} - 1\}$, est impair, puisque $2^{m-1} a + 2^{m-1} - 1$ est impair, donc il est prime avec 2^{m-1} et en consequence il divisera à p. C'est-à-dire, le nombre $b = \frac{p}{pgcd\{2^{m-1} p, 2^{m-1} a + 2^{m-1} - 1\}}$ est un entier impair.

Si nous possons $b = 2c + 1$, $\frac{n}{d} = 2^{m-1} b = 2^{m-1}(2c + 1) = 2^m c + 2^{m-1} \Rightarrow \frac{n}{d} \equiv 2^{m-1}\,(mod\ 2^m)$. D'ou $H = (2^m, 2^m - 1, 2^{m-1}) \simeq \mathcal{DC}_{2^{m-1}}$. □

Remarquez, que pour chaque élément μ d'indice 1, il y a seulement la possibilité de la proposition 26, où le 2-sous-groupe de sylow on peut décomposer. Si μ a indice 2, pour la duplication avec $\beta = \frac{n}{d}$, ce sous-groupe de sylow est isomorph ou bien à $\mathcal{C}_{2^{m+1}}$, ou bien à $\mathcal{DC}_{2^{m-1}}$, en etant touts les deux cas, groupes indecomposables.

5.2. Décomposition selon le degré de parité de n

Possons $n = 2^m p$ avec p un entier impair. Nous dirons que l'exposante m est le degré de parité de n. En ce que suit, si nous faisons attention à la décomposition précédent, selon les valeurs de sa parité.

Pour ça, nous donnerons quelques indications:

a) Les cas pour $p = 1$ ont été deja étudies.

Nous supposons que $m \geq 3$. De ça façon, nous pouvons appliquer la proposition 25 et pour le sous-groupe normal K, nous aurons que $K \simeq \mathcal{C}_p$.

Remarquez aussi, que en générale la décomposition $G = H\Big[K\Big]$ sera directe si et seulement si $\mu \equiv 1\,(mod\ p)$.

b) D'abort, nous étudierons le cas $m = 0$. Pour les autres cas, nous pouvons utiliser les propositions 20, 21 ou 22.

c) Si $\beta = 0$, nous utiliserons la proposition 20 pour établir la décomposition du sous-groupe H, qui sera directe si et seulement si $\mu \equiv 1\,(mod\ 2^m)$. Dans cette supposition, observons que la décomposition de G soit aussi directe, est equivalent à $\mu = 1$.

d) Si $Ind\,(\mu) = 2$ et $\beta = \frac{n}{d}$, avec $d = pgcd\,\{n, \mu - 1\}$, nous savons que $H = (2^m, 1, 1) = \mathcal{C}_{2^{m+1}}$ pour $\mu \equiv 1\,(mod\ 2^m)$ (proposition 21), ou bien que $H = (2^m, 2^m - 1, 2^{m-1})$ si $\mu \equiv 2^m - 1\,(mod\ 2^m)$ (proposition 22).

cas 1: $m = o \Leftrightarrow n = p$

Comme p est impair, tout élément involutif avec indice 1, donc nous pouvons prendre $\beta = 0$. Alors, $t = s^p = s$, $h = g^p = e$, $k = g$. En consequent (proposition 19), nous avons, $H =< s >\simeq \mathcal{C}_2 \Rightarrow G \simeq \mathcal{C}_2 \times \mathcal{C}_p$.

Le seul cas de décomposition directe est pour $\mu = 1$ et alors $g \simeq \mathcal{C}_{2p}$. Pour $\mu = p - 1$ on a $G \simeq \mathcal{D}_n$.

cas 2: $m = 1 \Leftrightarrow n = 2p$

Tout élément involutif μ vérifie que $Ind\,(\mu) = 2$ et que $\mu \equiv 1\,(mod\ 2)$.

2a) $\beta = 0$

$$H = (2, 1, 0) \simeq \mathcal{C}_2 \times \mathcal{C}_2 \Rightarrow G \simeq (\mathcal{C}_2 \times \mathcal{C}_2) \times \mathcal{C}_p$$

2b) $\beta = \frac{n}{d}$

$$H = (2, 1, 1) \simeq \mathcal{C}_4 \Rightarrow G \simeq \mathcal{C}_4 \times \mathcal{C}_p$$

Si $\mu = 1$ (décomposition directe) on a $G \simeq \mathcal{C}_{4p}$.

cas 3: $m = 2 \Leftrightarrow n = 4p$

Tout élément involutif μ vérifie que $Ind\,(\mu) = 2$ et que $\mu \equiv 1, 3\,(mod\ 4)$.

3a) $\beta = 0$, $\mu \equiv 1\,(mod\ 4)$

$$H = (4,1,0) \simeq \mathcal{C}_2 \times \mathcal{C}_4 \Rightarrow G \simeq (\mathcal{C}_2 \times \mathcal{C}_4) \times \mathcal{C}_p$$

3b) $\beta = \frac{n}{d}$, $\mu \equiv 1\,(mod\ 4)$

$$H = (4,1,1) = \simeq \mathcal{C}_8 \Rightarrow G \simeq \mathcal{C}_8 \times \mathcal{C}_p$$

Si $\mu = 1$ (décomposition directe) on a $G \simeq \mathcal{C}_{8p}$.

3c) $\beta = 0$, $\mu \equiv 3\,(mod\ 4)$

$$H = (4,3,0) \simeq \mathcal{D}_4 \Rightarrow G \simeq \mathcal{D}_4 \times \mathcal{C}_p$$

3d) $\beta = \frac{n}{d}$, $\mu \equiv 3\,(mod\ 4)$

$$H = (4,3,2) \simeq \mathcal{DC}_2 \Rightarrow G \simeq \mathcal{DC}_2 \times \mathcal{C}_p$$

cas 4: $m \geq 3 \Leftrightarrow n = 2^m p$

Les éléments involutifs ont indice 2 si $\mu \equiv 1, 2^m - 1\,(mod\ 2^m)$ et ils ont indice 1 si $\mu \equiv 2^{m-1} - 1, 2^{m-1} + 1\,(mod\ 2^m)$.

4a) $\beta = 0$, $\mu \equiv 1\,(mod\ 2^m)$

$$H = (2^m,1,0) \simeq \mathcal{C}_2 \times \mathcal{C}_{2^m} \Rightarrow G \simeq (\mathcal{C}_2 \times \mathcal{C}_{2^m}) \times \mathcal{C}_p$$

4b) $\beta = \frac{n}{d}$, $\mu \equiv 1\,(mod\ 2^m)$

$$H = (2^m,1,1) \simeq \mathcal{C}_{2^{m+1}} \Rightarrow G \simeq \mathcal{C}_{2^{m+1}} \times \mathcal{C}_p$$

Si $\mu = 1$ (décomposition directe) on a que $G \simeq \mathcal{C}_{2^{m+1}p}$.

4c) $\beta = \frac{n}{d}$, $\mu \equiv 2^{m-1} - 1\,(mod\ 2^m)$

$$H = (2^m, 2^{m-1} - 1, 0) \simeq \mathcal{SD}_{m+1} \Rightarrow G \simeq \mathcal{SD}_{m+1} \times \mathcal{C}_p$$

4d) $\beta = \frac{n}{d}$, $\mu \equiv 2^{m-1} + 1\,(mod\ 2^m)$

$$H(2^m, 2^m + 1, 0) \simeq \mathcal{SC}_{m+1} \Rightarrow G \simeq \mathcal{SC}_{m+1} \times \mathcal{C}_p$$

4e) $\beta = 0$, $\mu \equiv 2^m - 1\,(mod 2^m)$

$$H = (2^m, 2^m - 1, 0) \simeq \mathcal{D}_{2^m} \Rightarrow \mathcal{D}_{2^m} \times \mathcal{C}_p$$

4f) $\beta = \frac{n}{d}$, $\mu \equiv 2^m - 1\,(mod\ 2^m)$

$$H = (2^m, 2^m - 1, 2^{m-1}) \simeq \mathcal{DC}_{2^{m-1}} \Rightarrow G \simeq \mathcal{DC}_{2^{m-1}} \times \mathcal{C}_p$$

5.3. Deuxième décomposition semi-directe

Lorsque nous pouvons prendre $\beta = 0$, on vérifie:

$G = \Big(< s > \Big[< g^p > \Big]\Big) \Big[< g^{2^m} >\Big] \simeq \Big(\mathcal{C}_2 \times \mathcal{C}_{2^m}\Big) \times \mathcal{C}_p$

Comme $< g^p >$ et $< g^{2^m} >$ sont touts les deux sous-groupes du groupe commutatif $< g >$, ceci nous suggére qu'ils pourraient s'echanger.

Proposition 23. *Supposons que $n = 2^m p$, avec $m \geq 1$ et $p \geq 3$ impair.*

Considérons une duplication $G =< s, g >= (2^m p, \mu, 0)$ et soit $\delta \equiv \mu \, (mod\ p)$. Alors, on aura une décomposition semi-directe

$(2^m p, \mu, 0) = M\Big[N\Big]$, *où* $M \simeq (p, \delta, 0) = s\Big[< g^{2^m} >\Big] \simeq \mathcal{C}_2 \times \mathcal{C}_p$, $n \simeq \mathcal{C}_{2^m}$.

La décomposition de M est directe si et seulement si $\mu \equiv 1 \, (mod\ p)$ et celle-là du groupe G sera directe si et seulement si $\mu \equiv 1 \, (mod\ 2^m)$.

Démonstration

Soient $t = s^p$, $h = g^p$ et $k = g^{2^m}$.

Nous savons que $< h >$ et $< k >$ sont normals dans G, que $ord\,(h) = 2^m$ et que $ord\,(k) = p$. En plus, comme p est impair et $s^2 = e$ on a que $t = s$.

1) Soit le sous-groupe $M =< s >< k >$. Comme $< s > \cap < k >= \{e\}$, $ord\,(M) = 2p$, et comme $t^{-1}kt = s^{-1}ks = k^\mu = k^\delta$ on a que

$M = (p, \delta, 0) =< s > \Big[< k >\Big] \simeq \mathcal{C}_2 \times \mathcal{C}_p$.

2) Si $N =< h >$, alors il est un sous-groupe normal isomorphe à $\mathcal{C}_{2^m}$.

3) Puisque $s < k > \subset s < g >$, aucun élément de la classe $s < k >$ peut appartenir à $< h >$ qui est un sous-groupe de $< g >$. Non plus, les éléments de $< k >$ (sauf le neutre), puisque $pgcd\,\{ord\,(h), ord\,(k)\} = 1$.

Finalement, comme $M =< k > \cup s < k >$ on a que $M \cap N = \{e\}$.

4) De tout ça d'avant on a que

$ord\,(MN) = ord\,(M)\, ord\,(N) = 2p2^m = ord\,(G) \Rightarrow G = MN$. D'où $G = M\Big[N\Big]$.

La décomposition $M =< s > \Big[< k >\Big]$ est directe (voir proposition 19) si et seulement si k est central, c'est-à-dire si $\mu \equiv 1 \, (mod p)$.

D'autre part, la décomposition $G = M\Big[N\Big]$ sera directe (voir proposition 20) si et seulement si h est central, c'est-à-dire, si $\mu \equiv 1 \, (mod\ 2^m)$. □

La décomposition $G \simeq (\mathcal{C}_2 \times \mathcal{C}_p) \times \mathcal{C}_{2^m}$ que nous avons obtenu, le même que la décomposition $G \simeq (\mathcal{C}_2 \times \mathcal{C}_{2^m}) \times \mathcal{C}_p$ dérivée des propositions 20 et 21, on reduit à $G \simeq \mathcal{C}_2 \times \mathcal{C}_{2^m}$ si $p = 1$ et $G \simeq \mathcal{C}_2 \times \mathcal{C}_p$ si $m = 0$.

Le facteur normal N, c'est un groupe cyclique indécomposable. Le sous-groupe M est une duplication du module impair p.

De maniére générale, seulement dans les cas $\mu = 1, p-1\,(mod\ p)$, nous pouvons expliciter des resultats:

$\mu \equiv 1\,(mod\ p) \Rightarrow M = (p, 1, 0) \simeq \mathcal{C}_2 \times \mathcal{C}_p \simeq \mathcal{C}_{2p} \Rightarrow G \simeq \mathcal{C}_{2p} \times \mathcal{C}_{2^m}$.

$\mu \equiv p-1\,(mod\ p) \Rightarrow M = (p, p-1, 0) \simeq \mathcal{D}_p \Rightarrow G \simeq \mathcal{D}_p \times \mathcal{C}_{2^m}$.

En étant ces dćompositions directes si et seulement si $\mu \equiv 1\,(mod\ 2^m)$.

6. Appendice : Groupes d'involutions

Par la relation qu'il y a, avec le sujet de ce travail, nous montrerons en suivant, quelques observations et petits résultats sur les sous-groupes multiplicatifs formés par les élément involutifs, dans les anneaux $\mathbf{Z}/n\mathbf{Z}$ pour $n \geq 2$.

Rappellerons, que l'ensemble d'éléments involutifs d'un anneau, forment un sous-groupe multiplicatif des unités du anneau. A l'avenir, nous noterons $\Im(n)$ au sous-groupe des éléments involutifs du anneaux $\mathbf{Z}/n\mathbf{Z}$.

Pour chaque $n \geq 2$, le groupe $\Im(n)$ est un groupe finite, où on vérifie l'écuation $x^2 = 1$, $\forall x \in \Im(n)$. Ainsi, d'après le théorème de Cauchy, le groupe $\Im(n)$ aura ordre une puisance de 2.

Si nous notons $\imath(n) = ord\,(\Im(n))$, nous avons que $\imath(n)$ divise au indicateur $\varphi(n)$ d'Euler. Remarquez, que si $\mu \in \Im(n)$, alors $n - \mu \in \Im(n)$. En consequence, il suffit de conaître la moitié des élément de $\Im(n)$, puisque le reste y seront leurs inverses.

D' autre part si $pgcd\,\{p, q\} = 1$, où $p, q \in I\!N$, du isomorphisme $\mathbf{Z}_{pq} \simeq \mathbf{Z}_p \times \mathbf{Z}_q$ on a que $\Im(pq) \simeq \Im(p) \times \Im(q)$, et en consequence $\imath(pq) = \imath(p)\imath(q)$.

Si nous posons chaque entier $n = 2^m p$, où $m \geq 0$ et p impair, il suffira de savoir calculer le groupe $\Im$ et la fonction $\imath$ pour les puissances 2^m et les primes p.

6.1. Calcul de $\Im(2^m)$ et $\imath(2^m)$, avec $m \geq 1$

Proposition 24. *Soit $n = 2^m$, avec $m \geq 3$, alors:*
$\Im(2^m) = \{1, 2^{m-1} - 1, 2^{m-1} + 1, 2^m - 1\}$.

Démonstration

Si $m = 3$, il est claire.

Supposons notre résultat vrai pour m.

Si $\mu \in [1, 2^{m+1} - 1]$ et $2^{m+1} \mid \mu^2 - 1$, alors aussi $2^m \mid \mu^2 - 1 \Leftrightarrow$ $\mu^2 - 1 \equiv 0\,(mod\ 2^m)$.

De ça façons, μ sera congruent module 2^m, ou bien avec 1, ou bien avec $2^{m-1}+1$, ou bien avec $2^{m-1}-1$, ou avec 2^m-1. Alors:

1) Si $\mu \equiv 1 \Rightarrow \exists c \in I\!N/\mu = 2^m c + 1$

2) Si $c \geq 2$ alors $\mu \notin [1, 2^{m+1}-1]$, donc $c = 0$, auquel cas $\mu = 1$, ou bien $c = 1$ et alors $\mu = 2^m + 1$

2) $\mu \equiv 2^{m-1} \mp 1 \Rightarrow \exists c \in I\!N/\mu = 2^m c + (2^{m-1} \mp 1)$, alors $\mu^2 - 1 \equiv 2^{2m}c^2 + 2^{m+1}c\,(2^{m-1} \pm 1) + 2^{2m-2} \mp 2^m = 2^{m+1}c \Rightarrow 2^m c^2 + 2c\,(2^{m-1} \pm 1) + 2^{m-2} \mp 1 = 2c$, ce qui est contradictoire, puisque comme $m \geq 3$, le premier côté est impair et le deuxième est pair.

3) $\mu = 2^m \Rightarrow \exists c \in I\!N/\mu = 2^m c + 2^m - 1$.

Si $c \geq 2$, alors $\mu \notin [1, 2^{m+1}-1]$, donc il faut que $c = 0$ auquel cas $\mu = 2^{m-1}$, où bien $c = 1$, ce qui implique $\mu = 2^{m+1} - 1$. □

Pour les premieres puissances, c'est immediate $\Im(2) = \{1\}$, $\imath(2) = 1$, $\Im(4) = \{1, 3\}$, $\imath(4) = 2$.

6.2. Calcul de $\Im(p^h)$ et $\imath(p^h)$ pour $p \geq 3$ prime et $h \geq 1$

.

Proposition 25. *Soit $p \geq 3$ un entier prime et soit $h \geq 1$. Alors,* $\Im(p^h) = \{1, p^h - 1\}$, $\imath(p^h) = 2$.

Démonstration

Si $h = 1$, il suffit d'observer que dans le corp $\mathbf{Z}/n\mathbf{Z}$ l'écuation $x^2 = 1$ aura au plus deux racines (± 1).

Supposons le résultat vrai pour h et soit μ avec $1 \leq \mu \leq p^{h+1} - 1$ tel que $p^{h+1} \mid \mu^2 - 1$. Il existera un entier m tel que $\mu^2 - 1 = p^{h+1}m$, et aussi nous aurons la relation $p^h \mid \mu^2 - 1 \Leftrightarrow \mu^2 - 1 \equiv 0\,(mod\ p^h)$.

Grâce a notre hypothèse, on vérifie

$$\mu \equiv \begin{cases} 1 \\ p^h - 1 \end{cases} (mod\ p^h) \Rightarrow$$

$$\Rightarrow \mu = \begin{cases} p^h c + 1 \\ p^h d + (p^h - 1) = p^h(d+1) - 1 \end{cases} \Rightarrow$$

$$\Rightarrow \mu^2 - 1 = p^{h+1}m = \begin{cases} p^{2h}c^2 + 2p^h c \\ p^{2h}(d+1)^2 - 2p^h(d+1) \end{cases} \Rightarrow$$

$$\Rightarrow pm = \begin{cases} p^h c^2 + 2c \\ p^h(d+1)^2 - 2(d+1) \end{cases} \Rightarrow \begin{cases} p \mid 2c \\ p \mid -2(d+1) \end{cases} \Rightarrow \begin{cases} p \mid c \\ p \mid d+1 \end{cases}$$

puisque p est prime avec 2. Alors,

$$\begin{cases} p \mid c \Rightarrow c = \begin{cases} 0 \Rightarrow \mu = 1 \\ p\alpha \Rightarrow \mu = p^{h+1}\alpha + 1 \end{cases} \\ p \mid d+1 \Rightarrow d+1 = \begin{cases} 0 \Rightarrow \mu = -1 \\ p\beta \Rightarrow \mu = p^{h+1}\beta - 1 \end{cases} \end{cases}$$

Sur les quatre valeurs que nous avons pour μ, le premiere c'est approprié. Le deuxième et le troixième ne sont pas possibles parce que ils ne appartierons à $[1, p^{h+1}-1]$. Pour le quatrième valeur, il faut que $k\beta = 1 \Rightarrow \mu = p^{h+1}-1$. □

6.3. Calcul de $\Im(p)$ et $\imath(p)$, pour $p \geq 3$ impair

Soit $p = p_1 p_2 \dots p_r$, où chaque p_i est un entier impair prime ou une puisance de un entier impair prime. On a l'isomorphisme

$$\Im(p) \simeq \Im(p_1) \times \ldots \times \Im(p_r) \simeq \mathcal{C}_2 \times \mathcal{C}_2 .^r . \times \mathcal{C}_2 \text{ et } \imath(p) = 2^r$$

Pour calculer le groupe, il suffit de donner r générateurs $\mu_1, ...\mu_r$, et pour chaque générateur il faudra que $\mu_i \equiv -1 \, (mod \; p_i)$, $\mu_i \equiv 1 \, (mod \; p_j)$ si $j \neq i$.

En plus le nombre $\mu_i - 1$ sera multiple de p_j, donc sera multiple du plus petit multiple de touts eux, qui sera leurs produit p/p_i. De ça façon, nous devons chercher des entiers x et y tels que $\mu_1 = p_i x - 1 = (p/p_i)y + 1$. C'est-à-dire, nous devons résoudre l'écuation diophantine $p_i x - (p/p_i)y = 2$. Una foi qu'elle soit résolue ou bien pour l'inconnue x ou bien pour l'inconnue y, il suffira d'utiliser les égalites $\mu_1 = p_i x - 1 = (p/p_i)y + 1$ pour avoir un valeur de $\mu_i \in [1, p-1]$.

Remarquez que si $p \geq 3$ est impair, la moitié des élément involutifs seront pairs et l'autre moitié seront impairs.

Une formule pour le nombre $\imath(n)$

Maintenant, si nous possons $n = 2^m p$, avec $m \geq 0$ et p impair, et en utilisant la fonction $lpi\,(p)$ -longeur prime impair-, c'est-à-dire, la quantité de facteurs primes impairs qui sont dans p, nous pourrons êcrire:

$$\imath(n) = \imath(2^m p) = \begin{cases} 1 \cdot 2^{lpi\,(p)} & \text{si } m = 0 \\ 1 \cdot 2^{lpi\,(p)} & \text{si } m = 1 \\ 2 \cdot 2^{lpi\,(p)} & \text{si } m = 2 \\ 4 \cdot 2^{lpi\,(p)} & \text{si } m \geq 3 \end{cases}$$

Cette formule sert aussi pour les nombres $n = 2^m$, en prenant $lpi\,(1) = 0$

Les groupes pour les modules pairs qu'il ne sont pas puissance de 2

Si nous excluront les puissances de 2, tout nombre pair on peut êcrire comment $n = 2^m p$, $m \geq 1$ et $p \geq 3$ impair. Comme nous conaîssons les groupes $\Im(2^m)$ et $\Im(p)$, nous pouvons calculer le groupe $\Im(n)$. Pourtant, remarquez que chaque groupe $\Im(2^{m+1}p)$ on peut déterminer après de connaître le groupe $\Im(2^m p)$.

D'abort, nous observons que si $p \geq 3$ est un entier impair et $\mu \notin 2\mathbf{Z}$, alors $\mu \in \Im(2p)$ et $\mu \in \Im(4p)$. En effet:

Il existera c, tel que $\mu = 2c + 1$, donc $\mu^2 - 1 = 4c^2 + 4c = 4c(c+1) \Rightarrow 4 \mid \mu^2 - 1$. Mais par hypothèse $p \mid \mu^2 - 1$, donc $\mu^2 - 1$ est multiple du $ppcm\,\{4, p\} = 4p$ (plus petit commun multiple), multiple de 4 et p. en consequence $\mu \in \Im(4p)$. Aussi, il est multiple de $2p$ et $\mu \in \Im(2p)$.

Proposition 26. *Soient les entiers $p \geq 1$, $m \geq 1$, avec p impair. Alors,*

$$\mu \in \Im(2^m p),\ \ \mu = \mp 1\,(mod\ 2^m) \Rightarrow \mu \in \Im(2^{m+1}p)$$

Démonstration

1) Il existera c tel que $\mu = 2^m c \mp 1$, donc $\mu^2 - 1 = (2^m c \mp 1)^2 - 1 = 2^{2m}c^2 \mp 2^{m+1}c = 2^{m+1}c\,(2^{m-1}c \mp 1) \Rightarrow 2^{m+1} \mid \mu^2 - 1$

2) $p \mid 2^m p \mid \mu^2 - 1 \Rightarrow p \mid \mu^2 - 1$. De ça façon, $\mu^2 - 1$ est multiple du $ppcm\,\{2^{m+1}, p\} = 2^{m+1}p$. □

Maintenant il est claire que $\Im(2p) \subset \Im(4p) \subset \Im(8p)$.

Si nous partons de conaître le Groupe $\Im(p)$, nous observons:

1) Comme la moitié des élément de $\Im(p)$ sont impairs, alors touts ces élément seront dans $\Im(2p)$. Ainsi, nous connaissons la moitié de ce groupe; l'autre moitié seront leurs oposes module $2p$ et le groupe $\Im(2p)$ est determiné.

2) Puisque $\imath(4p) = 2\imath(2p)$ et $\Im(2p) \subset \Im(4p)$, les élément $\mu \in \Im(2p)$ sont la moitié des élément du groupe $\Im(4p)$. L'autre moitié est formée par les élément $4p - \mu$.

3) Puisque $\imath(8p) = 2\imath(4p)$ et $\Im(4p) \subset \Im(8p)$, nous pouvons raisonner comme avant.

Et de façon analogue si on connaît le groupe $\Im(2^m p)$, nous pourrons calculer les éléments du groupe $\Im(2^{m+1}p)$.

References

[1] Brauer R., Suzuki M. On finite groups of even order whose 2-Sylow subgroups is a quaternion group. Proc. Nat. Acad. Sci.,45, pp. 1757-1759, (1959).

[2] Burnside W. Theory of groups. Dover, New York, (1955).

[3] Derek J. S. Robinson. A Course in the Theory of Groups. Springer-Verlag, New-York, (1982).

[4] Feit W. Theory of finite groups in the twentieth century. American Mathematical Heritage: Algebra and Applied Mathematics, Texas Tech Univ., (1981).

[5] Gorenstein D. Finite groups. Chelsea Publishing Company, New York, (1980).

[6] Seksenbaev K. On the theory of polycyclic groups. Algebra i Logika 4, pp. 79-83, (1965).

[7] Suzuki, Michio. Group Theory I, Springer-Verlag,1982.

[8] Vinogradov I. Fundamentos de la teoría de números. Ed. Mir, Moscú, (1972).

Alfonso Ríder Moyano
Departamento de Matemáticas
Universidad de Córdoba
e-mail : ma1rimoa@uco.es

and

Rafael María Rubio Ruiz
Departamento de Matemáticas
Universidad de Córdoba
e-mail : ma1rurur@uco.es