Universidad Nacional Autónoma de México

FACULTAD DE CIENCIAS

CLASES DE EQUIVALENCIA DE MATRICES SOBRE CAMPOS FINITOS

T E S I S

QUE PARA OBTENER EL TITULO DE:

M A T E M A T I C O

P R E S E N T A:

MARIO GUTIERREZ LAGUNES

MEXICO, D. F. 1983

INTRODUCCION

En el presente trabajo estudiamos una relación de equivalencia definida en F_{mn}, el anillo de matrices de $m \times n$ sobre un campo finito F de orden q. Desarrollamos la teoría general que nos permitirá obtener fórmulas para contar el número de clases de equivalencia inducida por un grupo Ω de permutaciones del campo F.

Cuando Ω es el grupo de todas las permutaciones de F, y tenemos $A \in F_{mn}$, A con k elementos diferentes, obtenemos el orden de la clase de A en Ω, y encontramos el número de matrices de $m \times n$ con k elementos diferentes, cuyas clases tienen orden $\frac{q!}{(q-k)!}$.

Cuando Ω es un grupo cíclico finito de orden s, para cada divisor t de s, obtenemos el número de matrices que permanecen invariantes bajo la acción del subgrupo de Ω de orden t y sólo para este subgrupo; así también obtenemos el número de clases de orden s/t inducida por Ω.

Analizamos también el caso cuando Ω es el producto directo de subgrupos cíclicos.

Finalmente, deseo expresar mi agradecimiento a la Profra. Mary Glazman Nowalski, que gracias a su colaboración en la dirección de la presente tesis, fue posible su realización. Y en general, a todas las personas que me apoyaron en mis estudios, les doy las gracias.

INDICE

CAPITULO 1. TEORIA GENERAL. 1.

CAPITULO 2. AUTOMORFISMOS. 1.

CAPITULO 3. EL CASO Ω = Sq . 6.

CAPITULO 4. GRUPOS CICLICOS. 18.

CAPITULO 5. PRODUCTO DIRECTO. 30.

CLASES DE EQUIVALENCIA DE MATRICES SOBRE CAMPOS FINITOS.

1. TEORIA GENERAL.

Sea $F = GF(q)$ el campo finito de orden q, y Fmn el anillo de matrices de m x n sobre F.

Sea Ω un grupo de permutaciones de F.

DEFINICION 1. Si $A, B \in Fmn$, entonces B es equivalente a A si existe $\phi \in \Omega$ tal que $\phi(a_{ij}) = b_{ij}$; $a_{ij}, b_{ij} \in F$ para $i = 1,2,\ldots,m$ $j = 1,2,\ldots,n$

Esta es una relación de equivalencia en Fmn.

Notación. Sea $\mu(A,\Omega)$ el orden de la clase de A relativa a Ω y sea $\lambda(\Omega)$ el número de clases inducidas por el grupo Ω.

2. AUTOMORFISMOS.

DEFINICION 2. Si $A \in Fmn$, entonces $\phi \in \Omega$ es un automorfismo de A relativo a Ω si $\phi(A) = A$.

$Aut(A,\Omega) = \{\phi \in \Omega \,/\, \phi(A) = A,\ A \in Fmn\}$ es un subgrupo de Ω.

Al conjunto $Aut(A,\Omega)$ le llamaremos el grupo de automorfismos de la matriz A relativa a Ω.

Sea $v(A,\Omega)$ el número de automorfismos de la matriz A relativa a Ω.

Observación. Si A y B son equivalentes, es decir, si $\phi(A) = B$ para alguna $\phi \in \Omega$ entonces

$$Aut(B,\Omega) = \phi\, Aut(A,\Omega)\, \phi^{-1} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (2.0)$$

Por demostrar que

a) $\mathrm{Aut}(B,\Omega) \subset \phi\,\mathrm{Aut}(A,\Omega)\phi^{-1}$

b) $\phi\,\mathrm{Aut}(A,\Omega)\phi^{-1} \subset \mathrm{Aut}(B,\Omega)$

a) Sea $f \in \mathrm{Aut}(B,\Omega)$

$f = \phi\phi^{-1} f \phi\phi^{-1}$ pero $(\phi^{-1} f \phi)(\Omega) = (\Omega)$

$\therefore \quad \phi^{-1} f \phi \in \mathrm{Aut}(A,\Omega)$

$\therefore \quad \mathrm{Aut}(B,\Omega) \subset \phi\,\mathrm{Aut}(A,\Omega)\phi^{-1}$

b) Sea $f \in \phi\,\mathrm{Aut}(A,\Omega)\phi^{-1}$

Tenemos $f = \phi\sigma\phi^{-1}$ con $\sigma \in \mathrm{Aut}(A,\Omega)$

$$\therefore \quad f(B) = (\phi\sigma\phi^{-1})(B) = \phi(\sigma(\phi^{-1}(B))) = \phi(\sigma(\Omega)) = \phi(\Omega) = B$$

$\therefore \quad f \in \mathrm{Aut}(B,\Omega)$

$\therefore \quad \phi\,\mathrm{Aut}(A,\Omega)\phi^{-1} \subset \mathrm{Aut}(B,\Omega)$

□

Así que $v(A,\Omega) = v(B,\Omega)$, por lo que tenemos que el número de automorfismos depende solamente de la clase y no en particular de las matrices dentro de la clase.

TEOREMA 2.1. Sea $A \in Fmn$. Entonces para cualquier grupo Ω, tenemos

$$\mu(A,\Omega)\, v(A,\Omega) = |\Omega| \quad \ldots\ldots\ldots\ldots\ldots \quad (2.1)$$

donde $|\Omega|$ denota el orden de Ω.

Demostración.

Por Lagrange,

$v(A,\Omega)$ · número de clases determinadas por $Aut(A,\Omega) = |\Omega|$

Bastará ver que el número de clases determinadas por $Aut(A,\Omega)$ es igual al orden de la clase de A determinada por la relación de equivalencia, es decir, bastará ver que el número de clases determinadas por $Aut(A,\Omega)$ es igual a $\mu(A,\Omega)$.

Sea $C = \{H_\phi\}_{\phi\in\Omega}$ donde $H_\phi = \{\psi\in\Omega / \phi\psi^{-1} \in Aut(A,\Omega)\}$,

$$(A,\Omega) = \{ B \in Fmn \,/\, \exists\ \theta\in\Omega \ni \theta(B) = A \}$$

y sea $f : (A,\Omega) \longmapsto C$, dado $B \in (A,\Omega) \ni \exists\ \phi\in\Omega$, $\phi(B) = A$ definido $B \longmapsto H_\phi$

Veamos que está bien definido.

Sea $B, B' \in (A,\Omega) \ni B = B'$.

Por lo tanto,

$$\exists\ \phi,\psi \in \Omega \ni \phi(B) = A, \quad \psi(B') = A .$$

P.D. $H_\phi = H_\psi$ es decir, $\phi.\psi^{-1}(A) = A$.

Si $\psi(B') = A$ entonces $\psi^{-1}(A) = B'$

Por otro lado

$$(\phi \circ \psi^{-1})(A) = \phi(\psi^{-1}(A)) = \phi(B') = \phi(B) = A$$

$$\therefore \quad H_\phi = H_\psi$$

Ahora bien, veamos que es inyectiva.

Sea $f(B) = f(B')$.

P.D. $B = B'$

Como $B, B' \in (A, \Omega)$

$\Longrightarrow \quad \exists\ \phi, \psi \in \Omega \ni \phi(B) = A$ y $\psi(B') = A$

pero $H_\phi = H_\psi$

$\Longrightarrow \quad (\phi \cdot \psi^{-1}) \in \mathrm{Aut}(A, \Omega)$

$\Longrightarrow \quad (\phi \cdot \psi^{-1})(A) = A$

$\Longrightarrow \quad \psi^{-1}(A) = \phi^{-1}(A)$

$$\therefore \quad B = B'$$

Ahora, veamos que es suprayectiva.

P.L. Dado $H_\phi \in C$, $\exists\ B \in (A,\Omega) \ni \phi(B) = A$

Sea $\Psi \in H_\phi \in C$, $H_\phi = \{\Psi \in \Omega / \ \phi\Psi^{-1} \in Aut(A,\Omega)\}$

$(\phi\cdot\Psi^{-1}) \in Aut(A,\Omega)$, por lo tanto, haciendo

$\Psi^{-1}(A) = B$, tendremos

$\phi(B) = (\phi\cdot\Psi^{-1})(A) = A$, es decir, $B \in (A,\Omega)$.

Por lo tanto, hemos encontrado una función biyectiva entre el conjunto de clases determinadas por $Aut(A,\Omega)$ y el conjunto de la clase de A determinada por la relación de equivalencia, por lo cual llegamos a que tienen la misma cardinalidad.

□

Si ϕ es una permutación, sea $N_\phi(m,n)$ el número de matrices A, $A \in Fmn$, tal que $\phi(A) = A$.

TEOREMA 2.2. Si l_ϕ es el número de elementos invariantes de ϕ, entonces $N_\phi(m,n) = l_\phi^{mn}$

Demostración.

Un elemento $a \in F$ se dice que es invariante si $\phi(a) = a$

Por lo que tenemos, si l_ϕ es el número de elementos invariantes de ϕ, $\phi \in \Omega$ y $A \in Fmn$, entonces en cada entrada de A podemos colocar l_ϕ elementos invariantes, es decir,

$\phi(A) = A$ si y sólo si $\phi(a_{ij}) = a_{ij}$ para $i = 1,2,\ldots,m$

$j = 1,2,\ldots,n$

$\therefore$ $N_\phi(m,n)$ son las ordenaciones de l_ϕ elementos tomados de mn en mn veces, es decir, $N_\phi(m,n) = l_\phi^{mn}$.

□

3. EL CASO $\Omega = S_q$

Sea Ω el grupo de todas las permutaciones de F.

Ω es isomorfo al grupo simétrico Sq con q elementos.

DEFINICION. Un grupo de permutaciones Ω se dice que es un k-'pliego' transitivo sobre F, si para cualesquiera k-tuplas ordenadas $(\alpha_1,\alpha_2,\ldots,\alpha_k)$, $(\beta_1,\beta_2,\ldots,\beta_k)$ de elementos de F, donde $\alpha_i \neq \alpha_j$, $\beta_i \neq \beta_j$ si $i \neq j$, existe una permutación $\phi \in \Omega$ tal que $\phi(\alpha_i) = \beta_i$ para $i = 1,2,\ldots,k$

El grupo simétrico Sq es un q-'pliego' transitivo sobre F.

Así que si $mn \leq q$, entonces el grupo Sq induce una relación de equivalencia trivial sobre Fmn, puesto que cualesquiera dos matrices pueden ser equivalentes relativas para Sq.

Supongamos que $mn > q$.

TEOREMA 3.1. Sea $A \in F_{mn}$. Si A tiene k elementos diferentes, entonces $\mu(A,\Omega) = \frac{q!}{(q-k)!}$

Demostración.

Supongamos que los elementos diferentes de A son $\{\alpha_i\}_{i=1}^{k}$ donde $\alpha_i \in F$. Tenemos que hay $(q-k)!$ permutaciones en Sq tales que dejan fijos a $\alpha_1,\alpha_2,\ldots,\alpha_k$, es decir, $v(A,\Omega) = (q-k)!$

Por teorema 2.1, tenemos que

$\mu(A,\Omega)\, v(A,\Omega) = |\Omega|$ Como $\Omega = Sq$, $|\Omega| = q!$

$\therefore \quad \mu(A,\Omega)\,(q-k)! = q! \quad \therefore \quad \mu(A,\Omega) = \frac{q!}{(q-k)!}$ □

Si dos matrices A, $B \in F_{mn}$ tienen diferentes números de distintos elementos, entonces obviamente, A no es equivalente a B relativo a Sq.

Supongamos $A \in Fmn$, $A = (a_{ij})$, $i = 1,2,\ldots,m$ y A con k diferentes elementos $\alpha_1, \alpha_2, \ldots, \alpha_k$ donde α_τ aparece m_τ veces, así que $m_1 + m_2 + \ldots + m_k = mn$

Para cada $t = 1,2,\ldots,k$ sea

$$\Omega_\tau = \{(i,j) / a_{ij} = \alpha_\tau\}$$

Por ejemplo, si

$$\Omega = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

sobre GF(3), entonces si $\alpha_1 = 1$, $\alpha_2 = 2$, $\alpha_3 = 0$, tenemos

$A_1 = \{(1,1),(2,2),(2,3),(3,3)\}$

$A_2 = \{(1,2),(2,1)\}$

$A_3 = \{(1,3),(3,1),(3,2)\}$

Notemos que si A y B tienen el mismo número de elementos distintos, A puede no ser equivalente a B.

Por ejemplo $\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$ no es equivalente a $\begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}$ en S_3, ya que no existe una permutación $\phi \in \Omega$ tal que $\phi(1) = 0$ y $\phi(1) = 2$.

El siguiente teorema da una condición necesaria y suficiente para que dos matrices A y B sean equivalentes relativas en Sq.

TEOREMA 3.2. Sean A, B $\in$ Fmn, A con k elementos diferentes, y B con ℓ elementos diferentes. Si A genera los conjuntos $A_1,\ldots,A_k$ y B genera los conjuntos $B_1,B_2,\ldots,B_\ell$, entonces A es equivalente a B relativa a Sq si y sólo si $k = \ell$, y una vez reordenando,

$A_i = B_i$, para $i = 1,2,\ldots,k$.

Demostración.

Supongamos A equivalente a B relativa a Sq.

Por lo tanto, existe $\phi \in \Omega \ni \phi(A) = B$, es decir $\phi(a_{ij}) = b_{ij}$

Sea $\alpha_1, \alpha_2, \ldots, \alpha_k$ los elementos distintos de A. Además, $\phi(\alpha_1), \phi(\alpha_2), \ldots, \phi(\alpha_k)$ son todos los elementos de B y éstos son diferentes, porque si $\gamma \in B$ entonces $\phi(\alpha_j) = \gamma$ para alguna j por ser A equivalente a B, por lo tanto γ tiene que ser alguna de las $\phi(\alpha_1), \phi(\alpha_2), \ldots, \phi(\alpha_k)$.

$\therefore$ $k = l$ (tienen el mismo número de elementos distintos)

Ahora bien, supongamos que $\alpha_1, \alpha_2, \ldots, \alpha_k$ y $\beta_1, \beta_2, \ldots, \beta_k$ son los elementos distintos de A y B respectivamente.

Puesto que $k \leq q$, y Sq es un q-'pliego' transitivo sobre F, entonces existe $\phi \in Sq$ tal que $\phi(\alpha_i) = \beta_i$ para $i=1,2,\ldots,k$

Para cada i, α_i aparece en la misma posición de A como β_i lo hace en B, es decir,

$$\phi(\alpha_s) = \beta_s \quad \forall \; a_{ij} \quad si \quad (i,j) \in \Omega_s = B_s, \; i.e., \; \phi(a_{ij}) = b_{ij} \; \forall \; i,j$$

sin perdida de generalidad, podemos reordenar los términos, por lo tanto $\phi(A) = B$.

□

Sea $N(k,Sq)$ el número de matrices $A \in Fmn$ con k elementos distintos tales que $\mu(A,Sq) = \frac{q!}{(q-k)!}$.

Determinamos este número en el siguiente teorema

TEOREMA 3.3. El número $N(k,Sq)$ está dado por

$$N(k,Sq) = \frac{q!}{(q-k)!} \sum \prod_{i=1}^{s} \frac{1}{l_i!} \prod_{j=0}^{l_i-1} \binom{mn - \sum_{r=1}^{i-1} l_r m_r - j m_i}{m_i} \quad \ldots(3.1)$$

donde la suma es sobre todas las particiones $l_1 m_1 + l_2 m_2 + \ldots + l_s m_s = mn$ tales que $l_1 + l_2 + \ldots + l_s = k$ y donde $\binom{mn - \sum_{r=1}^{i-1} l_r m_r - j m_i}{m_i}$ denota las combinaciones de $mn - \sum_{r=1}^{i-1} l_r m_r - j m_i$ elementos tomados de m_i en m_i

Demostración.

Supongamos que $A \in Fmn$ tiene k elementos distintos $\alpha_1, \alpha_2, \ldots, \alpha_k$ donde α_r aparece m_r veces en A, así que $m_1 + m_2 + \ldots + m_k = mn$.

Supongamos que en esta partición de mn, son distintos $m_1, m_2, \ldots, m_s$ y que m_i aparece l_i veces en esa suma, o sea, $l_1 m_1 + l_2 m_2 + \ldots + l_s m_s = mn$, donde $l_1 + l_2 + \ldots + l_s = k$.

Si $\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1l_1}$ aparecen m_1 veces en A, donde $\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1l_1} \in \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ entonces

α_{11} se puede colocar de $\binom{mn}{m_1}$ maneras,

α_{12} se puede colocar de $\binom{mn-m_1}{m_1}$ maneras,

α_{13} se puede colocar de $\binom{mn-2m_1}{m_1}$ maneras,

. . . . . .

. . . . . .

. . . . . .

α_{1l_1} se puede colocar de $\binom{mn-(l_1-1)m_1}{m_1}$ maneras,

por lo que tenemos que $\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1l_1}$ se pueden colocar, no importando el orden, de

$$\frac{1}{l_1!}\binom{mn}{m_1}\binom{mn-m_1}{m_1}\cdots\binom{mn-l_{1-1}m_1}{m_1} = \frac{1}{l_1!}\prod_{j=0}^{l_1-1}\binom{mn-jm_1}{m_1}$$

maneras. Por lo tanto, ya se llenaron $l_1 m_1$ lugares.

Si $\alpha_{21}, \alpha_{22}, \ldots, \alpha_{2l_2}$ aparecen m_2 veces en A, donde $\alpha_{21}, \alpha_{22}, \ldots, \alpha_{2l_2} \in \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ entonces

α_{21} se puede colocar de $\binom{mn-l_1m_1}{m_2}$ maneras,

α_{22} se puede colocar de $\binom{mn-l_1m_1-m_2}{m_2}$ maneras,

α_{23} se puede colocar de $\binom{mn-l_1m_1-2m_2}{m_2}$ maneras,

. . . .

. . . .

. . . .

α_{2l_2} se puede colocar de $\binom{mn-l_1m_1-(l_2-1)m_2}{m_2}$ maneras,

entonces $\alpha_{21}, \alpha_{22}, \ldots, \alpha_{2l_2}$ se pueden colocar, no importando el orden, de

$$\frac{1}{l_2!}\binom{mn-l_1m_1}{m_2}\binom{mn-l_1m_1-m_2}{m_2}\cdots\binom{mn-l_1m_1-(l_2-1)m_2}{m_2} = \frac{1}{l_2!}\prod_{j=0}^{l_2-1}\binom{mn-l_1m_1-jm_2}{m_2}$$

maneras. Por lo que ya se llenaron en A, $l_1 m_1 + l_2 m_2$ lugares.

Similarmente, para colocar $\alpha_{i1}, \alpha_{i2}, \ldots \alpha_{il_i}$ en A, donde $\alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{il_i} \in \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ aparecen cada una m_i veces en A, teniendo en cuenta que ya se llenaron $l_1 m_1 + l_2 m_2 + \ldots + l_{i-1} m_{i-1}$ lugares, se puede hacer de

$$\frac{1}{l_i!}\prod_{j=0}^{l_i-1}\binom{mn-\sum_{r=1}^{i-1} l_r m_r - jm_i}{m_i}$$

maneras.

Por consiguiente, para una partición fija de $mn = l_1 m_1 + l_2 m_2 + \ldots + l_s m_s$, donde $l_1 + l_2 + \ldots + l_s = k$ existen

$$\prod_{i=1}^{s} \frac{1}{l_i!} \prod_{j=0}^{l_i - 1} \binom{mn - \sum_{\tau=1}^{i-1} l_\tau m_\tau - jm_i}{m_i} \qquad (3.4)$$

caminos para construir matrices $A \in Fmn$ con k elementos distintos.

Notemos que en $\sum_{\tau=1}^{i-1} l_\tau m_\tau$,

si $i = s$, tenemos $\sum_{\tau=1}^{s-1} l_\tau m_\tau = l_1 m_1 + l_2 m_2 + \ldots + l_{s-1} m_{s-1}$,

si $i = s-1$, tenemos $\sum_{\tau=1}^{(s-1)-1} l_\tau m_\tau = l_1 m_1 + l_2 m_2 + \ldots + l_{s-2} m_{s-2}$,

. . . .

. . . .

. . . .

si $i = 2$, tenemos $\sum_{\tau=1}^{2-1} l_\tau m_\tau = l_1 m_1$,

por lo que suponemos, cuando $i = 1$, que $\sum_{\tau=1}^{i-1} l_\tau m_\tau = 0$

Así que el número total de matrices $A \in Fmn$ con k diferentes elementos fijos, tales que $\mu(A, Sq) = \frac{q!}{(q-k)!}$ se obtiene sumando en (3.4) sobre todas las particiones $l_1 m_1 + l_2 m_2 + \ldots + l_s m_s = mn$, donde $l_1 + l_2 + \ldots + l_s = k$.

Para obtener $N(k, Sq)$ multiplicamos por $\frac{q!}{(q-k)!}$ puesto que los k diferentes elementos pueden ser escogidos de $q(q-1)\cdots(q-k+1)$ maneras, y terminamos.

□

Sin embargo, aunque todas las matrices contadas en (3.1) tienen k diferentes elementos, pueden ser no equivalentes relativas en Sq.

Si C(k,q) es el número de clases de equivalencia de orden $\frac{q!}{(q-k)!}$ y $\lambda(Sq)$ es el número total de clases inducidas por Sq, tenemos

COROLARIO 3.4. Para cada $k = 1, 2, \ldots, q$.

$$C(k,q) = \frac{(q-k)!\, N(k,S_q)}{q!}$$

y $$\lambda(Sq) = \sum_{k=1}^{q} C(k,q)$$

Demostración.

Tenemos que $N(k,Sq) = \frac{q!}{(q-k)!}\, C(k,q)$

esto es,

$$C(k,q) = \sum \prod_{i=1}^{s} \frac{1}{j_i!} \prod_{j=0}^{j_i-1} \binom{mn - \sum_{r=1}^{i-1} j_r m_r - j m_i}{m_i}$$

que es el número de clases de equivalencia de orden $\frac{q!}{(q-k)!}$

y por lo tanto, el número total de clases inducidas por Sq es

$$\lambda(Sq) = \sum_{k=1}^{q} C(k,q)$$

□

Como una ilustración, supongamos $q = 3$, y $m = n = 2$.

Usando (3.1), tenemos

Si k=1, es decir, si los distintos elementos de $A \in Fmn$ es únicamente uno, supongamos $\alpha_1 \in F(3)$, entonces α_1 aparece 4 veces, por lo que se tiene $m_1 = 4$, y por lo tanto,

$$1 \cdot 4 = 4 \text{ , donde } \quad l_1 = 1, \quad m_1 = 4$$

(la única partición es $l_1 m_1 = 4$)

$$\therefore \quad \binom{4}{4} = \frac{4!}{(4-4)!\,4!} = 1$$

$$\therefore \quad N(1,S_3) = \frac{3!}{(3-1)!} \cdot 1 = \frac{3!}{2!} \cdot 1 = 3$$

$$\therefore \quad N(1,S_3) = 3 \, .$$

Ahora, si k=2, supongamos que los dos elementos diferentes son $\alpha_1, \alpha_2 \in F(3)$, entonces las particiones posibles son:

i) Si α_1 aparece una vez, entonces α_2 aparece 3 veces, por lo que tenemos $m_1 = 1$, $l_1 = 1$, $m_2 = 3$, $l_2 = 1$.

$$\therefore \quad 1 \cdot 1 + 1 \cdot 3 = 4 \, , \qquad l_1 + l_2 = l_3 = 2 \, .$$

$$\therefore \quad \binom{4}{1}\binom{3}{3} = \frac{4!}{(4-1)!\,1!} \cdot \frac{3!}{(3-3)!\,3!} = 4$$

este conjunto de matrices tales que α_1, α_2 aparecen una y tres veces, respectivamente, es

$$\left\{ \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_2 & \alpha_2 \end{pmatrix}, \begin{pmatrix} \alpha_2 & \alpha_1 \\ \alpha_2 & \alpha_2 \end{pmatrix}, \begin{pmatrix} \alpha_2 & \alpha_2 \\ \alpha_1 & \alpha_2 \end{pmatrix}, \begin{pmatrix} \alpha_2 & \alpha_2 \\ \alpha_2 & \alpha_1 \end{pmatrix} \right\}$$

ii) Si α_1 aparece 2 veces, entonces α_2 aparece 2 veces, por lo que tenemos, $m_1 = m_2 = 2$, y $l = 2$

$$\therefore \quad l\, m_1 = mn, \text{ es decir, } \quad 2 \cdot 2 = 4$$

$$\therefore \quad \frac{1}{2!}\binom{4}{2}\binom{2}{2} = \frac{1}{2!}\cdot\frac{4!}{2!(4-2)!}\cdot\frac{2!}{(2-2)!\,2!} = \frac{1}{2!}\cdot\frac{4!}{2!2!}\cdot\frac{2!}{0!2!} = 3$$

Por consiguiente, de i) y ii) tenemos

$$N(2,S_3) = \frac{3!}{(3-2)!}\,(4+3) = 6\cdot 7 = 42$$

$$\therefore \quad N(2,S_3) = 42 .$$

Ahora bien, si $k = 3$, supongamos que los 3 elementos diferentes son $\alpha_1, \alpha_2, \alpha_3 \in F(3)$.

Si α_1 aparece una vez y α_2 aparece también una vez, entonces α_3 aparece 2 veces, por lo que tenemos que $m_1 = 1$, $l_1 = 1$; $m_2 = 1$, $l_2 = 1$; $m_3 = 2$, $l_3 = 1$
como $m_1 = m_2$ tenemos $l\, m_1 + l_3 m_3 = mn = 4$, es decir,
$2\cdot 1 + 1\cdot 2 = 4$, donde $l = 2$.

$$\therefore \quad \frac{1}{2!}\binom{4}{1}\binom{3}{1}\binom{2}{2} = \frac{1}{2!}\cdot\frac{4!}{(4-1)!\,1!}\cdot\frac{3!}{(3-1)!\,1!}\cdot\frac{2!}{(2-2)!\,2!}$$

$$= 6$$

$$\therefore \quad N(3,S_3) = \frac{3!}{(3-3)!}\cdot 6 = \frac{3!}{0!}\cdot 6 = 36$$

$$\therefore \quad N(3,S_3) = 36 .$$

Sea $F(3)$ el campo con 3 elementos: $0, 1, 2$, y sea S_3 el grupo simétrico con los mismos elementos: $0, 1, 2$, es decir,

$$S_3 = \left\{ \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 2 & 1 & 0 \end{pmatrix} \right\}$$

Las clases de equivalencia formadas por las matrices $A \in F_{2\times 2}$ cuyas entradas están en $F(3)$, son:

a) Para cuando A tiene un elemento diferente:

$$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix} \right\}$$

es decir, $C(1,3) = 1$, $N(1,S_3) = 3$.

b) Para cuando A tiene dos elementos diferentes:

$$\left\{ \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 0 & 0 \end{pmatrix} \right\}$$

$$\left\{ \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 2 & 0 \end{pmatrix} \right\}$$

$$\left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right\}$$

$$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

$$\left\{\begin{pmatrix}0&0\\1&0\end{pmatrix},\begin{pmatrix}0&0\\2&0\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}1&1\\2&1\end{pmatrix},\begin{pmatrix}2&2\\0&2\end{pmatrix},\begin{pmatrix}2&2\\1&2\end{pmatrix}\right\}$$

$$\left\{\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}2&0\\0&0\end{pmatrix},\begin{pmatrix}0&1\\1&1\end{pmatrix},\begin{pmatrix}2&1\\1&1\end{pmatrix},\begin{pmatrix}0&2\\2&2\end{pmatrix},\begin{pmatrix}1&2\\2&2\end{pmatrix}\right\}$$

$$\left\{\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}0&2\\0&0\end{pmatrix},\begin{pmatrix}1&0\\1&1\end{pmatrix},\begin{pmatrix}1&2\\1&1\end{pmatrix},\begin{pmatrix}2&0\\2&2\end{pmatrix},\begin{pmatrix}2&1\\2&2\end{pmatrix}\right\}$$

es decir,

$$C(2,3) = 7, \quad N(2,S_3) = 42.$$

c) Para cuando A tiene 3 elementos diferentes:

$$\left\{\begin{pmatrix}0&0\\1&2\end{pmatrix},\begin{pmatrix}0&0\\2&1\end{pmatrix},\begin{pmatrix}1&1\\0&2\end{pmatrix},\begin{pmatrix}1&1\\2&0\end{pmatrix},\begin{pmatrix}2&2\\0&1\end{pmatrix},\begin{pmatrix}2&2\\1&0\end{pmatrix}\right\}$$

$$\left\{\begin{pmatrix}0&2\\1&1\end{pmatrix},\begin{pmatrix}2&0\\1&1\end{pmatrix},\begin{pmatrix}0&1\\2&2\end{pmatrix},\begin{pmatrix}1&0\\2&2\end{pmatrix},\begin{pmatrix}1&2\\0&0\end{pmatrix},\begin{pmatrix}2&1\\0&0\end{pmatrix}\right\}$$

$$\left\{\begin{pmatrix}0&1\\0&2\end{pmatrix},\begin{pmatrix}0&2\\0&1\end{pmatrix},\begin{pmatrix}1&2\\1&0\end{pmatrix},\begin{pmatrix}1&0\\1&2\end{pmatrix},\begin{pmatrix}2&0\\2&1\end{pmatrix},\begin{pmatrix}2&1\\2&0\end{pmatrix}\right\}$$

$$\left\{\begin{pmatrix}1&0\\2&0\end{pmatrix},\begin{pmatrix}2&0\\1&0\end{pmatrix},\begin{pmatrix}0&1\\2&1\end{pmatrix},\begin{pmatrix}2&1\\0&1\end{pmatrix},\begin{pmatrix}0&2\\1&2\end{pmatrix},\begin{pmatrix}1&2\\0&2\end{pmatrix}\right\}$$

$$\left\{\begin{pmatrix}0&2\\1&0\end{pmatrix},\begin{pmatrix}0&1\\2&0\end{pmatrix},\begin{pmatrix}1&2\\0&1\end{pmatrix},\begin{pmatrix}1&0\\2&1\end{pmatrix},\begin{pmatrix}2&1\\0&2\end{pmatrix},\begin{pmatrix}2&0\\1&2\end{pmatrix}\right\}$$

$$\left\{\begin{pmatrix}1&0\\0&2\end{pmatrix},\begin{pmatrix}2&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\1&2\end{pmatrix},\begin{pmatrix}2&1\\1&0\end{pmatrix},\begin{pmatrix}0&2\\2&1\end{pmatrix},\begin{pmatrix}1&2\\2&0\end{pmatrix}\right\}$$

es decir,

$$C(3,3) = 6, \quad N(3,S_3) = 36$$

Además,

$$\lambda(S_3) = C(1,3) + C(2,3) + C(3,3) = 14$$

donde $\lambda(S_3)$ es el número total de clases inducidas por S_3 y

$$N(1,S_3) + N(2,S_3) + N(3,S_3) = 81 = \#\left\{A \in F_{2\times 2}\right\}$$

4. GRUPOS CICLICOS.

Sea Ω un grupo cíclico de orden s, es decir, existe $\phi \in \Omega$ tal que $\Omega = \langle \phi \rangle$, $\phi^s = 1$.

Sea H(t) el subgrupo de Ω de orden t.

Sabemos que $t \mid s$ puesto que :

Sea $H(t) = \langle \psi \rangle$ donde $\psi^r = 1$.

Como $\phi^n = \psi$ para alguna $n \in \mathbb{Z}^+$

$$\Rightarrow \quad \psi^s = (\phi^n)^s = (\phi^s)^n = 1^n = 1$$

Sea $s = tq + r$, $0 \leq r < t$

$$\Rightarrow \quad 1 = \psi^s = \psi^{tq+r} = \psi^{tq}\psi^r = 1 \cdot \psi^r = \psi^r$$

$$\therefore \quad \psi^r = 1$$

como el orden de ψ es t, tenemos que r = 0

$$\therefore \quad t \mid s \quad \therefore \quad H(t) = \langle \phi^{s/r} \rangle .$$

Ahora, sea $\lambda(t)$ el número de elementos invariantes de H(t), y supongamos que M(t,m,n) denota el número de matrices $A \in Fmn$ tal que $Aut(A,\Omega) = H(t)$, es decir,

$$\lambda(t) = \#\{a \in F / \psi(a) = a \ \forall \ \psi \in H(t)\}$$

$$M(t,m,n) = \#\{A \in Fmn / \psi(A) = A \ \forall \ \psi \in H(t) \text{ y sólo para éstas}\}$$

$$= \#\{A \in Fmn / \ Aut(A,\Omega) = H(t)\}$$

Por el teorema 2.2, $\lambda(t)^{mn}$ cuenta el número de matrices $A \in Fmn$ tal que $\psi(A) = A \ \forall \ \psi \in H(t)$, es decir,

sea $\int(t)^{mn} = \#\left\{ A \in Fmn / \Psi(A) = A \ \forall \ \Psi \in H(t) \right\}$

sea $M = \left\{ A \in Fmn / \Psi(A) = A \ \forall \ \Psi \in H(t) \right\}$

es decir, $\int(t)^{mn} = \# M$.

Sin embargo, tenemos que quitarle a M aquellas matrices que pudieran tener automorfismos que no estén en H(t), es decir

$$\left\{ B \in M / \exists \ \alpha \in \Omega - H(t) \ni \alpha(B) = B \right\}$$

Ahora ¿ de qué forma son esas matrices $B \in M$ tales que existe $\alpha \in \Omega - H(t)$, $\alpha(B) = B$?

Sea $\alpha \in \Omega - H(t)$ tal que $\alpha^u = 1$, $u \in Z^+$ y u el orden de α, donde $u \mid s$

Como $\alpha \in \Omega$, existe $\gamma \in Z$ tal que $\alpha = \phi^\gamma$,

$$1 = (\alpha^u)^u = \left[(\phi^\gamma)^u\right]^u$$

y

$$1 = (\alpha^u)^\tau = \left[(\phi^\gamma)^u\right]^\tau , \quad u \neq \tau$$

$$\Rightarrow \quad 1 = \phi^{\gamma uu} = \phi^{\gamma u \tau}$$

$$\Rightarrow \quad \phi^u = \phi^\tau \Rightarrow \phi^{u-\tau} = 1 \Rightarrow s \mid u-\tau$$

como $t \mid s$, existe $m \in Z$ tal que $s = tm$, por lo que tenemos

$$s \mid u - t \Rightarrow u - t = sx , \ x \in Z$$

$$\Rightarrow \quad u = sx + t \Rightarrow u = (tm)x + t = t(mx + 1)$$

$$\therefore \quad t \mid u$$

Ahora, $u \nmid t$ porque si $u \mid t \Rightarrow t = un$, $n \in \mathbb{Z}$

$\Rightarrow \alpha^{\tau} = (\alpha^{u})^{n} = 1$ ↯ porque $\alpha \notin H(t)$

Por consiguiente, tenemos el teorema siguiente

TEOREMA 4.1. Para cada divisor t de s,

$$M(t,m,n) = \mathfrak{J}(t)^{mn} - \sum M(u,m,n) \quad \ldots\ldots\ldots\ldots (4.1)$$

donde la suma es sobre toda $u \mid s$, $t \mid u$ y $t \neq u$.

COROLARIO 4.2. Para cada divisor t de s, hay

$\frac{tM(t,m,n)}{s}$ clases de orden $\frac{s}{t}$ y

$$\lambda(\Omega) = \frac{1}{s} \sum_{\tau \mid s} tM(t,m,n) \quad \ldots\ldots\ldots\ldots (4.2)$$

Demostración.

Sea $\overline{A} = \left\{ B \in Fmn \,/\, \exists\, \psi \in \Omega \Rightarrow \psi(A) = B \right\}$

¿ Cuántas clases hay de orden $\frac{s}{t}$?

Por (2.0), para toda $B \in \overline{A}$, $v(A,\Omega) = v(B,\Omega)$,

pero

$$v(A,\Omega) = \frac{s}{\mu(A,\Omega)} = \frac{s}{s/t} = t$$

todas estas matrices $A \in Fmn$ tienen en común que su grupo de automorfismos tienen orden t, es decir, si k es el número de clases de orden s/t,

$$\frac{s}{t}\cdot k = \#\left\{A \in Fmn \;/\; Aut(A,\Omega) = H(t)\right\}$$

$$\frac{s}{t}\cdot k = M(t,m,n)$$

$$\therefore \qquad k = \frac{tM(t,m,n)}{s}$$

Ahora bien, $\lambda(\Omega)$ es el número total de clases inducidas por Ω y

$\frac{tM(t,m,n)}{s}$ es el número de clases de orden $\frac{s}{t}$

$$\therefore \qquad \lambda(\Omega) = \sum_{t|s} \frac{tM(t,m,n)}{s} = \frac{1}{s}\sum_{t|s} tM(t,m,n)$$

□

Si $F_{H(t)}$ denota el conjunto de elementos invariantes de $H(t)$, y A_d representa el conjunto de elementos distintos de la matriz $A \in Fmn$, tenemos

COROLARIO 4.3. Si $A \in Fmn$, entonces $v(A,\Omega) = t$ ó equivalentemente, $\mu(A,\Omega) = \frac{s}{t}$ si y sólo si $H(t)$ es el mayor subgrupo de Ω tal que $A_d \subseteq F_{H(t)}$

Demostración.

$\Rightarrow$) Supongamos $v(A,\Omega) = \#\left\{\Psi\in\Omega \;/\; \Psi(A)=A\right\} = t$,
es decir, $\mu(A,\Omega) = \frac{s}{t}$

Sea G subgrupo de Ω tal que $|G| = r$ y
$H(t) \subseteq G \subset \Omega$ con la propiedad $A_d \subset F_G$
Por lo tanto, si $a \in A_d$ entonces $\Psi(a) = a \;\forall \Psi \in G$
es decir, existen al menos r morfismos en Ω
tal que $\Psi(A) = A$, i.e., $v(A,\Omega) \geq r$
pero $t \leq r \Rightarrow r = t$
$\therefore \quad |G| = t$

$\Leftarrow$) Supongamos que H(t) es el subgrupo de Ω más grande tal que $A_d \subset F_{H(t)}$
es decir, existen t morfismos en H(t) para los cuales

$\Psi(a_{ij}) = a_{ij}$ esto es $\Psi(A) = A$.

Ahora bien, si $\exists\ \phi \in \Omega - H(t) \Rightarrow \phi(A) = A$

$\Rightarrow \quad A_d \subset F_{H(t)\cup\{\phi\}}$ ∇

ya que H(t) es el máximo subgrupo de Ω con esa propiedad

$\therefore \quad v(A,\Omega) = t$, es decir, $\mu(A,\Omega) = \frac{s}{t}$

□

Decimos que dos grupos Ω_1 y Ω_2 inducen descomposiciones equivalentes de Fmn, si inducen el mismo número de clases del mismo tamaño.

TEOREMA 4.3. Supongamos Ω_1, Ω_2 grupos cíclicos de orden s. Entonces Ω_1 y Ω_2 inducen descomposiciones equivalentes de Fmn si y sólo si para cada divisor t de s, $H_1(t)$ y $H_2(t)$ tienen el mismo número de elementos invariantes, donde $H_i(t)$ denota el subgrupo de Ω_i de orden t, para $i = 1, 2$.

Demostración.

$\Longrightarrow$) Supongamos que Ω_1 y Ω_2 inducen descomposiciones equivalentes de Fmn. Por lo tanto, Ω_1 y Ω_2 inducen el mismo número de clases del mismo tamaño.

Por el Corolario 4.2, para cada divisor t de s, hay $\frac{tM(t,m,n)}{s}$ clases de orden $\frac{s}{t}$

Además, supongamos que

$\# P_{H_1(t)} = k$ y $\# P_{H_2(t)} = r$ con $k \neq r$.

En particular, si $t = s$, entonces existen

$\frac{tM(t,m,n)}{s} = M(t,m,n)$ clases de orden $\frac{s}{t} = 1$.

$\therefore$ en Ω_1, si $t = s$, existen $M(t,m,n) = M(s,m,n)$ clases de orden 1, es decir

$M(s,m,n) = f(s)^{mn} = k^{mn}$

Análogamente en Ω_2, si $t = s$, existen $M(s,m,n)$ clases de orden 1, es decir

$M(s,m,n) = f(s)^{mn} = r^{mn}$

Pero como Ω_1 y Ω_2 inducen descomposiciones

equivalentes, tenemos que $k^{mn} = r^{mn} \Rightarrow k = r$ $\forall$

$\therefore \quad \# F_{H_1(t)} = \# F_{H_2(t)}$

$\Leftarrow$) Supongamos que $\# F_{H_1(t)} = \# F_{H_2(t)}$

Por el Corolario 4.2,

$\forall \; t \mid s \; \exists \quad \frac{tM(t,m,n)}{s}$ clases de orden $\frac{s}{t}$

tanto en Ω_1 como en Ω_2

$\therefore \quad \Omega_1$ y Ω_2 inducen descomposiciones equivalentes de Fmn.

□

Como una ilustración, supongamos $q = 3$, $m = n = 2$, y $\phi(x) = 2x$, $\phi \in \Omega$; así que en notación de ciclos, tenemos $\phi = (1\ \ 2)$.

$$\text{Si} \quad \Omega = \langle \phi \rangle = \langle (1\ \ 2) \rangle = \left\langle \begin{pmatrix} 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix} \right\rangle$$

entonces $\Omega = \left\{ \mathcal{C}, (1\ \ 2) \right\}$ donde $\mathcal{C} = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix}$, $|\Omega| = 2$

Ahora bien,

$$H(1) = \langle (1\ \ 2)^{2/1} \rangle = \langle (1\ \ 2)^2 \rangle = \langle \mathcal{C} \rangle = \mathcal{C}$$

$$\therefore \quad H(1) = \left\{ \mathcal{C} \right\}$$

$\therefore$ $\ell(1) = 3$ que es el número de elementos invariantes de $H(1)$.

$$H(2) = \langle (1\ \ 2)^{2/2} \rangle = \langle (1\ \ 2) \rangle = \left\{ (1\ \ 2), \mathcal{C} \right\}$$

$$\therefore \quad H(2) = \left\{ \mathcal{C}, (1\ \ 2) \right\}$$

$\therefore$ $\ell(2) = 1$ que es el número de elementos invariantes de $H(2)$.

Sea $M(t,m,n) = \#\left\{ A \in Fmn \,/\, Aut(A,\Omega) = H(t) \text{ y sólo para éstas} \right\}$

$$\therefore \quad M(1,2,2) = \ell(1)^{mn} - M(2,2,2)$$

es decir $M(1,2,2) = 3^4 - M(2,2,2)$

y $M(2,2,2) = \ell(2)^4 = 1^4 = 1$

$$\therefore \quad M(1,2,2) = 80$$

Además, tenemos que el número de clases de orden 2

es $$\frac{1\cdot M(1,2,2)}{2} = \frac{1\cdot 80}{2} = 40$$

y que el número de clases de orden 1 es

$$\frac{2\cdot M(2,2,2)}{2} = \frac{2\cdot 1}{2} = 1$$

Por consiguiente, tenemos que hay 40 clases de orden 2 y una clase de orden 1

$$\therefore \quad \lambda(\Omega) = 41$$

Estas clases son las siguientes:

i) La clase de orden 1 es

$$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$$

ya que si $A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $\Omega = \left\{ \varphi, (1\ \ 2) \right\}$

donde $\Psi = (1\ \ 2)$, tenemos que $\varphi(A) = \Psi(A) = A$.

ii) Las clases de orden 2 son:

1.- $$\left\{ \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix} \right\}$$

2.- $$\left\{ \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix} \right\}$$

3.- $$\left\{ \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 0 & 0 \end{pmatrix} \right\}$$

4.- $$\left\{ \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 2 & 2 \end{pmatrix} \right\}$$

5.- $\left\{\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}, \begin{pmatrix}2 & 1\\ 2 & 1\end{pmatrix}\right\}$

6.- $\left\{\begin{pmatrix}1 & 0\\ 1 & 0\end{pmatrix}, \begin{pmatrix}2 & 0\\ 2 & 0\end{pmatrix}\right\}$

7.- $\left\{\begin{pmatrix}0 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}0 & 2\\ 0 & 2\end{pmatrix}\right\}$

8.- $\left\{\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}, \begin{pmatrix}2 & 1\\ 1 & 2\end{pmatrix}\right\}$

9.- $\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}\right\}$

10.- $\left\{\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}0 & 2\\ 2 & 0\end{pmatrix}\right\}$

11.- $\left\{\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}, \begin{pmatrix}2 & 2\\ 2 & 1\end{pmatrix}\right\}$

12.- $\left\{\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}2 & 2\\ 2 & 0\end{pmatrix}\right\}$

13.- $\left\{\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}0 & 0\\ 0 & 2\end{pmatrix}\right\}$

14.- $\left\{\begin{pmatrix}1 & 1\\ 2 & 1\end{pmatrix}, \begin{pmatrix}2 & 2\\ 1 & 2\end{pmatrix}\right\}$

15.- $\left\{\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}2 & 2\\ 0 & 2\end{pmatrix}\right\}$

16.- $\left\{\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 2 & 0\end{pmatrix}\right\}$

17.- $\left\{\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}, \begin{pmatrix}0 & 2\\ 2 & 2\end{pmatrix}\right\}$

18.- $\left\{\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}, \begin{pmatrix}1 & 2\\ 2 & 2\end{pmatrix}\right\}$

19.- $\left\{\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix}2 & 0\\ 0 & 0\end{pmatrix}\right\}$

20.- $\left\{\begin{pmatrix}1 & 2\\ 1 & 1\end{pmatrix}, \begin{pmatrix}2 & 1\\ 2 & 2\end{pmatrix}\right\}$

21.- $\left\{\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}, \begin{pmatrix}2 & 0\\ 2 & 2\end{pmatrix}\right\}$

22.- $\left\{\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 2\\ 0 & 0\end{pmatrix}\right\}$

23.- $\left\{\begin{pmatrix}1 & 1\\ 2 & 0\end{pmatrix}, \begin{pmatrix}2 & 2\\ 1 & 0\end{pmatrix}\right\}$

24.- $\left\{\begin{pmatrix}1 & 1\\ 0 & 2\end{pmatrix}, \begin{pmatrix}2 & 2\\ 0 & 1\end{pmatrix}\right\}$

25.- $\left\{\begin{pmatrix}0 & 0\\ 1 & 2\end{pmatrix}, \begin{pmatrix}0 & 0\\ 2 & 1\end{pmatrix}\right\}$

26.- $\left\{\begin{pmatrix}2 & 0\\ 1 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 2 & 2\end{pmatrix}\right\}$

27.- $\left\{\begin{pmatrix}0 & 2\\ 1 & 1\end{pmatrix}, \begin{pmatrix}0 & 1\\ 2 & 2\end{pmatrix}\right\}$

28.- $\left\{\begin{pmatrix}1 & 2\\ 0 & 0\end{pmatrix}, \begin{pmatrix}2 & 1\\ 0 & 0\end{pmatrix}\right\}$

29.- $\left\{\begin{pmatrix}1 & 2\\ 1 & 0\end{pmatrix}, \begin{pmatrix}2 & 1\\ 2 & 0\end{pmatrix}\right\}$

30.- $\left\{\begin{pmatrix}1 & 0\\ 1 & 2\end{pmatrix}, \begin{pmatrix}2 & 0\\ 2 & 1\end{pmatrix}\right\}$

31.- $\left\{\begin{pmatrix}0 & 1\\ 0 & 2\end{pmatrix}, \begin{pmatrix}0 & 2\\ 0 & 1\end{pmatrix}\right\}$

32.- $\left\{\begin{pmatrix}2 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 2\\ 0 & 2\end{pmatrix}\right\}$

33.- $\left\{\begin{pmatrix}0 & 1\\ 2 & 1\end{pmatrix}, \begin{pmatrix}0 & 2\\ 1 & 2\end{pmatrix}\right\}$

34.- $\left\{\begin{pmatrix}1 & 0\\ 2 & 0\end{pmatrix}, \begin{pmatrix}2 & 0\\ 1 & 0\end{pmatrix}\right\}$

35.- $\left\{\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}, \begin{pmatrix}2 & 1\\ 0 & 2\end{pmatrix}\right\}$

36.- $\left\{\begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}, \begin{pmatrix}2 & 0\\ 1 & 2\end{pmatrix}\right\}$

37.- $\left\{\begin{pmatrix}0 & 2\\ 1 & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\ 2 & 0\end{pmatrix}\right\}$

38.- $\left\{\begin{pmatrix}2 & 1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}1 & 2\\ 2 & 0\end{pmatrix}\right\}$

39.- $\left\{\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}, \begin{pmatrix}0 & 2\\ 2 & 1\end{pmatrix}\right\}$

40.- $\left\{\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}, \begin{pmatrix}2 & 0\\ 0 & 1\end{pmatrix}\right\}$

5. PRODUCTO DIRECTO.

Supongamos $\Omega = H_1 \pi H_2$ donde $H_i = \langle \phi_i \rangle$, $i = 1, 2$

Si $\alpha \in F$, sea $\sigma_\phi(\alpha)$ el ciclo de ϕ conteniendo a α.

TEOREMA 5.1.

$$\mathrm{Aut}(A, \Omega) = \mathrm{Aut}(A, H_1) \; \pi \; \mathrm{Aut}(A, H_2) \quad \forall \quad A \in \mathrm{Fmn}$$

$$\iff \quad \sigma_{\phi_1}(\alpha) \cap \sigma_{\phi_2}(\alpha) = \{\alpha\} \; \forall \alpha \in F \quad \ldots\ldots\ldots (5.1)$$

Demostración.

$\Longrightarrow$) Supongamos

$$\mathrm{Aut}(A, \Omega) = \mathrm{Aut}(A, H_1) \; \pi \; \mathrm{Aut}(A, H_2) \quad \forall \quad A \in \mathrm{Fmn}$$

Sea $\alpha \in F$ tal que $\sigma_{\phi_1}(\alpha) \cap \sigma_{\phi_2}(\alpha)$ contiene alguna $\beta \in F$, $\beta \neq \alpha$.

Entonces existen $k_1, k_2 \in \mathbb{Z}^+$ tal que

$$\phi_1^{k_1}(\beta) = \alpha \qquad y \qquad \phi_2^{k_2}(\alpha) = \beta$$

así que $\phi_1^{k_1} \cdot \phi_2^{k_2}(\alpha) = \alpha$.

Sea $A = (a_{ij})$, donde $a_{ij} = \alpha \; \forall \; i, j$; entonces $\phi_1^{k_1} \cdot \phi_2^{k_2}(A) = A$, así que por hipótesis $\phi_2 \in \mathrm{Aut}(A, H_2)$, es decir, $\phi_2^{k_2}(A) = A$, lo que implica $\phi_2^{k_2}(\alpha) = \alpha$ que es una contradicción con $\phi_2^{k_2}(\alpha) = \beta$, $\alpha \neq \beta$.

$\Leftarrow$) Supongamos $\sigma_{\phi_1}(\alpha) \cap \sigma_{\phi_2}(\alpha) = \{\alpha\} \ \forall \alpha \in F$

Sea $A = (a_{ij})$ arbitraria.

Claramente $Aut(A, H_1) \pi Aut(A, H_2) \subseteq Aut(A, \Omega)$

Sea $\psi_1 \cdot \psi_2(A) = A$ con $\psi_1 \in H_1$, $\psi_2 \in H_2$

$\Rightarrow \psi_1 \cdot \psi_2 \in Aut(A, \Omega)$

Así pues, $\psi_1 \cdot \psi_2(a_{ij}) = a_{ij} \ \forall \ i, j$.

Si $\psi_2(a_{ij}) = a_{ij} \ \forall \ i, j$ entonces $\psi_1(A) = \psi_2(A) = A$ y terminamos.

Supongamos que existe a_{ij} tal que $\psi_2(a_{ij}) = b \neq a_{ij}$ así que $\psi_1(b) = a_{ij}$ pero ahora $a_{ij}, b \in \sigma_{\phi_1}(a_{ij}) \cap \sigma_{\phi_2}(a_{ij})$ que contradice el hecho de que $\sigma_{\phi_1}(\alpha) \cap \sigma_{\phi_2}(\alpha) = \{\alpha\} \ \forall \alpha \in F$ □

COROLARIO 5.2. Bajo las hipótesis del Teorema 5.1,

$v(A, \Omega) = v(A, H_1) \ v(A, H_2)$ y $\mu(A, \Omega) = \mu(A, H_1) \ \mu(A, H_2)$

Demostración.

Por el Teorema 5.1, tenemos

$Aut(A, \Omega) = Aut(A, H_1) \pi Aut(A, H_2) \ \forall \ A \in Fmn$

$\Longleftrightarrow \quad \sigma_{\phi_1}(\alpha) \cap \sigma_{\phi_2}(\alpha) = \{\alpha\} \ \forall \alpha \in F$

entonces, como $\Omega = H_1 \pi H_2$ tenemos $|\Omega| = |H_1| \, |H_2|$ y

$Aut(A, \Omega) = Aut(A, H_1) \pi Aut(A, H_2)$

$\Rightarrow \quad v(A, \Omega) = v(A, H_1) \ v(A, H_2)$

además $v(A, \Omega) \ \mu(A, \Omega) = v(A, H_1) \ \mu(A, H_1) \ v(A, H_2) \ \mu(A, H_2)$.

$\Rightarrow \quad \mu(A, \Omega) = \mu(A, H_1) \ \mu(A, H_2)$

□

En el caso general, supongamos

$$\Omega = H_1 \pi H_2 \pi \ldots \pi H_k$$

Para cada $i = 1, 2, \ldots, k$ y $\alpha \in F$, sea

$$C_i(\alpha) = \bigcup_{\psi_i \in H_i} \overline{\sigma_{\psi_i}}(\alpha)$$

así que si $H_i = \langle \phi_i \rangle$ entonces $C_i(\alpha) = \overline{\sigma_{\phi_i}}(\alpha)$

Similarmente, si $j \neq i$, definimos

$$C_j(C_i(\alpha)) = \bigcup_{\gamma \in C_i(\alpha)} C_j(\gamma)$$

TEOREMA 5.3. Si $\Omega = H_1 \pi H_2 \pi \ldots \pi H_k$, $H_i = \langle \phi_i \rangle$, $i = 1, 2, \ldots, k$ entonces

$$\mathrm{Aut}(A, \Omega) = \mathrm{Aut}(A, H_1) \pi \ldots \pi \mathrm{Aut}(A, H_k) \quad \forall \; A \in Fmn$$

si y sólo si para cada $i = 1, 2, \ldots, k$ y $\alpha \in F$

$$C_i(\alpha) \cap C_{i_1}(\cdots(C_{i_s}(\alpha))) = \{\alpha\}$$

para toda s-tupla $(i_1, i_2, \ldots, i_s)$ no conteniendo a i, $1 \leq s < k$

Demostración.

$\Rightarrow$) Supongamos $\mathrm{Aut}(A, \Omega) = \mathrm{Aut}(A, H_1) \pi \ldots \pi \mathrm{Aut}(A, H_k)$

Sea $\beta \in C_i(\alpha) \cap C_{i_1}(\cdots(C_{i_s}(\alpha)))$, $\alpha \neq \beta$

$\Rightarrow \beta \in C_i(\alpha)$ i.e., $\beta \in \overline{\sigma_{\phi_i}}(\alpha)$ con $H_i = \langle \phi_i \rangle$

$\Rightarrow \exists \; r_i \in \mathbb{Z}^+ \ni \phi_i^{r_i}(\beta) = \alpha$

Por otra parte,

$$\beta \in C_{i_1}(\cdots(C_{i_s}(\alpha)))$$

$$\beta \in \bigcup_{\gamma_1 \in C_{i_2}(\cdots(C_{i_s}(\alpha)))} C_{i_1}(\gamma_1) \Rightarrow \exists\, r_1 \in \mathbb{Z}^+ ,\ \phi_{i_1}^{r_1}(\gamma_1) = \beta ,\ H_{i_1} = \langle \phi_{i_1} \rangle$$

si $\gamma_1 \in C_{i_2}(\cdots(C_{i_s}(\alpha)))$

$$\Rightarrow \gamma_1 \in \bigcup_{\gamma_2 \in C_{i_3}(\cdots(C_{i_s}(\alpha)))} C_{i_2}(\gamma_2) \Rightarrow \exists\, r_2 \in \mathbb{Z}^+ ,\ \phi_{i_2}^{r_2}(\gamma_2) = \gamma_1 ,\ H_{i_2} = \langle \phi_{i_2} \rangle$$

si $\gamma_2 \in C_{i_3}(\cdots(C_{i_s}(\alpha)))$

$$\Rightarrow \gamma_2 \in \bigcup_{\gamma_3 \in C_{i_4}(\cdots(C_{i_s}(\alpha)))} C_{i_3}(\gamma_3) \Rightarrow \exists\, r_3 \in \mathbb{Z}^+ ,\ \phi_{i_3}^{r_3}(\gamma_3) = \gamma_2 ,\ H_{i_3} = \langle \phi_{i_3} \rangle$$

$\vdots$

si $\gamma_{s-2} \in C_{i_{s-1}}(C_{i_s}(\alpha))$

$$\Rightarrow \gamma_{s-2} \in \bigcup_{\gamma_{s-1} \in C_{i_s}} C_{i_{s-1}}(\gamma_{s-1}) \Rightarrow \exists\, r_{s-1} \in \mathbb{Z}^+ ,\ \phi_{i_{s-1}}^{r_{s-1}}(\gamma_{s-1}) = \gamma_{s-2} ,\ H_{i_{s-1}} = \langle \phi_{i_{s-1}} \rangle$$

si $\gamma_{s-1} \in C_{i_s}(\alpha)$

$$\Rightarrow \gamma_{s-1} \in \sigma_{\phi_{i_s}}(\alpha) \Rightarrow \exists\, r_s \in \mathbb{Z}^+ ,\ \phi_{i_s}^{r_s}(\alpha) = \gamma_{s-1} ,\ H_{i_s} = \langle \phi_{i_s} \rangle$$

$$\therefore \quad \phi_i^{r_i} \phi_{i_1}^{r_1} \cdots \phi_{i_s}^{r_s}(\alpha) = \alpha$$

Ahora bien,

sea $A = (a_{ij}) = (\alpha) \quad \forall \quad i, j \; ; \; \alpha \in F$

$$\therefore \qquad \phi_i^{r_i} \phi_{i_1}^{r_1} \cdots \phi_{i_s}^{r_s} (\Omega) = \Omega \; ,$$

como $\quad \phi_i^{r_i} \phi_{i_1}^{r_1} \cdots \phi_{i_s}^{r_s} \in \mathcal{L}$

entonces $\quad \phi_i^{r_i} \phi_{i_1}^{r_1} \cdots \phi_{i_s}^{r_s} \in \mathrm{Aut}(A, \mathcal{L})$

Por hipótesis,

$$\mathrm{Aut}(A,\mathcal{L}) = \mathrm{Aut}(A,H_1) \pi \mathrm{Aut}(A,H_2) \pi \cdots \pi \mathrm{Aut}(A,H_k)$$

Ahora nos fijamos en

$$\phi_i^{r_i} \in H_i = \langle \phi_i \rangle$$

como $\quad \phi_i \in \mathrm{Aut}(A,H_i) \quad \Longrightarrow \quad \phi_i^{r_i} \in \mathrm{Aut}(A,H_i)$

$$\Longrightarrow \quad \phi_i^{r_i}(A) = A \quad \therefore \quad \phi_i^{r_i}(\alpha) = \alpha \; , \quad A = (a_{ij}) = (\alpha) \; \forall i,j \; \blacksquare$$

(ya que $\quad \phi_i^{r_i}(\beta) = \alpha \quad$)

$\Longleftarrow$) Supongamos que

$$C_i(\alpha) \cap C_{i_1}(\cdots(C_{i_s}(\alpha))) = \{\alpha\}$$

Sea $A = (a_{ij})$ arbitraria.

Claramente

$$\mathrm{Aut}(A,H_1) \wr \mathrm{Aut}(A,H_2) \wr \cdots \wr \mathrm{Aut}(A,H_k) \leq \mathrm{Aut}(A,\Omega)$$

Sea $\phi_1 \phi_2 \cdots \phi_k(A) = A$

$\Rightarrow \quad \phi_1 \phi_2 \cdots \phi_k(a_{ij}) = a_{ij} \quad \forall \quad i, j$

Si $\phi_r(a_{ij}) = a_{ij} \ \forall \ i,j \ \forall \ r = 1,\ldots,k$ terminamos.

Supongamos que existe a_{ij} tal que

$\phi_t(a_{ij}) = b \neq a_{ij}$ y $\phi_{t-1}(b) = a_{ij}$ para alguna t, $t-1 \in \{1,\ldots,k\}$

$\therefore \quad \phi_1 \phi_2 \cdots \phi_{t-1} \phi_t \cdots \phi_k(a_{ij}) = a_{ij}$

donde $\phi_p(a_{ij}) = a_{ij} \quad \forall \quad p \neq t, t-1.$

$\Rightarrow \quad \phi_{t-1} \phi_t \phi_1 \cdots \phi_k(a_{ij}) = a_{ij} \quad \forall \quad i, j$

$\Rightarrow \quad b, a_{ij} \in C_{t-1}(a_{ij}) \cap C_t(\cdots(C_k(a_{ij}))) \ \nabla$

□

BIBLIOGRAFIA

GARY, L. Mullen.
Equivalence Classes of Matrices over Finite Fields.
Linear Algebra and its Applications. 27:61-68 (1979).
Elsevier North Holland, Inc.

HERSTEIN, I. N.
Algebra Moderna.
Ed. Trillas, México, 1979.

LEDERMANN, Walter.
Introduction to the theory of finite groups.
New York, Interscience Publishers, Inc., 1957.

WALACE, D.A.R.
Grupos.
Ed. Limusa, México, 1978.

WIELANDT, Helmut.
Finite Permutation Groups.
Academic Press Inc., 1964.