Ayudantia 1

Viernes 19 de Agosto 2022

Lo primero en la ayudantía fue mostrar el grupo $(Q_8, \cdot)$, donde la operación es la multiplicación de matrices. En lo que sigue demostraremos que efectivamente sea un grupo.

Problema 1.1: Sea $Q_8 = \{\pm 1 = \pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \pm i = \pm\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right), \pm j = \pm\left(\begin{smallmatrix}0&i\\i&0\end{smallmatrix}\right), \pm k = \pm\left(\begin{smallmatrix}i&0\\0&-i\end{smallmatrix}\right)\}$ el grupo de cuaterniones con la multiplicación de matrices (Es necesario remarcar, que tiene ocho elementos. Ya que por ejemplo, ± 1, representa al elemento 1 y al elemento -1). Para ganarse el nombre de grupo, debemos verificar que la operación esté bien definida y que cumpla con las tres propiedades de la definición de grupo.

Demostración: 1° ¿La operación está bien definida? En este caso, solo debemos verificar que el recorrido del operador esté bien definido. O sea, que si multiplicamos dos elementos del conjunto, el elemento resultante debe seguir estando en el conjunto (otra forma de decir esto, es decir que el conjunto sea cerrado bajo la multiplicación). Con el dolor de mi corazón, la forma para probar esto que ocuparemos, será multiplicar cada elemento con otro y ver el resultado.
Calculando tenemos: $(\pm 1)^2 = 1, (\pm i)^2 = (\pm j)^2 = (\pm k)^2 = -1, (\pm i)(\pm j) = (\pm k), (\pm j)(\pm k) = (\pm i), (\pm k)(\pm i) = (\pm j), (\pm j)(\pm i) = (\mp k), (\pm k)(\pm j) = (\mp i), (\pm i)(\pm k) = (\mp j)$.
Antes de seguir, recordemos que -1 conmuta con todas las matrices, en particular, con los elementos de Q_8. Por lo tanto, casi todo el resto de posibles combinaciones podemos otenerla al multiplicar por -1. Al recordar que 1 es la matriz identidad, obtenemos el resto de combinaciones.
Concluimos que la operación es cerrada bajo multiplicación, ergo, esta bien definida.

2° ¿La operación satisface la asociatividad? Nosotros sabemos que la multiplicación de matrices es asociativa, de todas formas lo haremos para matrices cualesquiera. Hay que verificar que (AB)C=A(BC) $\forall A, B, C \in Q_8$.
Sean $a, b, c, d, e, f, g, h, , l, m, n, p \in \{\pm 1, \pm i, 0\}$, calculando y reorganizando tenemos: $[\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\left(\begin{smallmatrix}e&f\\g&h\end{smallmatrix}\right)]\left(\begin{smallmatrix}l&m\\n&p\end{smallmatrix}\right) = \left(\begin{smallmatrix}ae+bg & af+bh\\ce+dg & cf+dh\end{smallmatrix}\right)\left(\begin{smallmatrix}l&m\\n&p\end{smallmatrix}\right) = \left(\begin{smallmatrix}ael+bgl+afn+bhn & aem+bgm+afp+bhp\\cel+dgl+cfn+dhn & cem+dgm+cfp+dhp\end{smallmatrix}\right) = \left(\begin{smallmatrix}ael+afn+bgl+bhn & aem+afp+bgn+bph\\cel+cfn+dgl+dhn & cem+cfl+dgn+dhp\end{smallmatrix}\right) = \left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\left(\begin{smallmatrix}el+fn & em+fp\\gl+hn & gn+hp\end{smallmatrix}\right) = \left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)[\left(\begin{smallmatrix}e&f\\g&h\end{smallmatrix}\right)\left(\begin{smallmatrix}l&m\\n&p\end{smallmatrix}\right)]$. Como eran matrices cualesquiera, concluimos que la operación si satisface la propiedad.

3° ¿Existe un neutro?, para todo elemento. Este apartado es más directo. Esto se debe a que ya sabemos que el $1 \in Q_8$, satisface: 1A=A1=A, $\forall A \in Q_8$; lo sabemos porque 1 lo satisface para toda matriz, por lo que en particular, para toda matriz en Q_8. Concluimos que si existe un neutro, para todo elemento.

4° Para todo elemento, ¿existe un inverso? Por último, debemos verificar que $\forall A \in Q_8 \, \exists A^{-1} \in Q_8$ tal que $AA^{-1} = A^{-1}A = 1$. Volviendo a ver las multiplicaciones, nos damos cuenta que: $(\pm 1)^4 = (\pm i)^4 = (\pm j)^4 = (\pm k)^4 = 1$, reordenando tenemos: $(\pm 1)(\pm 1)^3 = (\pm i)(\pm i)^3 = (\pm j)(\pm j)^3 = (\pm k)(\pm k)^3 = 1$, así podemos decir que: $A^{-1} = A^3 \, \forall A \in Q_8$. Concluimos que para todo elemento, si existe un inverso.

Luego de haber verificado todo, obtenemos que Q_8 con la multiplicación de matrices, es un grupo.□

Siguiendo con la ayudantía, vimos una definición de subgrupo generado por un conjunto. Luego, un ejemplo de tal definición, ejemplo el cual demostramos que es un grupo.
Pero antes, debemos definir la ïnversa"de un conjunto.

Definición 1.2: Sea G un grupo y S⊆G. $S^{-1} := \{s^{-1} \in G | s \in S\}$. Es importante remarcar, que S^{-1} es un subgrupo sí y solo si S es un subgrupo. Y cuando eso pasa, queda como ejercicio para el lector demostrar que $S^{-1} = S$.

Definición 1.3: Sea G un grupo y S⊆G no vacío. Denotamos por $\langle S \rangle$ al subgrupo generado por S, definido como: $\langle S \rangle := \{g \in G | \exists n \in \mathbb{N}, \exists s_1, s_2, ..., s_n \in S \cup S^{-1} : g = s_1 \cdot s_2 \cdot \cdots \cdot s_n\}$.

Recordatorio: Si $[x], [y] \in \mathbb{Z}/n\mathbb{Z}$, tendremos que [x]=[y] sí y solo si $x - y|n$.

Ejemplo 1.4: Sea $G = \mathbb{Z}/4\mathbb{Z} = \{[0], [1], [2], [3]\}$, en clases se vio que $(\mathbb{Z}/4\mathbb{Z}, +)$ es un grupo bajo la suma de clases. Sea $S = \{[2]\}$, calcularemos $\langle S\rangle = \langle\{[2]\}\rangle$ y demostraremos que es un subgrupo de G.
Comentario: Podriamos decir que, el subgrupo generado por S, es el conjunto de los elementos de S, de S^{-1} y de todas las posibles sumas entre los elementos de $S \cup S^{-1}$. Pero S tienes solo un elemento, deducimos que S^{-1} también tiene solo un elemento.
Surge la pregunta, ¿Cual es el inverso de [2]? Es fácil ver que: [2]+[2]=[2+2]=[4]=[0] (ya que $4 - 0|4$). Dado que [0] es el neutro de G, obtuvimos que [2] es su propio inverso. Y por lo tanto $S^{-1} = \{[2]\}$.
Así, por el comentario anterior, $\langle S\rangle = \{[2] + [2], [2]\} = \{[0], [2]\}$.
En lo que sigue, Demostraremos que efectivamente $\{[0], [2]\} \leq G$. Para eso ocuparemos una proposición vista en clases.

Recordatorio: Un subconjunto K de un grupo es un subgrupo sí y solo si K es no vacío, todos sus elementos tienen un inverso y es cerrado bajo la operación del grupo.

Demostración: 1° Nuestro conjunto, ¿es vacío? Es evidente que no es vacío, ya que posee dos elementos.

2° Los elementos de nuestro conjunto, ¿tienen a sus respectivos inversos dentro del conjunto? Ya vimos que [2] es su propio inverso, ya sabemos que [0] es su propio inverso. Concluimos que todos los elementos del conjunto tienen un inverso en el conjunto.

3° Nuestro conjunto, ¿es cerrado bajo la operación del grupo? Para verificar esto, debemos ver que todas las posibles sumas entre los elementos de nuestro conjunto, siguen estando en el conjunto. Dado que nuetro conjunto tiene dos elementos y el grupo G es conmutativo, solo tenemos tres posibles sumas: $[2] + [2]$, $[2] + [0]$, $[0] + [0]$. Estas sumas dan [2] o [0], por lo que concluimos que nuestro conjunto es cerrado bajo la multiplicación.

Luego, $\langle S\rangle \leq G$. □

En la ayudantía además se mostró la notación exponencial usada en un grupo $(G, \cdot)$.

Notación 1.5: Sea $(g, n) \in (G \times \mathbb{N})$:
$g^n := g \cdots g. \, n - veces$
$g^0 := id_G.$
$g^{-n} := g^{-1} \cdots g^{-1}. \, n - veces$
Si la operación es suma envés de multiplicación, la notación queda:
$ng := g + \cdots + g. \, n - veces$
$0g := id_G.$
$(-n)g := (-g) + \cdots + (-g). \, n - veces$

Ejercicio para el lector: Teniendo en cuenta la notación anterior. Sea $(G, \cdot)$ un grupo. Demostrar $\forall g \in G$ y $a, b \in \mathbb{Z}$ que:
$g^{a+b} = g^a g^b$
$g^{ab} = (g^a)^b$
Hint: Usar inducción. Queda a disposición del lector si usar inducción en a o en b.

De la definición 1.3, se preguntó por los subgrupos cíclicos.

Problema 1.6: Sea $(G, \cdot)$ un grupo. Demostrar que un subgrupo cíclico no es más que un subgrupo generado por un singleton.

Recordatorio: Sea $a \in G$. Denotamos por subgrupo cíclico a $\langle a\rangle := \{a^m | m \in \mathbb{Z}\}$. Si G es finito, m puede solo pertenecer a los naturales.

Demostración: La demostración consiste en probar la igualdad $\langle a\rangle = \langle\{a\}\rangle$, igualdad que probaremos por equivalencia de elementos.
Por el recordatorio anterior; $g \in \langle a\rangle \iff g = a^m$, para algún m entero.
Por notación 1.5; $g = a^m$, para algún m entero $\iff g = a^b \cdots a^b$; con $b = 1$ si $m > 0$; con $b = -1$ si $m < 0$; con

$b = 0$ si $m = 0$.
(Notar que $a^0 \cdots a^0 = id_G \cdots id_G = id_G$).
Como $a \in \{a\}$, $a^{-1} \in \{a\}^{-1}$(definición 1.2) y $id_G = a \cdot a^{-1}$. Tenemos que por definición 1.3; $g = a^b \cdots a^b$, con $b \in \{-1, 0, 1\} \iff g \in \langle\{a\}\rangle$. Aquí me parece importante recalcar que, la definición 1.3 no pide que los s_i ($i \in [1, n]$) deban ser distintos, perfectamente pueden ser iguales.
Con estas equivalencias demostramos que un elemento esta en un conjunto si y solo si esta en el otro. Concluimos que $\langle a \rangle = \langle\{a\}\rangle$. □

En la ayudantía se preguntó, ¿como podemos identificar todos los subgrupos de un grupo? A esta difícil pregunta, la abordamos en el caso particular de los enteron con la suma.

Problema 1.7: Sea K un subgrupo de $(\mathbb{Z}, +)$. Entonces $K = n\mathbb{Z}(:= \{tn \,|\, n \in \mathbb{Z}\} = \langle n \rangle)$ para algún n natural o el cero.

Demostración: Para esta demostración, denotaremos por $I(K) := \{k \in K \,|\, k \in \mathbb{N}\} = K \cap \mathbb{N}$.

Como K es un subgrupo, en particular, K es no vacío y contiene al 0. Además si K contiene un elemento negativo, debe contener a su inverso, o sea, contiene un natural.

Por el apartado anterior, nos quedamos con dos casos:

1° $I(K) = \emptyset$: Como K tiene un elemento negativo si y solo si tiene un natural, este caso solo puede suceder si $K = \{0\} = 0\mathbb{Z}$. Por lo que este caso esta verificado.

2° $I(K) \neq \emptyset$: En este caso, tenemos un conjunto de los naturales no vacío. Así, por el principio del buen orden, $I(K)$ tiene un elemento mínimo; esto quiere decir, $\exists n \in I(K)$ tal que $n \leq m$, $\forall m \in I(K)$. Así, nuestro objetivo será probar que $\forall a \in K$, $\exists b \in \mathbb{Z}$ tal que $a = bn$.

Primero probaremos nuestro objetivo para los naturales en K. Sea $m \in I(K)$; como n es minimal y por la división en $\mathbb{Z}$ tenemos: $m = tn + r$ tal que $t \in \mathbb{N}$ y $0 \leq r < n$.
Asumiremos que $m - tn \in K$, lo demostraremos depués. Así tenemos que $r = m - tn \in K$. Pero como n es el menor natural en K y $r < n$, necesariamente r no puede ser natural, por lo tanto $r = 0$.
Acabamos de probar, que si $m \in I(K)$, entonces $m = tn$ con $t \in \mathbb{Z}$. Entonces los naturales ya estan verificados, pero como dijimos, K tiene elementos naturales si y solo si tiene elementos negativos. Por lo que nos falta ver que pasa con los elementos negativos de K.

En segundo lugar, probaremos nuestro objetivo para los negativos en K. Sea $m \in \mathbb{Z}^- \cap K$. De nuevo, como K es un subgrupo, $-m \in K$. En particular, $-m \in I(K)$, por lo tanto $\exists t \in \mathbb{Z}$ tal que $-m = tn$, o sea, $m = (-t)n$, o sea, $\exists d \in \mathbb{Z}$ tal que $m = dn$. Por lo que los negativos en K ya están verificados.

En tercer lugar, alguien podría preguntarse ¿Que hay del 0? Una pregunta totalmente justificada. Puesto que dijimos que 0 está en K, pero ni es natural (ya que estamos en Chile) ni es negativo. Solo que sabemos que $0 = 0n$, ergo, ya podemos decir que $\forall a \in K$, $\exists b \in \mathbb{Z}$ tal que $a = bn$. Y concluir que $K = n\mathbb{Z}$, para algún $n \in \mathbb{N}$. □

Lema: Demostrar que $m - tn \in K$. Esta es la demostración de lo que asumimos en el problema 1.7.

Demostración: Ya sabemos que $n \in K$.
Luego, como K es cerrado bajo la suma, $n + \cdots + n \in K$, independiente cuantas veces se sume de maner finita n. Así, si la sumamos t-veces, llegamos a que $tn \in K$.
Como K contiene los inversos de todos sus elementos, en particular, $-tn \in K$.
Para terminar, nos acordamos que $m \in K$ y que K es cerrado bajo la suma, conlcuimos que $m - tn = m + (-t)n \in K$. □

Finalmente, vimos unos de los problemas que se habían preparado para la ayudantía.

Problema 1.8: Sea $(G, \cdot)$ un grupo. Sea $g \in G$ fijo. La función $\sigma_g : G \longrightarrow G$, $x \longmapsto gx$ ¿Es un homomorfismo?
a)Si, siempre.
b)No necesariamente. A veces si, a veces no.
c)No, nunca.

Para los que se lo preguntan, aquí la respuesta correcta es la opción b), pero hay que probarlo. Para demostrar que a veces si es un homomorfismo y a veces no, basta con dar un ejemplo en el que sea un homomorfismo y un ejemplo en el que no. Pero como a uno los ejemplos no siempre le caen del cielo, veremos que significa que tal función sea un homomorfismo, a ver si eso nos facilita el encontrar los ejemplos.

Supongamos que σ_g es un homomorfismo: Por definición de homomorfismo, nuestra suposición se cumple si y solo si $\sigma_g(xy) = \sigma_g(x)\sigma_g(y),\ \forall (x,y) \in G \times G$.
Ocupando la definición de nuestra función, $\sigma_g(xy) = \sigma_g(x)\sigma_g(y),\ \forall (x,y) \in G \times G$ si y solo si $g(xy) = (gx)(gy),\ \forall (x,y) \in G \times G$.
Utilizando la asociatividad de nuestro grupo, $g(xy) = (gx)(gy),\ \forall (x,y) \in G \times G$ si y solo si $(gx)y = (gx)(gy),\ \forall (x,y) \in G \times G$.
Multiplicando $(gx)^{-1}$ por la izquierda($\Rightarrow$), (gx) por la derecha($\Leftarrow$), $(gx)y = (gx)(gy),\ \forall (x,y) \in G \times G$ si y solo si $y = (gy),\ \forall (x,y) \in G \times G$.
Multiplicando $(y)^{-1}$ por la derecha($\Rightarrow$), (y) por la izquierda($\Leftarrow$), $y = (gy),\ \forall (x,y) \in G \times G$ si y solo si $id_G = g,\ \forall (x,y) \in G \times G$.

En conclusión, acabamos de demostrar que σ_g es un homomorfismo si y solo si $g = id_G$. Por lo que se deja encontrar los ejemplos al lector.
Comentario: Para esta demostración, solo ocupamos definiciones y un poco de cancelación de elementos.