Real Bermúdez Jesús M.

4 de abril de 2003

Ejercicios de las notas de la sección de subgrupos

1. Siguiendo el mismo razonamiento del ejemplo anterior se llegan a las siguientes definiciones de conjunto de matrices:

$$SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) | detA = 1\}$$
$$O(n) = \{A \in GL_n(\mathbb{R}) | A^t A = I\}$$
$$SO(n) = \{A \in O(n) | detA = 1\} = SL_n(\mathbb{R}) \cap O(n)$$

otros que son importantes:

$$SL_n(\mathbb{Q}) = \{A \in GL_n(\mathbb{Q}) | detA = 1\}$$
$$SL_n(\mathbb{Z}) = \{A \in GL_n(\mathbb{Z}) | detA = 1\}$$

como ejercicio determine cual de los anteriores son grupos y establezca los subgrupos.

Solución

Veamos si $SL_n(\mathbb{Z}) < SL_n(\mathbb{Q})$.
Veamos que $AB \in SL_n(\mathbb{Z})$ y que $B^{-1} \in SL_n(\mathbb{Z})$.
$AB \in SL_n(\mathbb{Z})$ pues $|AB| = |A||B| = 1$,
pero en general $B^{-1} \notin \mu_{n\times n}(\mathbb{Z})$, aunque $|B^{-1}| = 1$.
Por lo tanto $SL_n(\mathbb{Z}) \not< SL_n(\mathbb{Q})$

Ahora veamos que $O(n) < SL_n(\mathbb{R})$
$A, B \in O(n) \Rightarrow A^t A = I$ y $B^t B = I$ entonces

$$A = (A^t)^{-1} \tag{1}$$
$$B^t = B^{-1} \tag{2}$$

$(AB)^t AB = B^t A^t AB por 2$
$(AB)^t AB = B^t A^t AB = B^t IB = B^t B = I$
por tanto $AB' in O(n)$.
Ahora veamos que $B^{-1} \in O(n)$ o sea $B^{-1} \in \mu_{n\times n}(\mathbb{R})$ y $|B^{-1}| \neq 0$.
$(B^{-1})^t B^{-1} = (B^{-1})^t = (BB^{-1})^t = I^t = I$
Por tanto $O(n) < SL_n(\mathbb{R})$.

Veamos que $SO(n) < O(n)$
Sea $A, B \in SO(n) \Rightarrow |A| = 1 = |B|$.
Afirmación: $AB \in SO(n)$ pues $AB \in GL_n(\mathbb{R})$ y $|AB| = |A||B| = 1 \Rightarrow (AB)^t(AB) = I$.
Afirmación: $B^{-1} \in SO(n)$ pues $|B^{-1}| = \frac{1}{|B|} = 1$ y $(B^{-1})^t(B^{-1}) = I$.
Por lo tanto $SO(n) < O(n)$.

Similarmente se demuestra que $SL_n(\mathbb{Q}) < SO(n)$.

2. Observación: (Basándonos en la definición 8 de orden de a).Si $a^m = e$, entonces $o(a)|m$. Se deja como ejercicio al lector.

Demostración

Como $o(a) < m \quad o(a), m \in \mathbb{N}$, entonces por el algoritmo de la división $\exists q, r \in \mathbb{Z}$ tal que:

$$m = qo(a) + r \tag{3}$$

con $r = 0$ ó $r < o(a)$
Afirmamos que r=0, pues de lo contrario, r sería menor que el orden de a, y de 2

$$m - q[o(a)] = r$$

Así $a^r = a^m a^{-q[o(a)]} = e(a^{o(a)})^{-q} = \frac{e}{e^q} = e$
Así $a^r = e$ lo cual es una contradicción pues $r < o(a)$ y $o(a)$ es el mínimo con tal propiedad.

q.e.d.

3. Observación No 3: (De la definición 9)$\langle a \rangle = \langle a^{-1} \rangle$, se deja como ejercicio al lector.

Demostración

Sea $g \in \langle a \rangle = \{e, a, a^2, \dots a^n, \dots\}$
Por tanto $g = a^m$ para algún $m \in \mathbb{Z}$ además $a = (a^{-1})^{-1}$ pues $a(a^{-1}) = e \Rightarrow a = (a^{-1})^{-1}$
Por lo tanto $g = a^m = (a^{-1})^{-m} \Rightarrow e \in \langle a^{-1} \rangle$.
Por lo que podemos decir que cada elemento de $\langle a \rangle$ es elemento del $\langle a^{-1} \rangle$.
Por lo tanto $\langle a \rangle = \langle a^{-1} \rangle$.

q.e.d.

4. Escribir a los elementos de S_3 como palabras sobre $H_3 = \{\tau_1, \tau_2, \tau_3\}$.

Solución

Sea $S_3 = \{\sigma_1, \sigma_2, \sigma_3, \tau_1, \tau_2, \tau_3\}$ donde $\sigma_1, \sigma_2, \sigma_3, \tau_1, \tau_2, \tau_3$ están definidos de la misma forma que en los ejercicios preeliminares.

$$\sigma_1 = \tau_1 \circ \tau_2 \circ \tau_3$$

$$\sigma_2 = \tau_1 \circ \tau_2$$

$$\sigma_3 = \tau_3 \circ \tau_3$$

$$\tau_1 = \tau_1^1$$

$$\tau_2 = \tau_2^1$$

$$\tau_3 = \tau_3^1$$

1.7 Ejercicios

1. Sea G grupo, $a \in G$ elemento de orden finito. Demuestre que para todo $g \in G$ el elemento $g \cdot a \cdot g^{-1}$ tiene el mismo orden que a.

   Demostración

   Sea $g \in G$ y $n = o(a)$
   $(g \cdot a \cdot g^{-1})^n = g \cdot a \cdot (g^{-1} \cdot g) \cdot a \cdot g^{-1} \cdot \dots \cdot g \cdot a \cdot g^{-1} = g \cdot a^n \cdot g^{-1} = g \cdot g^{-1} = e$
   Por lo tanto $(g \cdot a \cdot g^{-1})^n = e$

Sea $m \in \mathbb{N}$ tal que $(g \cdot a \cdot g^{-1})^m = e$, probemos que $n|m$

$g \cdot a^{m} \cdot^{-1} = g \cdot a^n \cdot g^{-1} = e$

$g \cdot a^m \cdot g^{-1} = e$

$a^m = g^{-1} \cdot g = e$

Por lo tanto $n|m$ pues $n = o(a)$.

Por lo tanto para todo $g \in G$ el elemento $g \cdot a \cdot g^{-1}$ tiene el mismo orden que a si el orden de a es finito con G grupo.

q.e.d.

2. Sea G grupo.

   a) Demuestre que si $a, b \in G$ tales que $a \cdot b = b \cdot a$, con a,b de ordenes finitos, entonces $a \cdot b$ es también de orden finito.

   b) De un ejemplo que muestre que en *a*) no se puede suprimir la hipótesis $a \cdot b = b \cdot a$.

   Demostración

   a) Como a y b son de ordenes finitos entonces $a^{o(a)} = e$ y $b^{o(b)} = e$. Sea $k = máx\{o(a), o(b)\}$, entonces $a^k = e$ y $b^k = e$ y como $ab = ba \Rightarrow a^k \cdot b^k = e$ y $b^k \cdot a^k = e$, entonces $\Rightarrow (a \cdot b)^k = e$.
   Por lo tanto $a \circ b$ es también de orden finito si a y b lo son, y además, si $a \cdot b = b \cdot a$.

   b) Sea $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ y sea $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$
   y vemos que $A \times B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ y $B \times A = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$
   Veamos que: $o(A \times B) = \infty$.
   Vemos que $(A \times B)^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$
   Afirmamos que $(A \times B)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$
   Procedamos por inducción:
   Para $n = 1$ y $n = 2$ se cumple.
   Supongamos que se cumple para n=k y demostremos para $n = k + 1$.

$$\begin{aligned} (A \times B)^{k+1} &= (A \times B)^k (A \times B) \\ &= \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & k+1 \\ 0 & 1 \end{pmatrix} \forall k \in \mathbb{N} \end{aligned}$$

Por lo tanto $A \times B$ tiene orden infinito y con esto vemos que no se puede suprimir la hipótesis de que $a \cdot b = b \cdot a$.

q.e.d.

3. Sea G grupo infinito, tal que $\langle a \rangle = G$ generador. Demuestre que $b \in G$ genera a G si y sólo si $b = a$ ó $b = a^{-1}$.

   Demostración

   Sea $G = \langle a \rangle = \{e, a, a^2, a^3, \ldots\}$
   Queremos ver que $b \in G$ y $G = \langle b \rangle \Leftrightarrow b = a$ ó $b = a^{-1}$
   $\Leftarrow$) Si $b = a$ terminamos.
   Supongamos que $b = a^{-1}$, como $b \in G$, entonces $b = a^n$ así $a^{-1} = a^n$, luego $a^{-n} = a$, así $a^{-n} = a = b^n \Rightarrow a^n = b^{-n}$.
   Por lo tanto $\langle b \rangle = G$.

$\Rightarrow$) Queremos ver que si $G = \langle b \rangle$ entonces $b = a$ ó $a = b^{-1}$.
Si $b = a^n$ y $a = b^m$.
Si $b = a$ se tiene de inmediato.
Supongamos que $b \neq a$, entonces:

$$b^{m-1} \cdot b = a$$
$$b^{m-1} \cdot a^n = a$$
$$b^{m-1} = a^{1-n}$$
$$a^{nm-n} = a^{1-n} \Rightarrow nm - n = 1 - n$$
$$\Rightarrow nm = 1$$

Con $n, m \in \mathbb{Z} \Rightarrow n, m = 1$ ó $n, m = -1$
Entonces $b = a$ ó $b = a^{-1}$.

q.e.d.

4. Sea G grupo Abeliano, $g_1, g_2 \in G$ elementos de orden finito con $(|g_1|, |g_2|) = 1$. Demuestre que $|g_1 g_2| = |g_1||g_2|$.

Demostración

Sean $n = |g_1|$ y $m = |g_2|$, tal que $(m, n) = 1$ y además $(g_1)^n = e$ y $(g_2)^m = e$.
Sea $s = mn \Rightarrow$

$$\begin{aligned}(g_1 g_2)^s = (g_1 g_2)^{mn} &= g_1^{mn} g_2^{mn} \\ &= (g_1^n)^m (g_2^m)^n \\ &= e.\end{aligned}$$

Por lo tanto $|g_1 g_2| = s = mn = |g_1||g_2|$
Falta probar que s es el mínimo entero con tal propiedad, es decir, $(g_1 g_2)^{mn} = e$.
Sea $k \in \mathbb{N}$ tal que $(g_1 g_2)^k = e$. Por el algoritmo de la división existe $p, q \in \mathbb{Z}$ tal que

$$k = sp + q$$

con $0 \leq q < s$.
Por lo tanto $(g_1 g_2)^k = (g_1 g_2)^{sp+q} = [(g_1 g_2)^s]^p (g_1 g_2)^q = (g_1 g_2)^q$, por la minimalidad de k $\Rightarrow q = 0$.
Por tanto $s | k$.
Por lo tanto $|g_1 g_2| = s = mn$.

q.e.d.

5. Sea G un grupo cíclico finito con n elementos. Si $G = \langle a \rangle$.

   a) Demuestre que a^i con $1 \leq i \leq n$ genera si y sólo si $(i, n) = 1$.
   b) Demuestre que para cada divisor d de n, G contiene un único subgrupo de orden d.

   Demostración

   a) $\Rightarrow$) Supongamos que a^i genera, entonces $a = (a^i)^s$ y como $G = \langle a \rangle$ entonces $a = a^{n+1}$, así $a^{is} = a^{n+1} \Rightarrow$ $is \equiv 1$ mod n pues todo grupo cíclico finito es isomorfo a $\mathbb{Z}/n\mathbb{Z}$, $\Rightarrow is - 1 = nt \Rightarrow 1 = is - nt \Rightarrow (i, n) = 1$.

   $\Leftarrow$) Recíprocamente, supongamos que $(i, n) = 1$ y mostremos que a^i también es un generador de G.
   Sea $g \in G$, entonces $g = a^m$ pues $G = \langle a \rangle$, para algún $m \in \mathbb{Z}$ con $m < n$.
   Notemos que $a = a^1 = a^{ri+nt} = a^{ri} a^{nt} = a^{ri} e = a^{rk}$ (Lo anterior es dado que $(i, n) = 1$).
   Por lo tanto $g = (a^{ir})^m = (a^i)^{rm}$

Por lo tanto a^i también genera si $(i,n)=1$.

Por lo tanto Si $G=\langle a\rangle$ es un grupo cíclico de orden n, entonces el elemento a^i es generador si y sólo si $(i,n)=1$.

b) Sea $n=|G|$ y sea d un divisor de n. Sea $a\in G$ tal que $G=\langle a\rangle$.
El elemento $a^{\frac{n}{d}}$ tiene orden d, pues $(g^{\frac{n}{d}})^d=e$y si $|a^{\frac{n}{d}}|^{'}=d^{'}$, entonces $d^{'}|d\Rightarrow d=d^{'}l$ con $l\in\mathbb{N}$, luego $(a^{\frac{n}{d}})^{d'}=a^{\frac{n}{l}}\Rightarrow l=1$.
Por lo tanto d es el orden de $a^{\frac{n}{d}}$. Sea $H=\langle a^{\frac{n}{d}}\rangle$, entonces $|H|=d$.
Sea ahora $H_1<G$ talque $|H_1|=d$. Sabemos que H_1 es cíclico, sea $c\in H_1$ tal que $H_1=\langle c\rangle$. Por tanto $H_1\subseteq G=\langle a\rangle$.
Existe $n\in\mathbb{N}$ tal que $c=a^m$.
Entonces $e=c^d=a^{md}\Rightarrow n|md$, luego $md=nt$ para algún $t\in\mathbb{Z}$.

$$\Rightarrow m=\frac{n}{d}l\Rightarrow c=a^m=(a^{\frac{n}{d}})^t\in\langle a^{\frac{n}{d}}\rangle=H$$

Por lo tanto $H_1=\langle c\rangle\subseteq$ pero $|H|=|H_1|=d$
Por lo tanto $H=H_1$
Por lo tanto Si G es grupo cíclico finito con n elementos y si $G=\langle a\rangle$ entonces para cada divisor d de n, G contiene un único subgrupo de orden d.

q.e.d.

6. Demuestre que si un grupo G contiene como sus únicos subgrupos a G y $\{e\}$, entonces G debe ser un grupo cíclico finito con número primo de elementos.

Demostración

Procedamos por contradicción, es decir supongamos que G no es un grupo cíclico. Negando el ejercicio 5(*b*) tenemos que existe $d||G|$ tal que existe $H_1,H<G$ tal que $|H_1|=|H|=d$ y $H\neq H_1$.

Como G tiene a los únicos subgrupos $\{e\}$ y G entonces:

H_1 es igual a $\{e\}$ ó es igual a G.

H es igual a $\{e\}$ ó es igual a G.

Si $H_1=\{e\}=H\Rightarrow H_1=H$, lo cual es una contradicción.

Si $H_1=G=H\Rightarrow H_1=H$, lo cual es una contradicción.

Así G es cíclico finito.

Supongamos que $|G|=m$ con m no primo, así $\forall d|m$ tal que $d\neq 1$ y $d<m$ entonces existe un único $H<G$ tal que $|H|=d$. Pero G sólo tiene 2 subgrupos.

$H=\{e\}$ si $H=\{e\}\Rightarrow|H|=1=d$, lo cual es una contradicción.

$H=G$ si $H=G\Rightarrow d=m$, lo cual es una contradicción.

Por lo tanto m es primo.

q.e.d.

7. Sea G grupo Abeliano g_1,g_2 elementos de G con $o(g_1),o(g_2)$; finitos. Demuestre que existe $h\in G$ cuyo orden es igual al mínimo común múltiplo de $o(g_1)$ y $o(g_2)$.

Demostración

Sea $l=o(g_1)o(g_2)\Rightarrow(g_1g_2)^l=e$. Sean $m=o(g_1)$ y $n=o(g_2)$.

Afirmamos que $m|l$ pues $(g_1)^m=e$ y $(g_1)^l=e$ pues si $(g_1)^l\neq e\Rightarrow(g_1)^{ml}\neq e$ pero $(g_1)^m=e$, lo cual es una contradicción.

Así $m|l$ y $n|l\Rightarrow$ existe $q_1,q_2\in\mathbb{Z}$ talque $l=mq_1$ y $l=nq_2$.

Sea $h=(g_1)^{\frac{mq_1}{n}}$ entonces $|h|=l$ pues $h^l=(g_1^{\frac{mq_1}{n}})^l=(g_1)^{\frac{mq_1nq_2}{n}}=(g_1^m)^{q_1q_2}=e$

Así $h^l = e$.

Si existe $k \in \mathbb{Z}$ tal que $m|k$ y $n|k \Rightarrow g_1^k = e$ y $g_2^k = e$

$(g_1^{\frac{mq}{n}})^k = ((g_1)^k)^{\frac{mq}{n}} = e^{\frac{mq}{n}} = e$.

Por lo tanto $l|k$.

Así $l = mcm(m, n)$ y existe $h = g_1^{\frac{mq}{n}}$ tal que $|h| = l$.

q.e.d.

8. Sea G grupo Abeliano con $m \cdot n$ elementos, m y n primos relativos, suponga que a y b son elementos de G de ordenes m y n respectivamente. Demuestre que G es grupo cíclico.

Demostración

Sea $g \in G$ como $|G| = m \cdot n$ entonces:

$$g^{m \cdot n} = e$$

.

Sea $|a| = m$ y $|b| = n$ mostremos que G es cíclico.

Como $(m, n) = 1 \Rightarrow$ existen $s, t \in \mathbb{Z}$ talque $1 = m \cdot s + n \cdot t$ entonces:

$$g = g^{m \cdot s} g^{n \cdot t}$$

Sea $a = g^{n \cdot t}$ y $b = g^{m \cdot s}$ así $g^{m \cdot n} = (g^{n \cdot t} g^{n \cdot s})^{m \cdot n} = g^{m \cdot n \cdot t \cdot n} g^{n \cdot s \cdot m \cdot n}$

$g^{m \cdot n} = e$.

Así $G = \langle a \cdot b \rangle = \langle g^{n \cdot t} g^{m \cdot s} \rangle$

Por lo tanto G es grupo cíclico.

q.e.d.

9. Sea G grupo Abeliano finito, suponga que para todo número natural n hay a lo más n elementos en G que satisfacen la ecuación $x^n = e$. Demuestre que G debe ser grupo cíclico.

Demostración

Procedamos por contradicción, es decir, supongamos que G no es cíclico, entonces por la negación del ejercicio $5(b)$ existe $n|k = |G|$ tal que existen al menos dos subgrupos de G H, H_1 tal que $|H| = m \quad |H_1| = m$.

Luego para toda $h \in H$ entonces $h^n = e$, es decir, h satisface la ecuación $x^n = e$.

También para todo $h_1 \in H_1$ $h_1^n = e$, es decir h_1 satisface la ecuación $x^n = e$.

Por lo tanto en tendríamos n elementos que satisfacen la ecuación $x^n = e$ y en H_1 tendríamos el mismo número de elementos que satisfacen esta ecuación.

Así tendríamos por lo menos n+1 elementos en G que satisfacen la ecuación $x^n = e$, lo cual es una contradicción.

Por tanto G debe ser grupo cíclico.

q.e.d.

10. Sea G grupo Abeliano finito, T el conjunto de elementos de G de orden finito. Demuestre que T es subgrupo de G.

Demostración

Dado que T es el conujunto de elementos de G de orden finito, es claro que $T \neq$, $T \subset G$ y además T es finito (Ya que T es el conjunto de todos los elementos de G de orden finito, por la observación 6). Por la proposición 4 que dice que si un grupo G, $\neq H \subset G$ y T como conjunto finito, entonces para cualesquiera $h_1, h_2 \in T$ se tiene que $t_1 t_2 \in T$ entonces $T < G$.

Por lo tanto basta demostrar que $\forall t_1, t_2 \in T \Rightarrow t_1 T_2 \in T$.

Sea $t_1, t_2 \in T \Rightarrow t_1^{o(t_1)} t_2^{o(t_2)} = ee = e \in T$

Por lo tanto $T < G$.

q.e.d.

11. Pendiente 11

12. Sea $(GLM_2(\mathbb{C}), \cdot)$ el grupo de matrices no singulares 2×2 con entradas en $\mathbb{C}$ es decir

$$GLM_2(\mathbb{C}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{C}, a \cdot d - b \cdot c \neq 0 \right\}$$

y

$$s = \left\{ A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & i \\ i0 & \end{pmatrix} \right\} i^2 - 1$$

Demuestre que $\langle S \rangle$ es un subgrupo de ocho elementos.

Demostración

Dada la contrucción del árbol se obtuvo que

$$\begin{aligned} \langle S \rangle &= \{A^0 B^0, A, A^2, A^3, B, AB, A^2 B, A^3 B\} \\ &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \right\} \end{aligned} \tag{4}$$

Y vemos que

$$A^2 = B^2$$

$$AB = BA^{-1}$$

$$AA^{-1} = BB^{-1} = I$$

$$A^3 = A^{-1} = AB^2 A (A^{-1})^2 = BA^{-1} B = BB^{-1} A^{-1}$$

$$BA = BA$$

$$A^2 B = ABA^{-1} = BA^{-1} = BA^2 = BA^{-1} A^{-1} = A^3 B$$

$$A = BA^2 = A^2 A^{-1} = ABB^{-1} = AA^{-1} A = BA^{-1} B^{-1} = BB^{-1} A$$

Ahora veamos que $\langle S \rangle < GLM_2(\mathbb{C})$

Por la proposición 4 , que dice que si G es un grupo y $\neq H \subset G$ y H como conjunto es finito si $\forall h_1, h_2 \in H$ en se tiene que $h_1 h_2 \in H$ entonces : $H < G$.

Veamos que $\langle S \rangle < GLM_2(\mathbb{C})$.

Sea $A' \in \langle S \rangle$ veamos por casos :

Si:

a) $A' = I \Rightarrow detI \neq 0$

b) $A' = A \Rightarrow detA = 1 \neq 0$

c) $A' = A^2 \Rightarrow detA^2 = 1 \neq 0$

d) $A' = A^3 \Rightarrow detA^3 = A^{-1} = 1 \neq 0$

e) $A' = B \Rightarrow det B = 1 \neq 0$

f) $A' = AB \Rightarrow det AB = 1 \neq 0$

g) $A' = A^2B \Rightarrow det A^2 B = 1 \neq 0$

h) $A' = A^3B \Rightarrow det A^3 B = 1 \neq 0$

Por lo tanto $A' \in GLM_2(\mathbb{C}) \Rightarrow \langle s \rangle \subset GLM_2(\mathbb{C})$ y $\langle s \rangle$ es conjunto finito ya que consta de ocho elementos.

Por lo tanto $\langle s \rangle < GLM_2(\mathbb{C})$ ya que dados cualquier $A', B' \in \langle S \rangle \Rightarrow A'B' \in \langle S \rangle$.

q.e.d.

13. Sea $(GLM_2(\mathbb{R}), \cdot)$ el grupo de matrices no singulares 2×2 con entradas en $\mathbb{R}$.

a) Sea

$$S = \left\{ C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}. \tag{5}$$

Demuestre que $\langle S \rangle$ es un grupo no Abeliano de orden 8, lo denotaremos por D_4.

b) Calcule tres subgrupos no triviales de D_4

Demostración

(a) Dada la contrucción del árbol se obtuvo que

$$\begin{aligned} \langle S \rangle &= \{C^0D^0, C, C^2, C^3, D, CD, C^2D, C^3D\} \\ &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \end{aligned} \tag{6}$$

Y vemos que

$$C^4 = B^2 = e$$

$$AB = BA^{-1} = BA^3$$

$$A^{-1} = A^3$$

a) Es Asociativa: es inmediata, ya que la operación con matrices es asociativa.

b) D_4 tiene identidad, a saber , $I = A^0B^0$

c) Todo elemento de D_4 tiene inverso: pues si $A^iB^j \in D_4$ entonces:

$$(A^iB^j)^{-1} = \begin{cases} a^{-i} = a^{4-i} & si \quad j=0 \quad e \quad i=1,2,3,4 \\ a^ib \quad si \quad j=1 & e \quad i=1,2,3,4 \end{cases}$$

Además es no Abeliano pues por ejemplo: $AB \neq BA$ pues

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \neq \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Por lo tanto D_4 es un grupo no Abeliano de orden 8.

q.e.d.

(b)Pendiente

14. Sea G grupo tal que $a^2 = e \; \forall a \in G$. Demuestre que G es Abeliano.

Demostración

Sean $a, b \in G$, entonces $a^2 = a \cdot a = e$ y $b^2 = b \cdot b = e \Rightarrow a = a^{-1}$ y $b = b^{-1}$
Por lo tanto $a \cdot b = a^{-1} \cdot b^{-1} = (b \cdot a)^{-1} \Rightarrow$
$a \cdot b = (b \cdot a)^{-1} = b \cdot a$.
Por tanto $a \cdot b = b \cdot a$.
Por lo tanto G es Abeliano.

q.e.d.