XXI Congreso de Ecuaciones Diferenciales y Aplicaciones
XI Congreso de Matemática Aplicada
Ciudad Real, 21-25 septiembre 2009
(pp. 1–8)

Matrices $\{P, s+1\}$-potentes

Carmen Coll[1], Leila Lebtahi[2], Néstor Thome[1]

[1] *Instituto de Matemática Multidiscilpinar, Universidad Politécnica de Valencia, E-46022 Valencia.* *E-mails:* mccoll@mat.upv.es, njthome@mat.upv.es.
[2] *Dpto. de Matemática Aplicada, Universidad Politécnica de Valencia, E-46022 Valencia. E-mail:* leilebep@mat.upv.es.

Palabras clave: Matriz idempotente, matriz $\{k\}$-potente, grupo no conmutativo

Resumen

En los últimos años se han estudiado las situaciones en que una matriz cuadrada A coincide con alguna de sus potencias (naturales), estando este tipo de matrices relacionadas con ciertas inversas de grupo. Por otra parte, es posible introducir otra clase de matrices que involucran una matriz de permutación y que generalizan el concepto de matriz idempotente, ampliamente utilizadas en multitud de aplicaciones. En este trabajo se introduce un nuevo tipo de matrices, que se denominarán matrices $\{P, s+1\}$-potentes, como una extensión de las dos situaciones anteriormente citadas. Se realiza un estudio de las mismas y también se presentan algunos ejemplos ilustrativos.

1. Introducción

Sea $P \in \mathbb{C}^{n\times n}$ una matriz de permutación, es decir P tiene todos sus elementos iguales a 0, excepto uno cualquiera por cada fila y columna, el cual debe ser igual a 1. Dicho de otra manera, P es producto de matrices que se obtienen intercambiando dos filas (o columnas) en la matriz identidad de tamaño $n \times n$, denotada por I_n.

En los últimos años se han estudiado las situaciones en que una matriz cuadrada A coincide con alguna de sus potencias [3]. En el caso en que $A^{s+1} = A$ para algún $s = 2, 3, \ldots,$ se tiene que $A^{\#} = A^{s-1}$, donde $A^{\#}$ representa la inversa de grupo de $A \in \mathbb{C}^{n\times n}$ [4]. En este trabajo se generalizará este concepto mediante la siguiente definición.

Definición 1 *Sea $P \in \mathbb{C}^{n\times n}$ una matriz de permutación fija. Una matriz $A \in \mathbb{C}^{n\times n}$ se llama $\{P, s+1\}$-potente si para algún $s = 1, 2, 3, \ldots$ se cumple que*

$$PA^{s+1}P = A. \tag{1}$$

Es claro que la definición anterior extiende los casos estudiados hasta el momento.

Si $A \in \mathbb{C}^{n\times n}$ es una matriz de permutación entonces es evidente que A es una matriz invertible y $A^{-1} = A$, es decir $A^2 = I_n$. También es claro que cuando $P = I_n$ el concepto de $\{P, s+1\}$-potente coincide con el de matriz $\{s+1\}$-potente (es decir, $A^{s+1} = A$) [3] y el caso $P = A$ corresponde a la situación trivial $P = A = I_n$ para cualquier $s = 1, 2, 3, \ldots$.

En relación a la teoría de grupos, se recuerda también que si G es un grupo finito con elemento neutro e y $a \in G$ entonces $a^m = e$ implica orden$(a)/m$ para cualquier potencia natural m. Por otro lado, se recuerda que si un grupo H tiene un subgrupo cíclico normal N tal que el grupo cociente H/N es cíclico entonces este grupo se denomina grupo metacíclico [8]. Una representación de los grupos metacíclicos se basa en que están generados por dos elementos a y b sujetos a tres relaciones que dependen de varios parámetros: $a^m = e$, $b^l = e$, $b^{-1}ab = a^k$ siendo e el elemento neutro del grupo y cumpliéndose que $k^l \equiv 1[\mathrm{mod}\ m]$ y m y k relativamente primos entre sí [5]. Hempel dio en el año 2000 una clasificación completa de todos los grupos finitos metacíclicos [6]. Por otra parte, en el caso en que $A \in \mathbb{C}^{n\times n}$ cumpla que $A^2 = A$ es evidente que el conjunto $\{A\}$ es un grupo cíclico (y, por tanto, conmutativo y normal) de orden 1. En el caso más general en que se verifica que $A^{s+1} = A$, siendo $s \in \{1, 2, 3, \ldots\}$ el menor natural que satisface esta propiedad, también es claro que el conjunto $\{A, A^2, A^3, \ldots, A^s\}$ es un grupo cíclico (y, por tanto, normal) de orden s.

En este trabajo se estudian propiedades de las matrices $\{P, s+1\}$-potentes y se prueba que a partir de una de ellas es posible construir un grupo cuyos elementos cumplen ciertas relaciones y posteriormente se estudian algunas propiedades de dicho grupo. Finalmente, se demuestra que dicho grupo es cíclico o metacíclico y se dan algunos ejemplos ilustrativos.

2. Propiedades de las matrices $\{P, s+1\}$-potentes

En primer lugar se establecerán propiedades concernientes a las matrices A que son $\{P, s+1\}$-potentes y su relación con la matriz P de permutación y el escalar s.

Lema 1 *Sea $P \in \mathbb{C}^{n\times n}$ una matriz de permutación fija y s algún elemento de $\{1, 2, 3 \ldots\}$.*

(I) Entonces se cumple que A es $\{P, s+1\}$-potente si y sólo si $PAP = A^{s+1}$.

(II) Si además $A \in \mathbb{C}^{n\times n}$ es una matriz $\{P, s+1\}$-potente entonces se cumplen las siguientes propiedades:

(a) $PA = A^{s+1}P$ *y* $AP = PA^{s+1}$.
(b) $PA^{s+2} = A^{s+2}P$ *y* $PA^{s+2}P = A^{s+2}$.
(c) $A^{s+2} = (PA)^2 = (AP)^2$.
(d) $A^{(s+1)^2} = A$.
(e) $(A^{(s+1)^2-1})^k = A^{(s+1)^2-1}$ *para todo* $k \in \mathbb{N}$.
(f) $(A^{s+2})^{s+1} = A^{s+2}$.
(g) $(PA)^{2s+1} = PA$ *y* $(AP)^{2s+1} = AP$.
(h) $PA^jP = A^{j(s+1)}$ *y* $A^jP = PA^{j(s+1)}$ *para* $j \in \{1, 2, \ldots, (s+1)^2 - 1\}$.
(i) Para cada $j \in \{1, 2, \ldots, (s+1)^2 - 1\}$, *se tiene que* $(PA^j)(PA^k) = A^{(s+1)^2-1}$, *siendo k el único elemento de* $\{1, 2, \ldots, (s+1)^2 - 1\}$ *tal que* $k \equiv -j(s+1)\ [\mathrm{mod}\ ((s+1)^2 - 1)]$.

(j) $P(PA^j)^{s+1}P = \begin{cases} PA^{j\frac{s}{2}(s+4)+j} & \textit{si } s \textit{ es par} \\ \left(A^{j(s+2)}\right)^{\frac{s+1}{2}} & \textit{si } s \textit{ es impar.} \end{cases}$

Demostración. Teniendo en cuenta que $P^2 = I_n$ se tiene que multiplicando por P ambos lados de la igualdad $PA^{s+1}P = A$ resulta $P^2A^{s+1}P^2 = PAP$ con lo cual $A^{s+1} = PAP$. La recíproca se demuestra de manera semejante y así la equivalencia de (I) queda establecida.

Las dos igualdades de la parte (a) de (II) siguen directamente de (I) teniendo en cuenta que $P^{-1} = P$. A partir de (II) (a) se tiene que $PA^{s+2} = PA^{s+1}A = APA = AA^{s+1}P = A^{s+2}P$ lo que prueba la primera igualdad de (II) (b) y la segunda igualdad se deduce de esta postmultiplicando ambos lados por P. A partir de (II) (b) y de (II) (a) se tiene que $A^{s+2} = PA^{s+2}P = PAA^{s+1}P = PAPA = (PA)^2$. La otra igualdad de (II) (c) se obtiene de manera semejante. Por (I) y por la definición resulta que $A^{(s+1)^2} = (A^{s+1})^{s+1} = (PAP)^{s+1} = PA^{s+1}P = A$ con lo que se demuestra (II) (d). Usando la propiedad (II) (d) se tiene $(A^{(s+1)^2-1})^2 = A^{(s+1)^2}A^{(s+1)^2-2} = AA^{(s+1)^2-2} = A^{(s+1)^2-1}$, y ahora la propiedad (II) (e) se puede probar por inducción. De la propiedad (II) (d) se tiene $(A^{s+2})^{s+1} = (A^{s+1}A)^{s+1} = (A^{s+1})^{s+1}A^{s+1} = A^{(s+1)^2}A^{s+1} = AA^{s+1} = A^{s+2}$ y así (II) (f) queda probada. A partir de (II) (c) y (d) se tiene que $(PA)^{2s+1} = PA(PA)^{2s} = PA(A^{s+2})^s = PA^{s^2+2s+1} = PA^{(s+1)^2} = PA$, y de manera similar se puede ver la igualdad $(AP)^{2s+1} = AP$, lo que prueba (II) (g). Para la comprobación de (II) (h) se procederá por recurrencia. En efecto, por definición y por la propiedad (I) se tiene que

$$PAP = A^{s+1}. \tag{2}$$

Luego, por la propiedad (II) (a) y por (2) resulta $PA^2P = PAAP = A^{s+1}PAP = A^{s+1}A^{s+1} = A^{2(s+1)}$. Con esta última propiedad, junto a la propiedad (II) (a) y (2), se obtiene $PA^3P = A^{3(s+1)}$. Siguiendo un razonamiento similar se prueba que $PA^jP = A^{j(s+1)}$ para $j \in \{1, 2, \ldots, s\}$. Utilizando ahora la definición y que $A^{(s+1)^2} = A$ se obtiene esta propiedad para $j = s+1$ como sigue: $PA^{s+1}P = A = A^{(s+1)^2} = A^{(s+1)(s+1)}$. De ahora en más, siguiendo razonamientos similares a los anteriores se prueba que $PA^jP = A^{j(s+1)}$ para $j \in \{1, 2, \ldots, (s+1)^2-1\}$, y la otra igualdad se obtiene fácilmente del hecho que $P^2 = I_n$. A continuación se demostrará (II) (i). Para un conjunto S y un elemento a dados, se utilizará la notación $\{a\}+S = \{a+s : s \in S\}$ para indicar la traslación del conjunto S por el elemento a. Sea $j \in \{1, 2, \ldots, (s+1)^2-2\}$, se debe probar que $(PA^j)(PA^k) = A^{(s+1)^2-1}$, siendo k el único elemento de $\{1, 2, \ldots, (s+1)^2-2\}$ tal que $k \equiv -j(s+1)$ [mod $((s+1)^2-1)$]. Para ello, primero se construyen los conjuntos $J_1^0 = \{1, 2, \ldots, s\}$ y $J_1 = \{0, 1, 2, \ldots, s\}$ y, por recurrencia, para cada $i \in \{1, 2, \ldots, s-1\}$ se construyen los conjuntos $J_{i+1} = \{s+1\} + J_i$ y finalmente $J_{s+1} = \{s(s+1), s(s+1)+1, s(s+1)+2, \ldots, s(s+1)+(s-1)\}$. Es claro que, por construcción,

$$J_1^0 \cup \left(\bigcup_{i=2}^{s+1} J_i\right) = \{1, 2, \ldots, (s+1)^2 - 2\}.$$

Como $j \in \{1, 2, \ldots, (s+1)^2 - 2\}$, se tiene que $j \in J_1^0$ o bien existe $i \in \{2, 3 \ldots, s+1\}$ tal que $j \in J_i$. Ahora se analiza cada uno de los casos. Si

- $j \in J_1^0$, tomando $k = [(s+1)^2 - 1] - j(s+1)$ se cumplen las condiciones sobre k y la propiedad (II) (h) asegura que $(PA^j)(PA^k) = A^{j(s+1)}A^k = A^{k+j(s+1)} = A^{(s+1)^2-1}$.

- existe $i \in \{2, 3 \ldots, s+1\}$ tal que $j \in J_i$, es claro que tomando $k = i[(s+1)^2 - 1] - j(s+1)$ se cumplen las condiciones sobre k y además las propiedades (II) (e) y (h) aseguran que $(PA^j)(PA^k) = A^{j(s+1)}A^k = A^{k+j(s+1)} = [A^{(s+1)^2-1}]^i = A^{(s+1)^2-1}$.

Finalmente, sea $j = (s+1)^2 - 1$. En este caso se tiene que debe tomarse $k = j$ y así la propiedad (II) (i) queda demostrada puesto que $J_1^0 \cap J_j = J_i \cap J_j = \emptyset$, para todo $i, j \in \{2, 3, \ldots, s+1\}$, con $i \neq j$, con lo que la propiedad (II) (i) queda probada.

Para probar la propiedad (j) primero se supondrá que s es par. En este caso, usando las propiedades (II) (h) y (d), se tiene

$$
\begin{aligned}
P(PA^j)^{s+1}P &= A^jA^{j(s+1)\frac{s}{2}}A^{j\frac{s}{2}}P = A^{j(s+2)\frac{s}{2}}A^jP = A^{j(s+2)\frac{s}{2}}PA^{j(s+1)} \\
&= PA^{(s+1)\left(j(s+2)\frac{s}{2}\right)}A^{j(s+1)} = PA^{j(s+1)\left((s+1)\frac{s}{2}+\frac{s}{2}\right)}A^{j(s+1)} \\
&= P\left(A^{(s+1)^2}\right)^{j\frac{s}{2}}A^{\left(\frac{s}{2}+1\right)j(s+1)} = PA^{j\frac{s}{2}(s+4)+j}.
\end{aligned}
$$

En el caso en que s sea impar se tiene

$$
P(PA^j)^{s+1}P = A^jA^{j(s+1)\frac{s+1}{2}}A^{j\frac{s-1}{2}} = A^{j(s+1)\frac{s+1}{2}+j\frac{s+1}{2}} = \left(A^{j(s+2)}\right)^{\frac{s+1}{2}}.
$$

■

3. Un grupo asociado a una matriz $\{P, s+1\}$-potente

Del Lema 1 se puede deducir que a partir de una matriz $\{P, s+1\}$-potente es posible construir un grupo que contiene un subgrupo cíclico formado por matrices $\{P, s+1\}$-potentes.

Teorema 1 *Sea $P \in \mathbb{C}^{n\times n}$ una matriz de permutación fija, s un número natural y $A \in \mathbb{C}^{n\times n}$ una matriz $\{P, s+1\}$-potente. Entonces el conjunto*

$$
G = \{A, A^2, A^3, \ldots, A^{(s+1)^2-1}, PA, PA^2, PA^3, \ldots, PA^{(s+1)^2-1}\}
$$

es un grupo con respecto a la multiplicación de matrices que cumple las siguientes propiedades:

(a) A es un elemento de orden $(s+1)^2 - 1$, con lo que el conjunto

$$
S_A = \{A, A^2, A^3, \ldots, A^{(s+1)^2-1}\} \tag{3}
$$

forma un subgrupo cíclico de G.

(b) PA^s es un elemento de orden 2.

(c) $(PA^s)A(PA^s) = A^{s+1}$.

(d) El conjunto S_A forma un subgrupo normal de G donde todos sus elementos son matrices $\{P, s+1\}$-potentes.

(e) Los elementos PA^j del conjunto $G - S_A$ (si es no vacío) son $\{P,s+1\}$-potentes si y sólo si s es par y $j\frac{s}{2}(s+4) \equiv 0$ [mod $((s+1)^2 - 1)$].

(f) El orden de G es:

- $(s+1)^2-1$ *si* $PA = A^j$ *para algún* $j \in \{1, 2, \ldots, (s+1)^2-1\}$ *y, en este caso, el grupo* G *es conmutativo.*
- $2((s+1)^2-1)$ *si* $PA \neq A^j$ *para todo* $j \in \{1, 2, \ldots, (s+1)^2-1\}$ *y, en este caso, el grupo* G *es no conmutativo.*

Demostración. De las propiedades probadas en el Lema 1, es evidente comprobar que G es un grupo siendo $A^{(s+1)^2-1}$ su elemento neutro. Además, es claro que G contiene un subgrupo cíclico generado por el elemento A de orden $(s+1)^2-1$. Por su parte, la propiedad *(b)* se deduce del hecho que $(PA^s)^2 = PA^sPA^s = A^{s(s+1)}A^s = A^{s(s+2)} = A^{(s+1)^2-1}$ y por definición se tiene la propiedad *(c)* como sigue $(PA^s)A(PA^s) = PA^{s+1}PA^s = AA^s = A^{s+1}$. Se ha indicado ya que S_A es un subgrupo de G. Comprobando que para todo $j, k \in \{1, 2, \ldots, (s+1)^2-1\}$ se tiene $A^jA^k(A^j)^{-1} = A^{j+k}A^{(s+1)^2-1-j} = A^k$, y, puesto que los elementos inversos de PA^j son de la misma forma (por ejemplo, $(PA^j)^{-1} = PA^t$ donde t cumple las propiedades de (II) (i) del Lema 1), se tiene que para todo $j, k \in \{1, 2, \ldots, (s+1)^2-1\}$, queda claro que este subgrupo S_A es normal pues

$$(PA^j)A^k(PA^j)^{-1} = PA^{j+k}PA^t = A^{(j+k)(s+1)}A^t = A^{(j+k)(s+1)+t}.$$

Que el resto de la propiedad *(d)* se cumple es consecuencia directa de la primera parte de la propiedad *(II) (h)* del Lema 1, puesto que como A^j son matrices $\{P, s+1\}$-potentes para todo $j \in \{1, 2, \ldots, (s+1)^2-1\}$, todos los elementos de S_A son $\{P, s+1\}$-potentes. Para probar la propiedad *(e)* se observa que, como $G - S_A \neq \emptyset$, es claro que PA^j es $\{P, s+1\}$-potente si y sólo si s es par por la propiedad (II) (j) del Lema 1. Esta misma propiedad garantiza que, en este caso, $P(PA^j)^{s+1}P = PA^{j\frac{s}{2}(s+4)+j}$. Luego,

$$PA^j \text{ es } \{P, s+1\}-\text{potente} \iff PA^{j\frac{s}{2}(s+4)+j} = PA^j \iff A^{j\frac{s}{2}(s+4)+j} = A^j$$

$$\iff A^{j\frac{s}{2}(s+4)+j}A^{(s+1)^2-1-j} = A^{(s+1)^2-1} \iff A^{j\frac{s}{2}(s+4)} = A^{(s+1)^2-1}$$

y por consiguiente esto equivale a que $(s+1)^2-1 = s(s+2)$ divide a $j\frac{s}{2}(s+4)$, o sea $j\frac{s}{2}(s+4) \equiv 0$ [mod $((s+1)^2-1)$]. Finalmente, para demostrar la propiedad *(f)* se tiene en cuenta que si $PA = A^j$ para algún $j \in \{1, 2, \ldots, (s+1)^2-1\}$ entonces $PA^i = A^{j+i-1}$, es decir, también será una de las $(s+1)^2-1$ potencias de A indicadas en (3) para todo $i \in \{2, 3, \ldots, (s+1)^2-1\}$. De este modo el orden de G es $(s+1)^2-1$ y por tanto G sería conmutativo. En el caso en que $PA \neq A^j$ para todo $j \in \{1, 2, \ldots, (s+1)^2-1\}$ es claro que el orden de G será $2((s+1)^2-1)$ puesto que si fuese $PA^i = PA^j$ para algún $i, j \in \{1, 2, \ldots, (s+1)^2-1\}$ con $i \neq j$, se tendría que $A^i = P^2A^i = P^2A^j = A^j$, lo cual es imposible. Además, para ver que en este caso G no es conmutativo se comprueba, por ejemplo, que $(PA)(PA^{s+1}) \neq (PA^{s+1})(PA)$. En efecto, si por el contrario, lo fuese se tendría $(PA)(PA^{s+1}) = (PA^{s+1})(PA)$. Entonces usando la definición y la propiedad *(I)* del Lema 1 se tiene que $A^{2(s+1)} = A^2$. Multiplicando ambos miembros de la igualdad anterior por $A^{(s+1)^2-2(s+1)}$ y simplificando la expresión mediante la propiedad *(II) (d)* queda $A = A^{s^2+1}$ y claramente ambos son elementos distintos de G, lo que lleva a una contradicción y finaliza la demostración del teorema. ∎

Puesto que el Teorema de Cayley asegura que cualquier grupo finito de orden n es isomorfo a un subgrupo del grupo S_n de todas las permutaciones de un conjunto de n elementos, se tiene que el grupo G construido en el Teorema 1 también lo será. Para este grupo se puede precisar más, como se observa en el siguiente resultado.

Teorema 2 *El grupo G construido en el Teorema 1 es cíclico o metacíclico.*

Demostración. En el caso en que exista un $j \in \{1, 2, \ldots, (s+1)^2 - 1\}$ tal que $PA = A^j$, se tendrá que G coincide con S_A y por tanto G será cíclico.

Suponiendo que $PA \neq A^j$ para todo $j \in \{1, 2, \ldots, (s+1)^2 - 1\}$, es decir que G tiene orden $2((s+1)^2 - 1)$, de las propiedades mostradas en el Teorema 1, se observa que sólo falta comprobar que G/S_A es un grupo cíclico. En efecto, es claro que $G/S_A = \{\overline{A^{\text{pot}}}, \overline{PA^{\text{pot}}}\}$ donde $\overline{A^{\text{pot}}}$, que es la clase de todas las potencias de A que aparecen en S_A, es el elemento neutro de G/S_A y $\overline{PA^{\text{pot}}}$, que es la clase de todos los elementos de la forma P por una potencia de A como aparecen en G, es un elemento de orden 2 de la Propiedad (II) del Lema 1. Por tanto, G/S_A es cíclico y, por definición, se tiene que G es metacíclico. ■

Nota 1 *La verificación de la propiedad (II) (d) del Lema 1 hace posible la construcción del grupo G considerando el subgrupo S_A de orden $(s+1)^2 - 1$. En realidad, puede ocurrir que exista un exponente natural λ para el cual $A^\lambda = A$ siendo $2 \leq \lambda < (s+1)^2$. En este caso, también sería posible considerar la construcción de un grupo asociado a la matriz A de modo que sea $\{P, s+1\}$-potente para alguna matriz de permutación P y algún escalar s. Si este fuese el caso, el conjunto $S_A^\lambda = \{A, A^2, \ldots, A^{\lambda-1}\}$ formará un subgrupo del grupo S_A y por tanto $\lambda - 1$ será un divisor de $(s+1)^2 - 1 = s(s+2)$. Mediante un razonamiento similiar al realizado en el Teorema 2 es claro que si el grupo $G_\lambda = \{A, A^2, \ldots, A^{\lambda-1}, PA, PA^2, \ldots, PA^{\lambda-1}\}$ tiene orden $2(\lambda-1)$, también es metacíclico puesto que G_λ/S_A^λ está formado sólo por 2 clases de equivalencia.*

Se recuerda también que se denota por D_m al grupo diedral de orden $2m$ caracterizado por estar generado por un elemento a de orden m y un elemento b de orden 2 de modo que cumplan que $b^{-1}ab = a^{-1}$ [8]. También es fácil ver que si G es un grupo metacíclico en el cual $m = k+1$ y $l = 2$ entonces G coincide con el grupo diedral D_m.

Por su parte, también es conocido que el grupo casi-diedral[1], que se puede denotar por Q_{2^m}, para $m \geq 4$, se caracteriza por estar generado por un elemento a de orden 2^{m-1} y un elemento b de orden 2 que cumplen la relación $bab = a^{2^{m-2}-1}$.

Es evidente que el grupo G (construido en el Teorema 1) depende de A, P y s. Por ello, para el siguiente resultado, se denotará G por G_s remarcando así el parámetro s. La relación entre el grupo G_s y los grupos diedral y casi-diedral se aprecia a continuación.

Proposición 1 *Bajo la notación del Teorema 1 y suponiendo que G_s tiene orden:*

(I) $(s+1)^2 - 1$, *es posible establecer que $G_s \simeq \Omega_{(s+1)^2-1}$, donde este último representa al grupo de las raíces $((s+1)^2 - 1)$-ésimas de la unidad.*

(II) $2((s+1)^2 - 1)$, *es posible establecer que:*

[1] Cuyo nombre se atribuye a B. Huppert [7].

(a) $G_s \simeq D_{(s+1)^2-1}$ *si y sólo si* $s = 1$.

(b) $G_s \simeq Q_{2^m}$ *si y sólo si* $s = 2$ *y* $m = 4$.

Demostración. La demostración de la parte (I) es evidente, por tanto sólo se indicará la de la parte (II). Si $s = 1$, la demostración del caso *(a)* se deduce del hecho que G_s está generado por el elemento A de orden 3, por el elemento PA de orden 2 y además se cumple la relación $(PA)A(PA) = A^2$, siendo A^2 el inverso del elemento A.

Sea $s > 1$. En este caso, se sabe que el grupo G_s tiene el elemento A de orden $(s+1)^2-1$. Por otro lado, se comprueba que para cualquier $\alpha \in \{1, 2, \ldots, (s+1)^2-1\}$ el elemento PA^α es de orden 2 si y sólo si α es un múltiplo de s pues

$$A^{(s+1)^2-1} = (PA^\alpha)^2 \iff A^{s(s+2)} = PA^\alpha PA^\alpha = A^{\alpha(s+1)}A^\alpha = A^{\alpha(s+2)}$$

$$\iff s(s+2) \text{ divide a } \alpha(s+2) \iff s \text{ divide a } \alpha,$$

con lo que todos los elementos de orden 2 de G_s tienen esta forma. Sin embargo, para un elemento cualquiera PA^{st} de esta forma, siendo

$$t \in \left\{\frac{1}{s}, \frac{2}{s}, \ldots, \frac{(s+1)^2-1}{s}\right\} \cap \mathbb{N} = \{1, 2, 3, \ldots, s+2\},$$

no se cumple que $(PA^{st})A(PA^{st}) = A^{(s+1)^2-1}$ ya que $(PA^{st})A(PA^{st}) = PA^{st+1}PA^{st}$ $= A^{(st+1)(s+1)}A^{st} = A^{((s+1)^2-1)t+(s+1)} = (A^{(s+1)^2-1})^t A^{s+1} = A^{s+1}$ y como $s+2$ no divide a $s+1$ y siempre se tiene que $s+2$ divide a $s(s+2)$ entonces $s(s+2)$ no puede dividir a $s+1$, con lo que $A^{s+1} \neq A^{(s+1)^2-1}$. El caso recíproco es evidente.

Para la demostración del caso *(b)* es necesario tener en cuenta que las propiedades de G_s para $s = 2$ coinciden con las de Q_{2^m} para $m = 4$. En efecto, si $s = 2$ entonces G_s tiene un elemento A de orden $8 = 2^{4-1}$, otro elemento PA^2 de orden 2 y además por la Propiedad (c) del Teorema 1 se tiene $(PA^2)A(PA^2) = A^3 = A^{2^{4-2}-1}$ y por tanto $G_2 \simeq Q_{2^4}$. Recíprocamente, si $G_s \simeq Q_{2^m}$ entonces se tiene que $2^{m-1} = (s+1)^2 - 1 = s(s+2)$. Por la unicidad (salvo el orden de los factores) de la descomposición de un número natural mayor o igual que 2 en factores primos se deduce que debe ser $s = 2$ y $m = 4$. ■

4. Ejemplos

La matriz $A = iI_2$ es $\{P, 5\}$-potente para cualquier matriz de permutación $P \in \mathbb{C}^{2\times 2}$ y $s = 4$ y no es $\{P, t+1\}$-potente para $t = 1, 2, 3$ ni para $P = I_2$ ni para

$$P = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{4}$$

Este ejemplo sirve para mostrar una matriz de la clase con la que se está trabajando para la cual no se puede construir el grupo G como en el Teorema 1 puesto que $s = 4$ daría origen a un grupo de orden 24 (si $P = I_n$, por ejemplo) o bien 48. Sin embargo, para esta matriz se cumple $A^5 = A$ con lo cual se puede construir un grupo con características similares (con cualquiera de las permutaciones). En este caso el grupo será de orden 4 u 8 según que $PA = A^j$ para algún $j \in \{1, 2, 3, 4\}$ o no, y es fácil comprobar que también es cíclico o metacíclico, respectivamente. En efecto, si P es la misma matriz que en (4) se tiene que la forma del grupo es $G = \{iI_2, -I_2, -iI_2, I_2, iP, -P, -iP, P\}$. En este caso, $A = iI_2$ es un elemento de orden 4 y los dos elementos de orden 2 son $PA^2 = -P$ y $PA^4 = P$. Sin embargo, como $(PA^j)A(PA^j) = A \neq A^3$ para $j \in \{2, 4\}$ se tiene que G no es isomorfo al grupo de simetrías de un cuadrado. En este sentido, en el caso en que las potencias de A no agoten la cantidad de elementos del grupo, se tiene la situación de la Tabla 1.

s	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Orden(G)	6	16	30	48	70	96	126	160	198	240	286	336	390	448	510

Tabla 1: Orden$(G) = 2((s+1)^2 - 1)$ para algunos valores de s siendo $PA \neq A^j$ para todo $j \in \{1, 2, \ldots, (s+1)^2 - 1\}$.

Los posibles valores del orden de G para los 15 primeros valores de s cuando $PA = A^j$, para algún $j \in \{1, 2, \ldots, (s+1)^2 - 1\}$, se reducen a la mitad de los indicados en la Tabla 1.

Por otro lado, la siguiente matriz A es $\{P, s+1\}$-potente para toda matriz de permutación $P \in \mathbb{C}^{n\times n}$ y $\forall \in \mathbb{N}$ siendo el grupo asociado $G = \{A\}$:

$$A = \frac{1}{n}\begin{bmatrix} 1 & 1 & \ldots & 1 \\ 1 & 1 & \ldots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \ldots & 1 \end{bmatrix} \in \mathbb{C}^{n\times n}$$

Finalmente, para las siguientes matrices A y P, se tiene que A es $\{P, 2\}$-potente

$$A = \begin{bmatrix} 0 & 0 & -i \\ i & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \qquad \text{y} \qquad P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

y el grupo $G = \{A, A^2, A^3, PA, PA^2, PA^3\} \simeq D_3$ (Proposición 1) es de orden 6.

Agradecimientos

Este trabajo fue parcialmente subvencionado por el Proyecto DGI MTM2007-64477.

Referencias

[1] F. Clarke, *Optimization and Nonsmooth Analysis*, John Wiley & Sons, Inc., New York, 1983.

[2] J. Simon. *Compact sets in* $L^p(0, T; B)$. Ann. Mat. Pura Appl., sér. IV, CXLVI (1987), 65–96.

[3] J. Benítez, N. Thome, $\{k\}$*-group periodic matrices.* SIAM J. Matrix Anal. Appl. 28, 1 (2006), 9–25.

[4] R. Bru, N. Thome. *Group inverse and group involutory matrices.* Linear and Multilinear Algebra, 45 (2-3) (1998), 207–218.

[5] C. W. Curtis, I. Reiner. *Methods of representation theory: with applications to finite groups and orders*, John Wiley & Sons, Nueva York, 1981.

[6] C. E. Hempel. *Metacyclic Groups.* Communications in Algebra 28 (2000), 3865-3897.

[7] B. Huppert. *Character theory of finite groups*, Walter de Gruyter, Berlin, 1998.

[8] J.S. Rose, *A Course on Group Theory*, Cambridge, 1978.