

Control 1

Blanca Cano Camarero

11 de mayo de 2020

Índice

1. Ejercicio 1	1
1.1. Apartado primero	1
1.2. Apartado segundo	2
1.3. Apartado tercero	2
1.4. Apartado tercero	4
2. Ejercicio 2	5
2.1. Apartado primero	5
2.2. Apartado segundo	7
2.3. Tercer apartado	8
2.4. Cuarto apartado	10
3. Ejercicio 3	12
3.1. Apartadoo primero	12
3.2. Segundo apartado	16
3.3. Apartado tercero	17
4. Ejercicio 4	20
4.1. Apartado primero	20
4.2. Apartado segundo	21

1. Ejercicio 1

En el grupo simétrico S_8 se consideran los elementos

$$\pi = (145)(283)(67) \text{ y } \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 1 & 7 & 8 & 4 & 6 & 2 \end{pmatrix}$$

1.1. Apartado primero

Descomponed β como producto de ciclos disjuntos y como producto de transposiciones. ¿Cuál es el orden de β ? ¿Cuál es la signatura?

Descomposición como ciclos disjuntos

Toda permutación se puede expresar de forma única (salvo el orden) de ciclos disjuntos, es este caso:

$$\beta = (13)(258)(476)$$

Descomposición en productos de transposiciones

Todo ciclo se puede expresar como producto de transposiciones, que no necesariamente tiene porqué ser único (aunque sí siempre de la misma paridad). Para este caso tenemos que:

$$\beta = (13)(58)(28)(67)(46) \quad \beta = (34)(14)(58)(28)(67)(36)(34)$$

Orden de β

El orden de una permutación es el mínimo común múltiplo de las longitudes de los ciclos disjuntos que lo componen, en este caso sería $mcm(2, 3, 3) = 6$.

El orden de β es 6.

Signatura de β

La signatura, signo o paridad de una permutación s es $\sigma(s) = (-1)^n$ donde n es el número de transposiciones con el que se puede expresar.

Por el teorema anterior sabemos que éste es indiferente de la expresión que tomemos, ya que la paridad del número de transposiciones se mantiene.

En este caso $n = 5$ y por tanto $\sigma(\beta) = (-1)$.

1.2. Apartado segundo

Hallad un elemento $\alpha \in S_8$ tal que $\beta = \alpha\pi\alpha^{-1}$.

Para esto utilizaremos la siguiente proposición que caracteriza a los conjugados: $\beta(x_0 \dots x_r)\beta^{-1} = (\beta(x_0) \dots \beta(x_r))$

Por tanto nuestro α buscado cumple la siguiente propiedad:

Para todo $x \in \{1, 8\}$ se tiene que $\alpha\pi(x) = \beta(x)$; de lo que deducimos que si $\pi(x) = y$ entonces $\alpha(y) = \beta(x)$.

Veamos nuestro caso concreto:

- $\beta(1) = 3$ y $\pi(1) = 4$ entones $\alpha(4) = 3$
- $\beta(2) = 5$ y $\pi(2) = 8$ entones $\alpha(8) = 5$
- $\beta(3) = 1$ y $\pi(3) = 2$ entones $\alpha(2) = 1$
- $\beta(4) = 7$ y $\pi(4) = 5$ entones $\alpha(5) = 7$
- $\beta(5) = 8$ y $\pi(5) = 1$ entones $\alpha(1) = 8$
- $\beta(6) = 4$ y $\pi(6) = 7$ entones $\alpha(7) = 4$
- $\beta(7) = 6$ y $\pi(7) = 6$ entones $\alpha(6) = 6$
- $\beta(8) = 2$ y $\pi(8) = 3$ entones $\alpha(3) = 2$

Esto es $\alpha = (1857432)$

1.3. Apartado tercero

Si calculamos el producto $\alpha\pi\alpha^{-1}$ para todas las permutaciones de $\alpha \in S_8$. ¿Cómo podemos caracterizar a las permutaciones obtenidas? ¿Cuántos resultados diferentes obtenemos?.

Caracterización

En virtud de la proposición mencionada en el apartado anterior. Tenemos lo siguiente:

Sea s, r permutaciones cualquiera, y $s = s_0 s_1 \dots s_m$ es una descomposición en ciclos disjuntos de s , entonces tenemos que

$$rsr^{-1} = rs_0 s_1 \dots s_m r^{-1} = (rs_0 r^{-1})(rs_1 r^{-1}) \dots (rs_m r^{-1}).$$

Por consiguiente, para nuestro caso cada permutación obtenida tendrá tres ciclos disjuntos, dos de ellos de longitud 3 y uno de longitud 2.

~~BORRAR ESTO~~ Ahora ya podemos aplicar la caracterización del conjugado para cada $rs_i r^{-1}$ con $i \in \{0..m\}$. y es más si $s_i = (x_0^i \dots x_{w_i}^i)$ entonces sabemos que $(r(x_0^i) \dots r(x_{w_i}^i))$ deben de formar un ciclo disjunto, del resto, ya que de otra forma la aplicación no estaría bien definida.

Cardinalidad.

REDACTAR MEJOR, NO SE ENTIENDE BIEN

Número de permutaciones posibles, las podemos ver gracias a la división en ciclos disjuntos anterior y la biyectividad de las permutaciones: será de la forma $(x_0 x_1)(x_2 x_3 x_4)(x_5 x_6 x_7)$ con $x_i \neq x_j$ si $i \neq j$

Para el ciclo $(x_0 x_1)$ de dos elementos tenemos $\frac{8!}{(8-2)!}$, lo cual nos deja todavía $8 - 2$ elementos por combinar, para los dos ciclos de tres disjuntos será $\frac{6!}{3!} \frac{3!}{0!}$, pero le tenemos que quitar la mitad de estos casos ya que la composición de ciclos disjuntos es conmutativa y tendríamos la misma permutación para

Por tanto el número total de casos son: $\frac{8!}{6!} \frac{1}{2} \left(\frac{6!}{3!} \frac{3!}{0!} \right) = \frac{8!}{2}$. Ahora bien, estas son todas las posibles, pero ¿podemos obtenerlas todas? La respuesta a esta pregunta es afirmativa, y la demostración es constructiva, siguiendo la misma idea del apartado segundo.

Veámoslo:

Sea $\beta = (x_0 x_1)(x_2 x_3 x_4)(x_5 x_6 x_7)$ con $x_i \neq x_j$ si $i \neq j$ y queremos ver que existe α una permutación que cumple que $\beta = \alpha \pi \alpha^{-1}$, puesta está definida de manera única para cada elemento.

1.4. Apartado tercero

¿Es el grupo generado por β un subgrupo normal de S_8 ?

EMPEZAR POR EL CASO GENERAL DEL SEGUNDO PÁRRAFO

Por la caracterización de normalidad esto se dará si para cualquier $s \in S_8$ $s \langle \beta \rangle s^{-1} = \langle \beta \rangle$. esto es, que para cualesquiera $b \in \langle \beta \rangle$, $s \in S_8$ va a existir un $c_{b,s} \in \langle \beta \rangle$ que cumple que $sbs^{-1} = c_{b,s}$.

Ahora bien $\langle \beta \rangle = \{id, \beta = (13)(258)(476), \beta^2 = (285)(462), \beta^3 = (13), \beta^4 = (258)(476), \beta^5 = (13)(285)(462)\}$ y seleccionamos una permutación que no esté en $\langle \beta \rangle$ y que tenga el mismo número de ciclos disjuntos y de la misma logitud (la caracterización del apartado dos) por ejemplo $\gamma = (12)(358)(476)$ y por lo visto en el apartado anterior, sabemos que existirá algún $\alpha \in S_8$ que cumpla que $\gamma = \alpha\beta\alpha^{-1}$.

Y por consiguiente habremos probado que es no es normal.

De hecho acabamos de ver más, una caracterización para que sea normal: que no se pueda descomponer en ciclos disjuntos, es decir **que la permutación sea un ciclo**, ya que supongamos que existe β una permutación que se puede descomponer en ciclos disjuntos, $\beta = b_0b_1...b_n$, tendríamos por conmutatividad que $\beta^n = b_0^n b_1^n ... b_n^n$. Ahora cogemos una permutación γ que sea idéntica a β salvo que los dos primeros elementos de los ciclos disjuntos sea han intercambiado entre sí (esto es si $\beta = (x_0, x_1...)(y_0y_1...)(z_0, z_1...)$ entonces $\gamma = (y_0, x_1...)(x_0y_1...)(z_0, z_1...)$). y por lo visto en el apartado anterior, sabemos que existirá algún $\alpha \in S_8$ que cumpla que $\gamma = \alpha\beta\alpha^{-1}$.

Pero por otra parte hemos visto cómo son los elemento de $\langle \beta \rangle$, así que γ no pertenecerá.

2. Ejercicio 2

2.1. Apartado primero

Describid los subgrupos de orden 2 y de orden 4 del grupo diédrico D_8 . ¿Contiene D_8 algún subgrupo isomorfo a Q_2 , el subgrupo de los cuaternios?

Sabemos que $D_n = \langle r, s | r^n = 1 = s^2 \wedge sr = r^{n-1}s \rangle$. La cardinalidad de D_n es $2n$ y el teorema de Lagrange nos asegura que la cardinalidad de sus subgrupos será un divisor de $2n$. Por tanto para este caso tiene sentido plantearse cuáles son los subgrupos de orden 2 y 4 de D_8 .

Orden 2

Los subgrupos de este orden deberán de ser cíclicos, es decir, generados por algún elemento, ya que de otra forma el subgrupo S contendría dos elementos $x \neq y \neq 1$ para los que se cumpliría que no existe $n \in \mathbb{Z}$ tal que $x^n = y$, además como S es subgrupo $1 \in S$; por tanto necesariamente la cardinalidad de S sería mayor de dos, ya que $x, y, 1 \in S$.

Veamos ahora qué condiciones deben de cumplir los elementos que generen los grupos cíclicos de orden 2:

Por cómo se ha definido D_n , todos sus elementos son de la forma $r^i s^j$ con $i, j \in \mathbb{Z}$. y si $\langle a \rangle$ es de orden 2, entonces necesariamente $a^2 = 1$.

Por tanto los generadores deben cumplir que $1 = (r^i s^j)(r^i s^j)$ que por estar en D_n se tienen dos posibilidades $i \equiv 1$ o $i \equiv 0$; para el primer caso: $r^i (sr^i)s = r^i r^{i(n-1)} s^2 = r^{i-i} r^{in} s^2$

Donde para la primera igualdad se ha utilizado i veces la caracterización de $sr = r^{n-1}s$ de D_n .

Pero claro, también sabemos que $r^n = 1 = s^2$ y que $r^0 = 1$ por tanto si $i \equiv 1$, sea cual sea el valor de j ; $r^{i-i} r^{in} s^{2j} = 1$ y todo $\langle r^i s \rangle$ va a ser de orden 2.

Para el segundo caso ($j \equiv 0$) tenemos que se debe cumplir que $r^i r^i = 1$ y por otro lado sabemos que $r^n = 1$ entonces para que esto suceda no queda más remedio que $2i \equiv n$.

Conclusión: Los subgrupo de orden 2 de D_8 son de la forma $\langle r^i s \rangle$ o equivalentemente $\langle sr^i \rangle$ con $i \in \{0, 7\}$ o son el subgrupo $\langle r^4 \rangle$.

Subgrupos de orden 4

Por el apartado anterior los subgrupos candidatos serán o grupos cíclico $\langle r^i \rangle$ con i no congruente a 4 o grupos generados por r^i, s, sr^j con $i \in \{1..n-1\}$.

Veamos el primer caso:

Buscamos que el orden de $\langle r^i \rangle$ sea 4, entonces necesariamente $(r^i)^4 = 1$ y eso equivale a que $4i \equiv 1$.

Segundo caso $\langle r^i, s \rangle$. Como $n > 2$ en D_n entonces $r^i s \neq r^{i(n-1)} s$ y además ambos distintos del 1. Está claro pues que $1, r^i, s, r^i s$, pertenecen a $S = \langle r^i, s \rangle$. Y a demás por estar en D_8 necesariamente $i = 4$ ya que debe de cumplirse que $sr^i = r^{i(n-1)} s$ y que sea cerrado. También lo podríamos haber visto por cardinalidad, de sus subgrupos: S contendrá a $\langle r^i \rangle$ y a $\langle s \rangle$ y como hemos visto antes, $\langle r^4 \rangle$ era el único subgrupo de orden 2 de la forma $\langle r^i \rangle$, ya que los otros $i, \langle r^i \rangle$ tendrán necesariamente cardinalidad mayor o igualdad a 4 por tanto el único posible S será generado por $r^4 s$.

Veamos que es cerrado para terminar

	1	r^4	s	$r^4 s$
1	1	r^4	s	$r^4 s$
r^4	r^4	1	$r^4 s$	s
s	s	$r^4 s$	1	r^4
$r^4 s$	$r^4 s$	s	r^4	1

Conclusión: El de orden 4 es $\langle r^2 \rangle, \langle r^4, r^j s \rangle$ con $j \in \{0, 3\}$ (No hasta el siente porque si no se repetirían).

¿Contiene D_8 algún subgrupo isomorfo a Q_2 ?

No porque los órdenes de los elementos no es el mismo, en Q_2 el único elemento de orden 2 será -1 , mientras que en S $|Q_2| = 8$ por tanto nuestro subgrupo deberá de ser de orden 8, el teorema de lagrange nos dice que esto es posible.

Veamos si existe: Buscamos un subgrupo de orden 8, que por las consideraciones de los apartados anteriores será de la forma $S = \langle r^i, s \rangle$.

Supongamos que existe f un isomorfismo de grupos entre S y Q_2 existirán $a \in \{1, 7\}$ y $q \in i, k, q \in Q_2$ que cumpla que $f(r^a s) = b$ con como mucho existirá un b que cumpla que $f((r^b)^2) = -1$ porque sumpondría que $(r^b)^4 = 1$ y solo $b = 4$ cumpla eso) y $s^2 = 1$ así que $f(s)$ no podrá ser ni i, k, j .

Ahora bien si $f(r^a s) = b$ entonces se tendría que $-1 = b^2 = f(r^a s)f(r^a s)$ que por ser un isomorfismo sería equivaldría a $f((r^a s)^2) = f((r^a r^{a(n-1)}) = f(1)$ lo cual es una contradicción, ya que en un isomorfismo $f(1) = 1$.

Por tanto no puede existir.

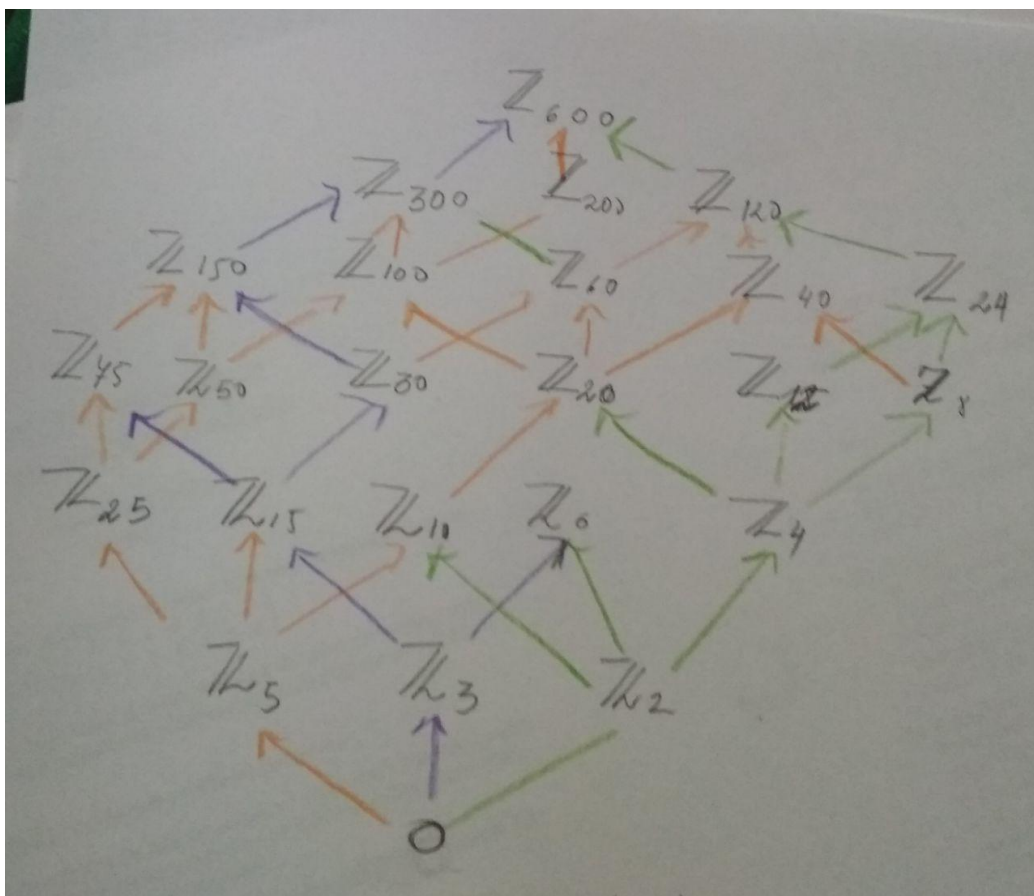
2.2. Apartado segundo

Describid el retículo de subgrupos del grupo \mathbb{Z}_{600}

Sabemos que si $\langle a \rangle$ es un grupo cíclico de orden n , todos sus subgrupos serán ciclos de orden divisor de n , y además $p, d \in \mathbb{N}$ con $pq = n$ entonces $\langle a^p \rangle$ será subgrupo de $\langle a \rangle$ y su orden será $\frac{n}{\gcd(n, p)} = q$.

Pues bien volvamos a nuestro caso particular, \mathbb{Z}_{600} con la operación suma seguirá esta misma estructura $\mathbb{Z}_{600} = \langle 1 | 1^{600} = 1 \rangle$. Por tanto si sus subgrupos serán los $\mathbb{Z}_p = \langle 1 | 1^p = 0 \rangle$ con p divisor de 600, que a su vez tendrán como subgrupos los \mathbb{Z}_t con t divisores

En pos de preservar mi salud mental y a riesgo de encutrecer el pdf, he decido hacerle el grafo del retículo manuscrito, espero que me sepa perdonar.



2.3. Tercer apartado

Consideramos las permutaciones de S_9 , $\sigma = (26)(132859)(263)$ y $\tau = (6734)(46)(37)$. Demostrad que el subgrupo generado por ellas $\langle \sigma, \tau \rangle$, es cíclico. Determine su orden y uno de sus generadores.

Lo primero que vamos a hacer es expresar σ y τ como ciclos disjuntos:

- $\sigma = (13859)$, que es un ciclo de longitud (y por tanto orden) 5.
- $\tau = (47)$, que es un ciclo de longitud (y por tanto orden) 2.

Observar los órdenes de una permutación es muy interesante porque si β es una permutación de longitud n entonces $\beta^n = 1$.

Además, supongamos ahora α es una permutación o composición de permutaciones que se puede descomponer como $\alpha = a_0 a_1 \dots a_r$ con a_i ciclos disjuntos de longitud l_i , entonces se tiene que el $mcm(l_1, l_2, \dots, l_r)$ será el orden de la permutación, ya que si $m = mcm(l_1, l_2, \dots, l_r)$ y además por ser a_0, a_1, \dots, a_r disjuntos serán conmutativos se tendrá que

$$\alpha^m = (a_0 a_1 \dots a_r)^m = a_0^m a_1^m \dots a_r^m = 1$$

Ya que m es múltiplo de todos las longitudes y además será el orden por ser el mínimo número en cumplir eso.

Y si además l_0, l_1, \dots, l_r son primos relativos, se tiene la siguiente igualdad: $m_0 = mcm(l_1, \dots, l_r)$ (nótese que hemos quitado el primero, ni que tampoco hemos perdido generalidad, ya que son conmutativos podemos reordenar.)

Por tanto

$$\alpha^{m_0} = (a_0 a_1 \dots a_r)^{m_0} = a_0^{m_0} a_1^{m_0} \dots a_r^{m_0} = a_0^{m_0} \quad (1)$$

Puesto que m_0 será múltiplo de todos los l_i salvo de l_0 .

Y esto va a describir a las permutaciones que generen $\langle \alpha \rangle$, ya que serán todas aquellas de la forma $s = a_0^{-L_0} a_1^{-L_1} \dots a_r^{-L_r}$ con L_i múltiplo de los l_j salvo del i -ésimo y primo relativo con el resto de L_j . Veamos que $\langle s \rangle = \langle \alpha \rangle$.

Si $\lambda = \prod_{i=0}^r L_i$ se tendrá por (1) que para cualquier ciclo disjunto a_i

$$a_i = s^{\frac{\lambda}{L_i}}$$

Con esto hemos probado que $\langle \alpha \rangle \subseteq \langle s \rangle$. Para la otra inclusión, si $L_i = \prod_{j=0}^{i-1} l_j \prod_{j=i+1}^r l_j$ (que recordamos que eran primos relativos) entonces el

$$\text{ord}(\langle s \rangle) = mcm(L_0, \dots, L_r) = L_i * l_i = mcm(l_0, l_1, \dots, l_r) = \text{ord}(\langle \alpha \rangle)$$

para cualquier i subíndice de los coeficientes.

Por lo que concluimos que

$$\langle \alpha \rangle = \langle s \rangle$$

y es un grupo cíclico.

Nuestro caso particular

Vamos a elegir los L_i más simples, para σ la longitud de τ y para τ la de σ . Por tanto

$$\gamma = \sigma^{-2}\tau^{-5} = \sigma^{5-2}\tau = (15398)(47)$$

Se tendrá que

$$\langle \gamma \rangle = \langle \sigma, \tau \rangle$$

Por tanto $\langle \sigma, \tau \rangle$ será un grupo cíclico y uno de sus generadores será γ .

Su **orden** será el mínimo común múltiplo de las longitudes de σ y τ :

$$\text{ord}(\langle \sigma, \tau \rangle) = \text{mcm}(\text{ord}(\sigma), \text{ord}(\tau)) = \text{mcm}(5, 2) = 10.$$

2.4. Cuarto apartado

Sea $n \geq 2$ y $p \leq n$ un número primo. Demostrad que en S_n los únicos elementos de orden p son los productos de ciclos disjuntos de longitud p . ¿Cuántos elementos de orden 2 tiene S_5 ?

Condición suficiente.

Sea $s \in S_n$ una permutación de orden p , si s es un ciclo entonces es evidente. Si no admitirá ser expresado como la composición de ciclos disjuntos $s = a_0..a_r$ que tendrá respectivamente l_0, \dots, l_r órdenes, y por tanto $\text{ord}(a) = \text{mcm}(l_0, \dots, l_r)$ pero claro el $\text{ord}(a) = p$ que es primo, entonces necesariamente $p = l_0 = \dots = l_r$.

Condición suficiente.

Por las consideraciones sobre orden del apartado anterior, sabemos que para $s \in S_n$, descomponible en ciclos disjuntos de longitud p ; entonces su orden va a ser el mínimo común múltiplo del orden de sus ciclos disjuntos, pero como este es siempre p entonces el orden de s es p .

Elementos de orden 2 en S_5

En S_5 existe $\frac{5!}{3!} = 5 \times 4 = 20$ ciclos de orden 2 diferentes.

Y por el apartado anterior todos los elementos de orden 2 que existe serán producto de estos ciclo disjuntos, (sin que importe el orden a la hora de componer):

De lo que deducimos que habrá elementos de orden dos: $2^{20} - 1$

3. Ejercicio 3

3.1. Apartadoo primero

Sean las matrices de Heisenberg.

Demostar que G es un grupo (con producto de matrices). ¿Es abeliano? ¿Es cíclico? ¿Es H un subgrupo de G ? En caso afirmativo, ¿Es normal en G ?

Probar que $f : \leftarrow \mathbb{R}$ defini como $f(A) = a + c$ es un homomorfismo de grupos

G es un grupo.

Por la caracterización de grupo debe cumplir:

1. **Existencia de un elemento neutro**, la matriz identidad pertenece a G (que por tanto es no vacío) y a demás es el elemento neutro.
2. **Propiedad asociativa**. El producto de matrices es asociativo, así que aquí también lo será.
3. **Existencia de un elemento inverso** en G para todo elemento de G . Esto se ve fácilmente de la siguiente manera:

$$\text{Sea } A \in G \text{ y por tanto es de la forma } A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

Con $a, b, c \in \mathbb{R}$

Y queremos encontrar una matriz de la forma

$$B = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

Con $x, y, z \in \mathbb{R}$ (incógnitas) que cumplan que $AB = 1$

Por tanto lo único que nos faltaría ver es que el sistem que forman x, y, z tiene solución,

las ecuaciones a las que da lugar son

$$\begin{cases} x + a = 0 \\ y + az + b = 0 \\ z + c = 0 \end{cases}$$

Que tienen como solución $x = -a, z = -c, y = ac - b$ que cumplen $x, y, z \in \mathbb{R}$ y como queríamos demostrar, para toda matriz de G existe su inversa en G .

Es abeliano

El producto de matrices no es conmutativo en general, sin embargo para cualesquiera $A, B \in G$ se cumple que

$$\begin{aligned} AB &= \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+a & y+az+b \\ 0 & 1 & z+c \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a+x & b+za+y \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = BA \end{aligned}$$

No es cíclico

También podríamos haberlo visto por la numerabilidad de \mathbb{R} (sí, confieso que he matado moscas a cañonazos). Que fuera cíclico supondría que \mathbb{R} es numerable, ya que si existiera una matriz $E \in G$, de tal forma que $\langle E \rangle = G$, necesariamente E distinta de la identidad entonces alguna de sus entradas correspondientes a a, b, c serán no nulas, llamemos a la posición en la matriz de esta entrada e . Pues bien si ahora, considera cualquier $r \in \mathbb{R}$, cogemos una matriz R igual a la identidad salvo en e que en vez de 0, tiene en esa casilla r .

Sabemos que por ser un ciclo existiría un n natural tal que $E^n = R$ y por tanto habríamos encontrado una inyección de los reales en los naturales, lo cual es una contradicción.

H es un subgrupo de G

Esto será si para todo $X, Y \in H$ se cumple que $XY^{-1} \in H$ Por el primer apartado hemos visto que si

$$X = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} Y = \begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

entonces la inversa Y será de la forma:

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

y finalente

$$XY^{-1} = \begin{pmatrix} 1 & 0 & x - y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Que es de las formas de las matrices de H , por lo que es un subgrupo.

Normalidad de H en G

Es normal porque G es conmutativo y por tanto para todo $a \in G$ se tendrá que $aH = Ha$

f es un homomorfismo de grupos

Para que sea homomorfismo debe cumplir que $f(AB) = f(A)f(B)$ para cualesquiera matrices $A, B \in G$.

$$f(A) + f(B) = f \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} + f \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} = (a + c) + (x + z)$$

y por otro lado

$$f(AB) = f \begin{pmatrix} 1 & x + a & y + az + b \\ 0 & 1 & z + c \\ 0 & 0 & 1 \end{pmatrix} = (x + a) + (z + c)$$

Ambas expresiones son iguales por tanto es un homomorfismo.

Núcleo de f

Se define el $\ker(f)$ como $\ker(f) = \{e \in G \mid f(e) = 0\}$ luego

$$\ker(f) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & -a \\ 0 & 0 & 1 \end{pmatrix} \text{ con } a, b \in \mathbb{R} \right\}$$

Imagen de f

REDACTAR MEJOR Es todo R , bastará con ver que cierto conjunto de G su imagen ya es R .

Dada una matriz de G fijamos a arbitrariamente y por cómo está definida c podrá ser cualquier real por tanto

No es monomorfismo

Ya que su núcleo no es la identidad.

Es epimorfismo

Ya que $\text{Img}(f) = \mathbb{R}$

3.2. Segundo apartado

Sea $f : S_4 \rightarrow S_6$ la aplicación dada por $f(\sigma) = \bar{\sigma}$, donde $\bar{\sigma}$ es el elemento de S_6 que actúa igual que σ sobre los elementos $\{1, 2, 3, 4\}$ y sobre los elementos $\{5, 6\}$ los fija si σ es par, o los intercambia si σ es impar.

Demostad que f es un homomorfismo inyectivo de grupos y que su imagen está contenida en A_6 .

Es homomorfismo

Para que sea homomorfismo debe cumplir que $f(ab) = f(a)f(b)$, para cualesquiera $a, b \in S_4$.

Distinguiremos los siguientes casos:

- $a, b \in S_4$ pares, entonces ab es par y por tanto $f(a)f(b) = ab = f(ab)$.
- $a, b \in S_4$ impares ambos, entonces ab es par y por tanto $f(a)f(b) = a(56)b(56)$. Como $b \in S_4$ no contendrá ni al 5 ni al 6 y será disjunto con (56) por tanto podemos conmutarlo (solo con ese, no con a .) $a(56)b(56) = ab(56)(56) = ab = f(ab)$ por ser ab par.
- $a, b \in S_4$ con a impar y b par: $f(a)f(b) = a(56)b$ y aplicando de nuevo que $(56), b$ son disjuntos podemos conmutarlos: $a(56)b = ab(56) = f(ab)$ por ser ab impar.
- $a, b \in S_4$ con b impar y a par: $f(a)f(b) = ab(56) = f(ab)$ ya que ab es impar.

Inyectividad de f

Sean $a, b \in S_4$ tales que $f(a) = f(b)$. vamos a ver que necesariamente $a = b$.

$$id = f(a)f^{-1}(b) = f(a)f(b^{-1}) = f(ab^{-1})$$

Donde hemos utilizado que f es un homomorfismo y ahora por cómo se ha construido f , llegamos a la igualdad $id = ab^{-1}$ de la que concluimos que $a = b$ como queríamos probar.

Imagen de f contenida en A_6

El grupo alterado A_n se define como las permutaciones pares de S_n , veamos pues que la imagen de f está formada por permutaciones pares.

Para ello distinguiremos dos casos, ya que toda permutación es par o impar.

- $a \in S_4$ par, luego $f(a) = a$ que será par.
- $a \in S_4$ impar, luego $f(a) = a(56)$ que es composición de dos impares, luego será par.

3.3. Apartado tercero

Sea K un cuerpo de $SL(K) = \{A \in GL_n(K) / \det(A) = 1\}, n \geq 2$.
Demostrad que $SL_n(K)$ es un subgrupo normal de $GL_n(K)$. ¿Quién es el grupo cociente $GL_n/SL_n(K)$?
Si K es un cuerpo finito con q elementos, determinad los órdenes de estos dos grupos, esto es, $|GL_n(K)|$ y $|SL_n(K)|$.

$SL_n(K)$ es un subgrupo de $GL_n(K)$

Sean cuales quiera $A, B \in SL_n(K)$, decir que el determinantes de ambos es 1. Por las propiedades de los determinantes: $\det(AB) = \det(A)\det(B) = 1$ luego $AB \in SL_n(K)$ y por tanto es un subgrupo.

Normalidad

Habremos probado que $SL_n(K)$ es un subgrupo normal de $GL_n(K)$ si para toda $m \in GL_n(K)$, se tiene que $mSL_n(K)m^{-1} \leq SL_n(K)$, o lo que es lo mismo que $\{msm^{-1} | s \in SL_n(K)\} \leq SL_n(K)$.

Y esto es cierto por las propiedades de los determinantes y por estar s en $SL_n(K)$ (ya que $\det(s) = 1$). Veámoslo:

$$\det(msm^{-1}) = \det(m)\det(s)\frac{1}{\det(m)} = \det(s) = 1.$$

por tanto $msm^{-1} \in SL_n(K)$.

y es un subgrupo normal.

Otra forma de verlo, más rápida que la anterior es darse cuenta que la definición dada de $SL(K)$ se corresponde con la del núcleo del determinante y esto es siempre un subgrupo normal.

Caracterización del grupo cociente

Vista la observación anterior y gracias al primer teorema de isomorfía tenemos que

$$\frac{GL_n(K)}{SL_n(K)} \cong \det_*(GL_n(K)) = K^\times \quad (2)$$

Nótose que no es isomorfo a K ya que $GL_n(K)$ son las matrices invertibles con entradas en K , es decir su determinante no puede ser nulo.

Órdenes para K finito de q elementos.

Por la caracterización del grupo cociente (2) y por ser K un cuerpo finito de q elementos tenemos que:

$$|GL_n(K)| = (q - 1)|SL_n(K)| \quad (3)$$

Si hay q elementos y las matrices son de $n \times n$. Se tendrá que cada fila admite q^n combinaciones, pero tenemos que tener en cuenta:

- Que la primera no puede ser nula, lo cual nos deja $q^n - 1$ posibilidades.
- Que la fila $m + 1 \leq n$ no puede ser combinación lineal de las m anteriores, es decir que admite $q^n - q^m$

De lo que se deduce que:

$$|GL_n(K)| = \prod_{i=0}^{n-1} (q^n - q^i)$$

y por (3) que si $q > 1$:

$$|SL_n(K)| = \frac{1}{q - 1} \prod_{i=0}^{n-1} (q^n - q^i)$$

El caso $q = 1$ no se puede dar ya que $n \geq 2$ y toda matriz con todas sus entradas iguales tienen determinante 0 y no son invertibles, es decir $GL_n(k) = \emptyset$.

Esto nos sugiere además que para que la ecuaciones sean válidas, $q \leq 2$, ya que la matriz identidad de $GL_n(k)$ tienen dos elementos y es siempre invertible.

4. Ejercicio 4

4.1. Apartado primero

Sean A, B, C subgrupos de un grupo G con $B \trianglelefteq A$.
Demostrad que $B \cap C \trianglelefteq A \cap C$ y que

$$\frac{A \cap C}{B \cap C} \cong \frac{B(A \cap C)}{B}$$

$B \cap C$ es subgrupo de $A \cap C$

Por la caracterización de subgrupo tenemos que comprobar que para cualquier $a, b \in B \cap C$ se cumple que $ab^{-1} \in B \cap C$.

Sean $a, b \in B \cap C$ o equivalentemente dos elementos que cumplen que $a, b \in B$ y $a, b \in C$ donde B, C son ambos subgrupos, y por tanto deducimos que $ab^{-1} \in B$ y $ab^{-1} \in C$, es decir que $ab^{-1} \in B \cap C$.

Por hipótesis sabemos además que $B \trianglelefteq A$ luego si $ab^{-1} \in B$ también se tendrá que $ab^{-1} \in A$; y como ya habíamos visto antes que $ab^{-1} \in C$ entonces $ab^{-1} \in A \cap C$; probando con ello lo que buscábamos, que $B \cap C$ es subgrupo de $A \cap C$.

$B \cap C$ es subgrupo normal de $A \cap C$

$$\frac{A \cap C}{B \cap C} \cong \frac{B(A \cap C)}{B}$$

Si además $C \trianglelefteq G$, demostrad que $BC \trianglelefteq AC$ y

$$\frac{AC}{AC} \cong \frac{A}{A \cap (BC)}.$$

4.2. Apartado segundo