Semana 10: Grupos

1. Grupos

Hasta ahora, hemos explorado la estructura de grupo en varias ocasiones pero sólo de manera incidental, sin embargo nos vemos en la necesidad de presentarla de manera explícita. En esta sección desarrollaremos los conceptos necesarios para clasificar como grupos algunas estructuras que hemos estado desarrollando a lo largo del curso.

Definición 10.1. Sea G un conjunto cualquiera y sea $*$ una operación binaria sobre G. La pareja $(G, *)$ se dice *un grupo* si satisface:

1. Para cualesquiera x, y y z en el conjunto G, se cumple
$$(x * y) * z = x * (y * z).$$
2. Existe un único elemento e de g, denominado *la identidad de* G, tal que para todo x en G,
$$e * x = x * e = x.$$
3. Para cada elemento x del conjunto G, existe un único elemento x^{-1} en el mismo conjunto, denominado *inverso de* x, de forma que
$$x * x^{-1} = x^{-1} * x = e.$$

Si además, un grupo satisface $x * y = y * x$ para todo x e y en el conjunto G) decimos que el grupo es *abeliano*. Una denominación alternativa, y más natural, es *conmutativo*. Por último, si el conjunto G tiene n elementos, diremos que *el grupo* G *tiene orden* n.

Presentamos ahora una serie de ejemplos los cuales se discuten únicamente de manrea informativa y bajo qué condiciones satisfacen la definición de grupo. La prueba que dichas elecciones en verdad satisfacen la definición de grupo queda a cargo del lector.

Ejemplo. El conjunto de los enteros $\mathbb{Z}$ con la suma entre enteros como la operación, forma un grupo tomando 0 como la identidad del grupo y $-m$ como el inverso de un entero m. De la misma forma lo hacen $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$. Estos grupos son ocasionalmente denotados como $\mathbb{Z}_+$, $\mathbb{Q}_+$ y $\mathbb{R}_+$.

Ejemplo. El conjunto $\mathbb{Z}_\times$, no forma un grupo, pues ninguno de sus elementos, salvo 1 y -1, tiene inverso multiplicativo.

Ejemplo. El conjunto de los todos los racionales distintos de cero, junto al producto racional como operación, forma un grupo tomando 1 como la identidad y $1/r$ como el inverso de un racional r. De manera similar, lo hacen los mismos subconjuntos en $\mathbb{R}$ y $\mathbb{C}$. A estos ocasionalmente se les denota como $\mathbb{Q}_\times$, $\mathbb{R}_\times$ y $\mathbb{C}_\times$.

Ejemplo. Para un anillo R, el conjunto base junto a la operación $+$ del anillo, forman un grupo tomando 0_R como identidad y los inversos de la suma en el anillo como los inversos; a este grupo se le denomina *el grupo aditivo de R* y es común denotarlo como R_+. Sin embargo, R junto al producto no necesariamente forma un grupo, pero si forma un grupo abeliano, entonces R resulta un campo. Si R es un campo, todos sus elementos distintos de 0_R forman un grupo bajo la multiplicación tomando 1_R como la identidad y a los inversos en el campo como los inversos del grupo. En ocasiones se denota a éste como $R_\times$.

Ejemplo. El conjunto $S^1 \subset \mathbb{C}$ definido

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$$

junto al producto complejo como operación, forma un grupo tomando 1 como la identidad y notando que los conjugados funcionan como los inversos.

Ejemplo. Para un conjunto cualquiera A, el conjunto S_A formado por las permutaciones de A es un grupo bajo la composición. La función identidad 1_A resulta su elemento identidad mientras que sus inversos están dados por las funciones inversas.

Ejemplo. Dado un conjunto E, el conjunto potencia 2^E junto a la diferencia simétrica, definida como

$$A + B = (A \backslash B) \cup (A \backslash B),$$

forma un grupo abeliano tomando $\varnothing$ como la identidad y el mismo conjunto A como su inverso.

En general, no indicaremos la operación asociada al grupo sino simplemente el conjunto G. Esto quiere decir que no haremos distinción entre un grupo $(G, *)$ y el conjunto base G. Esto, aunque parecería extraño, es en realidad una práctica que resulta muy útil cuando se describen muchos de los resultados que buscamos.

Comentario. En el caso del grupo $(\mathbb{Z}, +)$ es interesante observar que la notación derivada de la definición como grupo, vuelve la representación de los inversos un tanto extraña pues $m^{-1} = -m$. Esto, por supuesto, es indeseable y usaremos la siguiente convención: Un grupo G en el cual su operación asociada está representada por el símbolo $+$ se dirá en *notación aditiva*, su elemento identidad se escribirá 0_G mientras que sus inversos se escribirán $-g$. En otras palabras, los axiomas de grupo para la identidad e inversos toman la siguiente forma:

1. Para todo x en el conjunto G,
$$x + 0_G = 0_G + x = x.$$
2. Para todo x en el grupo G, existe $-x$ en el grupo de forma que
$$x + (-x) = (-x) + x = 0_G.$$

Además, se conviene que un grupo en notación aditiva es siempre abeliano. Esta convención no obliga a que todo grupo abeliano sea escrito en notación aditiva; de hecho, en todos los ejemplos anteriores las operaciones asociadas son conmutativas pero no todos están escritos en notación aditiva. Es importante señalar sin embargo y a pesar de los ejemplos, hay grupos que no son conmutativos, por ejemplo, en la lectura pasada mostramos que el grupo de permutaciones no es, en general, conmutativo.

Una de las ventajas de trabajar en abstracto, es dar respuesta a preguntas en un complejo bloque de estructuras. Como ejemplo de esto, se pueden probar las leyes de cancelación en la operación de grupo, por lo que se puede asumir el resultado en todos los ejemplos anteriores y posteriores. Lo anterior sucede sin necesidad de tomar en cuenta las particularidades de cada caso. Veamos algunos ejemplos más de estos resultados.

Proposición 10.1. *En grupo un G cualquiera, son válidas las leyes de cancelación, i.e., para cualesquiera a, b y c elementos del grupo, si se tiene $a * b = a * c$ o $b * a = c * a$, entonces $b = c$.*

Demostración. Por los axiomas de grupo, existe el elemento a^{-1} en el grupo. Por esto, si $a * b = a * c$, entonces

$$\begin{aligned} b &= e * b \\ &= (a^{-1} * a) * b \\ &= a^{-1} * (a * b) \\ &= a^{-1} * (a * c) \\ &= (a^{-1} * a) * c \\ &= e * c \\ &= c. \end{aligned}$$

Bajo la otra hipótesis, el resultado se demuestra por analogía. ■

La proposición anterior tiene el propósito de ilustrar lo explícito que puede resultar el usar los axiomas de grupo y, aunque en general no es necesaria tanta precisión, ante cualquier duda lo mejor será proveer un argumento tan explícito como el anterior.

Proposición 10.2. *Para cualesquiera elementos a y b de un grupo G, se tiene*

1. $(a^{-1})^{-1} = a$.
2. $(a * b)^{-1} = b^{-1} * a^{-1}$.

Demostración. El resultado sigue de manera muy natural de la unicidad del inverso. Debemos notar de la definición de grupo que

$$a^{-1} * \left(a^{-1}\right)^{-1} = e = a^{-1} * a,$$

y considerando que obtenemos la misma igualdad si invertimos lo papeles de a y su inverso, debemos concluir que $(a^{-1})^{-1} = a$. De manera similar,

$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * a^{-1} = e,$$

implica que lo expuesto en 2, comprobando el resultado. ■

Como se puede ver en la anterior proposición es relativamente incómodo escribir la operación del grupo cuando hay mas dos elementos involucrados. Por eso convendremos que $ab = a * b$ para simplificar nuestra discusión cuando esto no implique potenciales ambigüedades y cuando el grupo no esté escrito en notación aditiva.

Definición 10.2. Sea a un elemento cualquiera de un grupo G. Definimos $a^0 = e$ y para un entero positivo n,

$$a^n = \underbrace{a * \cdots * a}_{n \text{ veces}}.$$

Además,

$$a^{-n} = \left(a^{-1}\right)^n.$$

Comentario. Para un grupo en notación aditiva, los exponentes toman una notación completamente distinta: Para un entero no negativo n,

$$na = \underbrace{a + \cdots + a}_{n \text{ veces}}$$

y

$$(-n)a = n(-a).$$

Uno puede establecer una analogía directa con el caso de anillos, donde se definían de manera análoga usando la suma asociada al anillo. Sin embargo, cualquier resultado que se obtenga con exponentes se puede formular en notación aditiva sin mucho trabajo.

Proposición 10.3. *Sea G un grupo y sean a y b elementos de éste. Para enteros m y n se cumple:*

1. *Si $ab = ba$, entonces $(ab)^n = a^n b^n$.*
2. *$(a^n)^m = a^{mn}$.*
3. *$a^m a^n = a^{m+n}$.*

Demostración. Se probará sólo 1. Los otros incisos resultan idénticos a los probados en los naturales, enteros, reales, etc. y se dejan como ejercicio (10.3). Para probar 1) usaremos inducción para probar un resultado parcial. Primero, asumimos que a y b conmutan, en ese caso $(ab)^0 = e = a^0 b^0$; supongamos ahora $(ab)^n = a^n b^n$, entonces

$$\begin{aligned}(ab)^{n+1} &= (ab)^n (ab) \\ &= a^n b^n ab \\ &= (a^n a)(b^n b) \\ &= a^{n+1} b^{n+1}.\end{aligned}$$

Por inducción, se satisface para todo entero no negativo n, que $(ab)^n = a^n b^n$.

Para probar el resultado en los enteros negativos, debemos convencernos que a^{-1} y b^{-1} conmutan también (ejercicio 10.4) y suponiendo que n es un entero positivo, la conclusión del párrafo

anterior resulta en

$$\begin{aligned}(ab)^{-n} &= \left((ab)^{-1}\right)^n \\ &= \left(a^{-1}b^{-1}\right)^n \\ &= \left(a^{-1}\right)^n \left(b^{-1}\right)^n \\ &= a^{-n}b^{-n}.\end{aligned}$$

El resultado entonces sigue indistintamente para enteros positivos y negativos como afirma el resultado. ■

2. Subgrupos

Definición 10.3. Sea G un grupo. Un subconjunto $H \subseteq G$, se dice *un subgrupo* si:

1. $e \in H$.
2. Si para cada par x e y de H se tiene que $x * y \in H$.
3. Si x en un elemento de H, entonces x^{-1} también lo es.

Comentario. La segunda propiedad que define a un subgrupo es comúnmente mencionada diciendo que *H es cerrado en G*.

Para simplificar un poco nuestras expresiones escribiremos $H \leq G$ cuando H sea subgrupo de G. Es importante notar que cada subgrupo forma un grupo por si mismo. Veamos algunos ejemplos en el mismo espíritu que la sección anterior: Son informativos y los pasos deben proveerse por el lector.

Ejemplo. El subconjunto $\{e\}$ de un grupo G, es un subgrupo, al cual se le denomina *el subgrupo trivial*.

Ejemplo. En $\mathbb{Z}$ como grupo aditivo, los números pares forman un subgrupo. Los impares sin embargo no lo hacen al siempre obtener un par de la suma de dos impares. En general, para un entero cualquiera m, el conjunto H_m, formado por todos los múltiplos de m, forma un subgrupo de $\mathbb{Z}$ como grupo aditivo.

Ejemplo. El conjunto Γ_m formado por los complejos z de que satisfacen $z^m = 1$ es un subconjunto de S^1. Es además es un subgrupo de S^1.

Ejemplo. Si $F \subseteq E$, entonces $2^F \leq 2^E$, considerando a 2^E como grupo usando a la diferencia simétrica como operación.

Ejemplo. Considerando $\mathbb{R}^2$ como grupo aditivo, cualquier recta que pase por el origen es un subgrupo de $\mathbb{R}^2$. Por el contrario, si la recta no pasa por el origen, la linea no será un subgrupo.

Ejemplo. Como se discute en el addendum a la parte de teoría de grupos, el grupo ortogonal $\mathrm{O}_2(\mathbb{R})$ es un subgrupo del grupo euclidiano $\mathrm{E}(\mathbb{R}^2)$.

Ejemplo. El conjunto $SO_2(\mathbb{R})$ de rotaciones sobre el origen, es un subgrupo del grupo ortogonal $O_2(\mathbb{R})$. Al grupo $SO_2(\mathbb{R}^2)$ se le denomina *grupo ortogonal especial del plano*.

Podemos acortar la lista de propiedades necesarias para comprobar si un subconjunto de un grupo es un subgrupo (lo cual facilita mostrar que los ejemplos anteriores son en verdad subgrupos bajo la definición).

Proposición 10.4. *Un subconjunto H de un grupo G es un subgrupo si y sólo si H es no vacío y xy^{-1} es un elemento de H para cualesquiera x y y en H.*

Demostración. Primero, como e debe pertenecer a H, éste no puede ser vacío. Supongamos primero que H es un subgrupo y tomemos x y y como elementos cualquiera de éste. Por definición y^{-1} es también un elemento de H y como el conjunto es cerrado, también lo será xy^{-1}.

Supongamos ahora la segunda condición. Como H es no vacío, entonces existe algún elemento y dentro del conjunto. Por hipótesis, esto implica que y^{-1} pertenece de igual forma a H, pero $e = yy^{-1}$ por lo que H contiene a la identidad. Con esto, la hipótesis implica que $y^{-1} = ey^{-1}$ pertenece de igual forma a H. Por último, si x fuera otro elemento de H, como $xy = x\left(y^{-1}\right)^{-1}$ entonces debe también pertenecer a H. En resumen: la identidad está en H, H es cerrado y contiene a los inversos de todos sus elementos. Entonces, H es un subgrupo. ∎

Por último debe notarse que la condición impuesta a un conjunto para ser un subgrupo en notación aditiva resulta $x - y \in H$. Además, podemos ir un poco más lejos pues si observamos sólo subconjuntos finitos, entonces podemos simplificar aún más las propiedades que requiere un subconjunto para ser un subgrupo.

Proposición 10.5. *Sea H un subconjunto finito y no vacío de un grupo G. Si H es cerrado bajo la operación de G, entonces H es un subgrupo de G.*

Demostración. Como H es no vacío, sea $a \in H$. Como es cerrado bajo la operación de G, todos los elementos

$$a, a^2, \ldots a^n \ldots$$

están en H. Sin embargo, H es finito, por lo que la anterior secuencia no puede continuar indefinidamente, esto quiere decir que deben existir naturales $r > s > 0$ tales que $a^r = a^s$. En otras palabras $a^{r-s} = e$ al tener $r - s > 0$. De esto podemos concluir que $e \in H$. Además,

$$a \cdot a^{r-s-1} = a^{r-s} = e,$$

por lo que $a^{-1} = a^{r-s-1}$ y como $r - s - 1 \geq 0$, entonces $a^{-1} \in H$. Por la definición de subgrupo, esto es muestra que H es un subgrupo. ∎

3. Homomorfismos, monomorfismos e isomorfismos

Definición 10.4. Sean $(G, *)$ y $(H, \cdot)$ grupos cualquiera. Una función $f\colon G \to H$ se dice *un homomorfismo de grupos* si, para cualesquiera elementos x e y de G, se cumple, $f(x * y) = f(x) \cdot f(y)$.

Parecería que la estructura del grupo no se transfiere por completo en la definición de homomorfismo pues no hay mención alguna a la identidad, sin embargo, y como en el caso de subgrupos, podemos garantizarlo.

Proposición 10.6. *Si $f\colon G \to H$ es un homomorfismo de grupos, entonces se cumplen $f(e_G) = e_H$ y $f\left(x^{-1}\right) = f(x)^{-1}$ para todo $x \in G$,*

Demostración. Comencemos notando que $e_G = e_G^2$ por lo que

$$f(e_G) = f(e_G * e_G) = f(e_G) \cdot f(e_G).$$

Como $f(e_G)$ es un elemento de H, debe tener inverso, entonces

$$\begin{aligned} f(e_G) &= f(e_G) \cdot \left[f(e_G) \cdot f(e_G)^{-1}\right] \\ &= [f(e_G) \cdot f(e_G)] \cdot f(e_G)^{-1} \\ &= f(e_G) \cdot f(e_G)^{-1} \\ &= e_H. \end{aligned}$$

Además, según lo anterior, para cualquier elemento $x \in G$,

$$\begin{aligned} e_H &= f(e_G) \\ &= f(x * x^{-1}) \\ &= f(x) \cdot f(x^{-1}). \end{aligned}$$

Esto quiere decir que $f(x)^{-1} = f\left(x^{-1}\right)$ al ser los inversos en un grupo únicos. ■

Realmente, la definición junto a la proposición determinan las características que deben satisfacer los homomorfismos. Sin embargo, debe notarse que la notació involucrada se torna voluminosa con facilidad. La realidad es que no hace falta ser tan quisquillosos. Podemos describir estas propiedades sin hacer referencia a la estructura específica del grupo, la cual debe quedar clara en contexto. Esto nos permite simplificar las propiedades de homomorfismo de grupo como

$$f(e) = e,$$

$$f(a^{-1}) = f(a)^{-1}$$

y

$$f(ab) = f(a)f(b).$$

Bajo esta notación, los objetos involucrados en la evaluación de la función deben ser elementos del grupo en el dominio de f mientras el resultado de la evaluación deben ser elementos del grupo en el contradominio de f. En este sentido, no existe ambigüedad alguna al definir a los homomorfismos de esta manera.

Ejemplo. Si $\{e\}$ es un grupo con un elemento, existe sólo un homomorfismo de $\{e\}$ a grupo G, a decir la función $f\colon \{e\} \to G$ con regla de correspondencia $f(e) = e$. De manera similar, sólo hay un homomorfismo de un G al grupo con un elemento: La función constante en e.

Ejemplo. Para un grupo G y un elemento g en éste, siempre podemos considerar una función $f\colon \mathbb{Z} \to G$ de forma que $f(m) = g^m$. Considerando $\mathbb{Z}$ como un grupo aditivo, lo anterior define un homomorfismo pues $f(m+n) = g^{m+n} = g^m g^n = f(m)f(n)$. De alguna forma, esta función convierte a la suma de los enteros en la operación del grupo.

Ejemplo. Si R y S son anillos y $f\colon R \to S$ es un homomorfismo de anillos, entonces la restricción de f al conjunto de unidades de R, R^*, define una función $R^* \to S^*$ la cual es un homomorfismo entre los grupos de unidades.

Definición 10.5. Sea $f\colon G \to H$ un homomorfismo de grupos. Se define *el núcleo de* f como el conjunto

$$\ker f = \{x \in G \mid f(x) = e\}\,.$$

El núcleo de un homomorfismo contiene mucha más información de la que uno puede sospechar. En particular nos da una caracterización de la inyectividad de un homomorfismo. La prueba de este resultado se debe realizar en el ejercicio 10.6.

Proposición 10.7. *Sea $f\colon G \to H$ un homomorfismo de grupos. Entonces,*

1. $\ker f$ *es un subgrupo de* G.
2. f *es inyectiva si y sólo si* $\ker f = \{e\}$.

Definición 10.6. Sea $f\colon G \to H$ un homomorfismo entre grupos. Decimos que:

- f es *un monomorfismo de grupos* si ésta es inyectiva.
- f es *un isomorfismo de grupos* si ésta es biyectiva.

Además, decimos que G *se puede sumergir en* H si existe un monomorfismo de grupos de $G \to H$ y se dice que G y H *son isomorfos* si existe un isomorfismo entre ellos.

Proposición 10.8. *Para un homomorfismo $f\colon G \to H$, la imagen de f es un subgrupo de H.*

Demostración. Consideremos $K = \mathrm{im}(f)$, entonces $K \subseteq H$. Debemos probar que K es un subgrupo y para eso tomaremos un par de elementos a y b en K. En ese caso, podemos encontrar elementos c y d en G de forma que $a = f(c)$ y $f(d) = b$. En ese caso, $ab^{-1} = f(c)f(d^{-1}) = f(cd^{-1}) \in K$. Lo anterior muestra que K es un subgrupo de H y el resultado sigue entonces. ∎

Corolario 10.9. *Si f es un monomorfismo, entonces la imagen de f es isomorfa a G.*

Ejemplo (medio feo)**.** Un isomorfismo de G en G se dice *un automorfismo de* G y al conjunto de automorfismos de G se le denota por $\mathrm{Aut}(G)$. No es difícil convencernos que el conjunto de automorfismos bajo la composición es un subgrupo del grupo de permutaciones de G. Además, cada elemento $a \in G$ define el automorfismo $f_a\colon G \to G$ que tiene como regla de correspondecia $f_a(x) = axa^{-1}$. Esto permite definir la función $F\colon G \to \mathrm{Aut}(G)$ como $F(a) = f_a$ y afirmar que se trata de un homomorfismo. Además, el núcleo de F coincide con el centro de G, por lo que podemos concluir que si un grupo tiene centro trivial, entonces podemos sumergir G en $\mathrm{Aut}(G)$.

4. El teorema de Cayley

El teorema de Cayley es una resultado interesante que nos permite representar a un grupo cualquier como un grupo de permutaciones y las cuales hemos puesto cuidado estudiando. Es muy probable que el enunciado no parezca tan sorprendente, pero es un logro ejemplar. Lamentablemente, habrá que dejar pasar algún tiempo antes de que se pueda apreciar el resultado en todo su esplendor.

Teorema 10.10 (Cayley)**.** *Cada grupo se puede sumergir en un grupo de permutaciones.*

Demostración. Sea G un grupo cualquiera y sea S_G el grupos de permutaciones de G. Ahora, para cada $a \in G$ podemos definir la permutación $f_a \colon G \to G$ como $f_a(x) = ax$. Podemos con esto definir la función $F \colon G \to S_G$ usando la regla de correspondencia $F(a) = f_a$. Mostraremos primero que esta función es un homomorfismo. En efecto, para cualesquiera elementos a y b de G, entonces

$$\begin{aligned} f_{ab}(x) &= (ab)x \\ &= a(bx) \\ &= f_a\left(f_b(x)\right). \end{aligned}$$

Este homomorfismo es además inyectivo pues, si $f_a = 1_G$, entonces $ax = x$ para todo $x \in G$. Como la identidad es única, lo anteior muestra que $a = e$ esto quiere decir que el núcleo de f es el subgrupo trivial y por tanto f es una función inyectiva y por tanto f es un monomorfismo. Al existir un monomorfismo, entonces podemos sumergir G en el grupo de permutaciones S_G. ■

Como la imagen de un monomorfismo es un subgrupo, el teorema de Cayley nos permite representar a cualquier grupo a través de permutaciones. Esto es realmente interesante pues, hasta isomorfismo, los únicos grupos que existen son los subgrupos de los grupos de permutaciones, haciendo con esto a las permutaciones como el ejemplo arquetípico de grupos.

Ejemplo. Según el teorema anterior, el grupo aditivo de $\mathbb{Z}_3 = \{0, 1, 2\}$ puede ser sumergido en el grupo de permutaciones de 3 elementos, i.e., S_3. Los automorfismos definidos por cada elemento del grupo son $f_0, f_1, f_2 \colon \mathbb{Z}_3 \to \mathbb{Z}_3$ dadas por $f_0(i) = i$, $f_1(i) = i + 1$ y $f_2(i) = i + 2$. Esto quiere decir que f_0 es la identidad en S_3. Además, f_1 sólo recorre el elemento un paso adelante por lo que estamos transformando

$$1 \mapsto (1\,2\,3).$$

De manera similar, f_2 mueve los elementos dos pasos adelante por lo que estamos transformando

$$2 \mapsto (1\,3\,2).$$

Además, como

$$1 + 1 \mapsto (1\,2\,3)(1\,2\,3)$$

tenemos que

$$(1\,2\,3)(1\,2\,3) = (1\,3\,2).$$

En resumen, el grupo aditivo de $\mathbb{Z}_3$ es isomorfo al subgrupo de S_3:

$$\{(1), (1\,2\,3), (1\,3\,2)\}.$$

Ejemplo. Considerando el grupo aditivo $\mathbb{Z}_2$, no es difícil probar que el conjunto $\mathbb{Z}_2 \times \mathbb{Z}_2$ junto a la suma entrada a entrada, i.e., $(a, b) + (c, d) = (a + c, b + d)$, forma un grupo. A este grupo se le conoce como el 4-grupo de Klein (o Vierergruppe) el cual puede escribirse como

$$K_4 = \{(0,0), (0,1), (1,0), (1,1)\}.$$

Como es un grupo de 4 elementos, según la prueba del teorema de Cayley podemos sumergirlo en el grupo de permutaciones S_4 de la siguiente manera: Como el elemento $(0, 0)$ es la identidad,

a éste le corresponde la permutación identidad. También, $f_{(0,1)}(x,y) = (x, y+1)$ por lo que se transforma

$$(0,1) \mapsto (1\,2)(3\,4).$$

De manera similar, como $f_{(1,0)}(x,y) = (x+1, y)$, estamos transformando

$$(1,0) \mapsto (1\,3)(2\,4).$$

Finalmente, como $f_{(1,1)}(x,y) = (x+1, y+1)$, estamos transformando

$$(1,1) \mapsto (1\,4)(2\,3).$$

En resumen, el grupo K_4 es isomorfo al subgrupo de S_4 dado por

$$\{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}.$$

Ejercicios

Ejercicio 10.1. Comprueba que los ejemplos posteriores a la definición 10.1 son en verdad grupos.

Ejercicio 10.2. Como debía sospecharse, hemos impuesto demasiadas condiciones a la definición de un grupo. En este ejercicio vamos a debilitar las condiciones para obtener un grupo sin comprometer la estructura. Sea G un conjunto y sea $*$ una operación binaria sobre G que satisfacen las siguientes condiciones:

- La operación $*$ es asociativa.
- Existe un elemento e de forma que para todo x, se tiene $e * x = x$.
- Para cualquier elemento x en G, existe y en G de forma que $y * x = e$.

Demuestra que $(G, *)$ es un grupo. Sugerencia: Observa que las condiciones no son las mismas que en la definición.

Ejercicio 10.3. Termina la prueba de la proposición 10.3 y formula el resultado en notación aditiva.

Ejercicio 10.4. En un grupo G, comprueba que si a y b conmutan, entonces a^{-1} y b^{-1} también lo hacen.

Ejercicio 10.5. Sea $E = \{\alpha, \beta\}$ un conjunto con dos elementos. Demuestra que el grupo formado por el conjunto 2^E junto la diferencia simétrica es isomorfo al grupo de unidades módulo 8. Sugerencia: Escribe los conjunto lado a lado y asocia cada elemento de uno a uno y sólo uno del otro. Sólo hay una forma natural de hacer esto permitiendo que las operaciones se mantengan.

Ejercicio 10.6. Prueba la proposición 10.7.

Ejercicio 10.7. Muestra que $\mathbb{Z}_2 \times \mathbb{Z}_2$, junto a la suma entrada a entrada, es un grupo usando $(0,0)$ como la identidad. Observando la prueba, es posible establecer que éste es un fenómeno mucho más general: Si G y H son grupos, entonces el conjunto $G \times H$ es también un grupo usando la operación

$$(x_1, y_1)(x_2, y_2) = (x_1 x_2, y_1 y_2).$$

Da una prueba de lo anterior.

Ejercicio 10.8. Demuestra que el conjunto de automorfismos es un subgrupo del grupo de permutaciones.

Ejercicio 10.9. Sea $f\colon G \to H$ un homomorfismo de grupos. Demuestra que para todo elemento a del grupo, se cumple:

1. $f(x^{-1}) = f(x)^{-1}$.
2. $f(x^k) = f(x)^k$ para todo entero k.

Sugerencia: Es muy parecido al caso de anillos.

Ejercicio 10.10. Muestra que la función $\varphi\colon G \to \mathrm{Aut}(G)$ definida como $\varphi(a) = f_a$, donde f_a es el automorfismo inducido por a, i.e., $f_a(x) = axa^{-1}$, resulta un homomorfismo.

Para entregar: Ejercicio 10.5

Referencias

[BM70] Birkohff, Garrett y Mac Lane, Saunders: *Álgebra Moderna*. Vicens-vives, 4ª edición, 1970.

[Chi95] Childs, Lindsay N.: *A concrete introduction to higher algebra*. Springer, 2ª edición, 1995.

[Fra87] Fraleigh, John B.: *Álgebra abstracta: primer curso*. Addison Wesley, 1987.

[Rot05] Rotman, Joseph J.: *A first course in abstract algebra*. Pearson, 3ª edición, 2005.

Considerar notas el texto precedente es producto de la imaginación febril de autor. El único propósito al que sirven es dar una interpretación personal de algunos textos que han sido usados para preparar el curso de «Matemáticas discretas» impartido en la carrera de Matemáticas Aplicadas y Computación de la FES Acatlán. Es muy probable que el presente texto esté lleno de errores gramaticales, imprecisiones técnicas y sea sujeto a cambios constantes.