Estructuras algebraicas

Pedro Valero Mejía

29 de septiembre de 2013

1. Grupos

Por definición, sea X un conjunto no vacío, podemos construir el conjunto de pares ordenados X*X=$\{(x,y)/x,y \in X\}$ Vamos a fijar un conjunto X$\neq \varnothing$ y una función φ: X*X $\longrightarrow$ X que a cada par (x,y) le asocia un elemento φ(x,y) $\in$X que expresamos como x*y, siendo '*' cualquier operación.

Definición 1.1 . Sea S un subconjunto no vacío de G, diremos que S es cerrado por φ si la combinación por φ de dos elementos de S da otro elemento del mismo.

Dados x,y,z $\in$ X puede ser interesante el resultado x*y*z pero, por definición, esto no tiene sentido. Sin embargo, si tendrían sentido (x*y)*z ó x*(y*z). Estas operaciones podrían tener, o no, el mismo resultado. Queremos un conjunto con una operación donde no tengamos que preocuparnos por la colocación de los paréntesis. Para ello debemos buscar una operación asociativa.

Dado G$\neq \varnothing$ y φ: G*G $\longrightarrow$ G, diremos que G es un grupo si:

1. (G,*) es asociativa
2. $\exists$ e $\in$G t.q. $\forall$x$\in$G: x*e=x
3. $\forall$x$\in$G $\exists$ x' $\in$G t.q. x*x'=x'*x=e

Ejemplo ($\mathbb{Z}$, +); ($\mathbb{R}$, +); ($\mathbb{R}$-0, $\cdot$); ($\mathbb{R}$/x>0, $\cdot$) son grupos, mientras que ($\mathbb{Z}$, $\cdot$); ($\mathbb{R}$, $\cdot$) no lo son.

A partir de un conjunto A definimos B(A) como el conjunto de todas las biyecciones de A en sí mismo. Puesto que la composicón de dos biyecciones es otra biyección, la composición es una operación definida sobre B(A). Si tomamos como elemento 'e' la biyección identidad y como x' la función inversa, podemos comprobar que B(A) es un grupo respecto a la composición.

En todo grupo se cumplen las propiedades de unicidad del elemento neutro y del inverso. La demostración de estas propiedades es bastante trivial.

Sean dos elementos e, y e' dos elementos neutros de nuestro grupo G, se cumple que e*e'=e', pero tambien se cumple que e'*e=e. Esto implica que e'=e.

Por otro lado, si suponemos la existencia de dos elementos inversos a', a'' $\in$G, entonces $e = a*a' = a*a''$. Si multiplicamos por a en ambos lados de la ecuación tenemos: $a*(a*a') = (a*a')*a''$, pudiendo reordenar los paréntesis por la propiedad asociativa. Así pues, obtenemos $a' = a''$. En esta última demostración nos hemos apoyado en la propiedad cancelativa, que sólo se presenta cuando trabajamos en un grupo.

Definición 1.2 . Transformaciones lineales rígidas son aquellas que conservan las distancias. (En $\mathbb{R}^2$ sólo están las simetrías y giros).

Ejemplo Vamos a trabajar con un triángulo equilátero, Δ en $\mathbb{R}^2$ y vamos a encontrar el conjunto de todas las aplicaciones lineales rígidas que llevan el triángulo en si mismo. $D_3 = \{f \in G / f(\Delta) \longrightarrow \Delta\}$. Para empezar, dentro de este grupo encontramos todos los giros de águlo 120º. Si defino $a = g_{2\pi/3}$, tenemos las aplicaciones: e, a y $a * a$, ya que la aplicación $a * a * a = e$, $a * a * a * a = a$ y así sucesivamente, por completar vueltas al círculo unidad. Por otro lado, también tenemos las simetrías que tienen como eje las alturas del triángulo. Denotaremos estas simetrías como: S_1, S_2 y S_3. Sabemos que la combinación de un giro y una simetría tiene como resultado otra simetría. Si combinamos $a * S_1$ obtenemos otra simetría, que también deja el triángulo en si mismo. Así pues, esta simetría, debe tratarse de S_2 ó S_3. Lo mismo ocurre con $a * a * S_1$.

Así, tenemos: $D_3 = \{e, a, a * a, S_1, a * S_1, a^2 * S_1\}$

La representación geométrica de un grupo consiste en la descripción de los elementos geométricos que lo constituyen. En el caso del ejemplo, consistiría en indicar qué giros y simetrías constituyen el grupo. La representación abstracta o algebraica de un grupo suele realizarse por medio de una tabla, o una serie de restricciones sobre las operaciones de combinación de los elementos del grupo, sin necesidad de indicar qué es realmente cada elemento.

Ejemplo La representación abstracta de D_3 viene dada por tres condiciones:

- ord(g)=3
- ord(s)=2
- $g * s = s * g^2$

Ya que con estas condiciones podríamos construir una tabla con todas las combinaciones 2 a 2 de elementos del grupo sin necesidad de saber nada acerca de esos elementos.

Definición 1.3 . Se dice que un elemento $a \in G$, siendo G un grupo, tiene orden finito si $\exists k \in \mathbb{N}$ t.q $a^k = e$

Definición 1.4 . Dado un elemento de orden finitio, decimos que su orden es el menor entero positivo con el que se cumple $a^k = e$

1.1. Subgrupos

Sea G un conjunto y φ la operación con la que forma un grupo, vamos a ver cuando un subconjunto de G es un grupo de forma natural, esto es lo que denominaremos subgrupo.

Definición 1.5 . Diremos que un subconjunto no vacío S es un subgrupo si:

1. S es cerrado por la operación
2. e $\in$S

3. s ∈S⇒ s^{-1} ∈S.

Teorema 1.6. *Dados S_1, S_2 subgrupos de G ⇒ $S_1 \cap S_2$ es un subgrupo de G.*

Este teorema también puede aplicarse con una intersección numerable de grupos.

Definición 1.7 . Fijado un elemento g ∈G, definimos el grupo generado por g como: $< g >$={..., g^{-2}, g^{-1}, e, g, g^2,...}. Este grupo es un subgrupo de G

Teorema 1.8. *Si H es un subgrupo de G y g∈H ⇒ $< g >$⊂H.*

A partir de un conjunto C=$\{g_1, g_2, g_3 ... g_s\}$, contenido en G, vamos a buscar el menor subgrupo que lo contiene. $< g_1, g_2, g_3 ... g_s >$=$\cup_{k\in\mathbb{N}}$ $\{ a_1{}^* a_2{}^* a_3 ... a_k / (a_i \in C) \vee (a_i \in C^{-1})\}$. Es un subgrupo que contiene a todos los elementos de C.

Si H es un subgrupo que contiene a los elementos de C, el grupo generado por esos elementos se contiene en H.

Notación: H<G denota H subgrupo de G

Definición 1.9 . Dado H<G se dice que H es cícilico si existe g∈G t.q. H=$< g >$

Teorema 1.10. *Si G es un grupo finito y S⊂G es un subconjunto no vacío ⇒ S es un subgrupo ⇔ S es cerrado por la operación.*

Demostración. La implicación hacia la derecha es obvia por la propia definición de subgrupo. Para la implicación hacia la izquierda partimos de que S es cerrado y finito. Por tanto ∃ d ∈ S t.q. ord(d)=n y $< d > \subset S \Rightarrow d^n = e \in S$ y $d^{n-1} = d^{-1} \in S \Rightarrow$ S es un grupo □

Dentro de los grupos podríamos realizar una claisficación según fueran finitos o infinitos, por ejemplo. No obstante, nos resultará más interesante la clasificación de grupos según sean abelianos o no.

Definición 1.11 . Un grupo es abeliano si cumple la propiedad conmutativa.

Ejemplo $(\mathbb{Z}, +)$; $(\mathbb{Z}/n\mathbb{Z}, +)$ y $< s, g^2 >=\{1, g^2, s, sg^2\}$ son abelianos

Lema 1.12. *Todo subgrupo cíclico de un grupo G es abeliano. Por tanto un grupo no abeliano no puede ser cíclico.*

Ejemplo Dado $D_4 = \{id, g, g^2, g^3, s, sg, sg^2, sg^3\}$, (Recordemos que era el conjunto de aplicaciones que mantenían un cuadrado invariante), vamos a ver los grupos cíclicos contenidos en él. $< 1 >= 1$, $< g >=\{1, g, g^2, g^3\}$, $< g^2 >=\{1, g^2\}$, $< g^3 >= \{1, g, g^3\}$, $< s >=\{1, s\}$, $< sg >=\{1, sg\}$, $< sg^2 >=\{1, sg^2\}$, $< sg >=\{1, sg^3\}$.

Además podemos destacar el caso de $(\mathbb{Z}, +)$, un grupo cíclico para el cual, todo subgrupo es también cíclico. Esto se demuestra de forma general considerando que un grupo no cíclico estaría generado por varios elementos. En este caso, el máximo común divisor de estos número sería generador del grupo. Por tanto, el grupo sería cíclico.

De forma más estricta podemos decir que dado un subgrupo H$< \mathbb{Z}$ podrá ser H$=\{0\}$ ó H$\neq \{0\}$. En el primer caso, H ya sería cíclico. En el segundo caso, tenemos que $\exists$ d $\in$ H t.q. d$\neq$0. Lo que implica que $< d > \subset H$.

La duda sería si es cierto o no H$\subset <$ d $>$. Sea h $\in$H $\Rightarrow$ h=qd+r. Puesto que tanto h como d pertenecen a H, tenemos que r pertenece a H tambien. Esto implica que r puede expresarse r=dp. Lo que conlleva h=qd+pd=(q+p)d. Por tanto h $\in < d >$

Teorema 1.13. *En un grupo finito G todo elemento tiene orden finito. Además si g$\in$G tiene ord(g)=k $\Rightarrow$ $< g >$ tiene k elementos.*

Definición 1.14 . Un retículo de subgrupos es aquel retículo (estructura algebraica parcialmente ordenada) formado por subgrupos de un determinado grupo con una relación de contención. En este retículo, la unión de dos subgrupos es el subconjunto generado por su conexión.

Ejemplo Tomamos una vez más el grupo $D_4 = \{1, g, g^2, g^3, s, sg, sg^2, sg^3\}$. Aquí obtenemos el retículo:

Teorema 1.15 (Teorema de Lagrange). *Si G es un grupo finito y H un subgrupo de G, entonces el número de elementos de H divide el número de elementos de G.*

Lema 1.16. *Sea $\varphi : G \to G$, son equivalentes:*

1. *φ es inyectiva.*

2. φ *es biyectiva.*

3. φ *es sobreyectiva.*

La demostración de este teorema es totalmente trivial. Con apoyarnos en que el conjunto G es finito, puede observarse que una de esas propiedades implica directamente las demas.

Lema 1.17. *Si* φ *es un biyección y A,B son subconjuntos de G:*

1. *card(A)=card(*$\varphi(A)$*)*

2. *A=B* $\Leftrightarrow \varphi(A) = \varphi(B)$

3. $\varphi(A \cap B) = \varphi(A) \cap \varphi(B)$

Lema 1.18. *Sea G un grupo finito y g* $\in$*G.* $\varphi_g(x) = g * x$*. Además, por la propiedad cancelativa, podemos ver que* φ_g *es inyectiva. Además, por ser G finito, sabemos que* φ_g *es biyectiva.*

También podemos definir φ_g=$\{g * h \ / \ h \in H\}$

Lema 1.19. $H < G \Rightarrow$ *H es subconjunto de G.*

Notación: gH=$\varphi_g(H)$

Corolario 1.20. *Extraemos las siguientes conclusiones:*

1. *g*$\in$ *gH*

2. *card(H)=card(gH)*

3. *H=gH* $\Leftrightarrow$ *g* $\in$*H*

Demostración.

1. e $\in$ H. Por tanto g*e$\in$gH. g*e=g$\in$ gH

2. Se puede ver apoyándonos en los lemas anteriores puesto que H es finito.

3. $\Rightarrow$: e $\in$H $\Rightarrow$ e=gh con h $\in$ H $\Rightarrow$ h=g^{-1} $\in$H $\Rightarrow$ g $\in$H.
   $\Leftarrow$: g $\in$H $\Rightarrow$ g^{-1} $\in$H y todo elemento h $\in$H cumple h=$g(g^{-1}h)$ $\in$H.

□

Proposición 1.21. *Dados* g_1,g_2 $\in$*G y* $H < G \Rightarrow g_1H = g_2H \vee g_1H \cap g_2H = \varnothing$

Demostración. $g_1H \cap g_2H \neq \varnothing \Leftrightarrow \exists h_1, h_2$ t.q. $g_1h_1 = g_2h_2 \Rightarrow h_1 = g_1^{-1}g_2h_2 \Rightarrow h_2^{-1}h_1 = g_1^{-1}g_2$ $\in$H $\Leftrightarrow g_1^{-1}g_2H = H \Rightarrow g_2H = g_1H$ □

Ejemplo Tomando el famoso grupo D_4, podemos obtener H=$\{1, g, g^2, g^3\}$; sH=$\{s, sg, sg^2, sg^3\}$

1.2. Particiones

Definición 1.22 **Relación de equivalencia**. Fijado un conjunto G$\neq \varnothing$. Una relación R en G es de equivalencia si:

1. $\forall x \in G$ xRx
2. $\forall x, y \in G$ xRy $\Leftrightarrow$ yRx
3. $\forall x, y, z \in G$ xRy $\wedge$ yRz $\Rightarrow$ xRz

Definición 1.23 **Partición**. Familia de subconjuntos disjuntos dos a dos tales que su unión constituye el total.

Una partición define una relación de equivalencia y viceversa. Si R es una relación de equivalencia en un grupo G, definimos una partición en la que los subconjuntos son de la forma: $S_x = \{y \in G \nearrow xRy\}$

> *Demostración.* [Volvamos a demostrar la proposición 1.22]
> Definimos una relación de equivalencia R en G a partir del grupo H. $g_1 R g_2 \Leftrightarrow g_1^{-1} g_2 \in H$ y comprobamos que, efectivamente, esta relación es de equivalencia. Tenemos $S_e = H$. Así S_g o ya cubre junto con H todo G, o cojo otro g' y repito el proceso con $S_{g'}$. Así formare una serie de grupos de la forma S_x disjuntos dos a dos y cuya unión me da G.
> De esta forma podemos ver que card(G)=card(H)*s □

Corolario 1.24 (Teorema de Lagrange). *Dado g $\in$ G, siendo G un grupo finito $\Rightarrow$ ord(g) divide a |G| (cardinal de G). Así, suponiendo |G|=p primo, los únicos subrgupos que tiene G son los triviales:* $< 1 >, G$

Teorema 1.25. *Si |G|=p primo $\Rightarrow$ G es cíclico. Además, si |G|=n, $\forall$g ord(g) divide a n $\Rightarrow g^n = e$*

Ejemplo Con ayuda de este teorema puede demostrarse el pequeño teorema de Fermat. Definimos $\mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}..., \bar{p-1}\}$. Si tomamos el grupo de las unidades de $\mathbb{Z}/p\mathbb{Z}$ tenemos $\{\bar{1}, \bar{2}, ...\bar{p-1}\} \Rightarrow \bar{a} \in \mathbb{Z}/p\mathbb{Z} \wedge \bar{a} \neq 0 \Rightarrow a^{p-1} = \bar{1}$.

Teorema 1.26. *Si |G|=p^2 con p primo $\Rightarrow \exists g \in G \nearrow ord(g) = p$*

Demostración. Tomamos g $\in G \wedge g \neq e \Rightarrow ord(g) = p$ ó $ord(g) = p^2$. En el primer caso ya lo tenemos, vamos a por el segundo. ord(g)=$p^2 \Rightarrow ord(g^p) = p$ □

Ejemplo Por todo lo explicado anteriormente, si tomamos el anillo de polinomios $\mathbb{Z}/p\mathbb{Z}[x]$, tenemos $X^{p-1} - \bar{1} = \prod_{\bar{a} \in \mathbb{Z}/p\mathbb{Z} \wedge \bar{a} \neq 0}(x - \bar{a})$

Teorema 1.27 (Teorema de Lagrange Bis). *Dados* $H < G \; \exists a_1, ..., a_r \in G \; / \;$ *G=*$a_1H \cup a_2H.... \cup a_rH \wedge a_iH \cup_j H = \varnothing \forall i, j$. *Es decir, |G|=r|H|*

Definimos ahora otra relación a partir de H<G: $cR'd \Leftrightarrow cd^{-1} \in H$. La comprobación de que esto es una relación la omitiremos por ser trivial. En esta partción, el conjunto de elementos relacionados con d es: Hd=$\{hd / h \in H\}$

Definición 1.28 . Decimos que $H < G$ es un subgrupo normal si aH=Ha $\forall$a. Por tanto, si G es un grupo abeliano, H también lo será y cualquier subgrupo será normal. Un subgrupo normal se expresa como $H \lhd G$

Ejemplo Tomamos G=$\mathbb{Z}$ y H=$4\mathbb{Z}$. El subgrupo de los elementos que son equivalentes a n es nH=$\{n + 4k \; / \; k \in \mathbb{Z}\}$. En este caso tenemos 4 subgrupos según esta condición: $\bar{0}, \bar{1}, \bar{2}, \bar{3}$

Si $H \lhd G$ podemos definir una estructura de grupo en el subconjunto de clases. Dados g_1H y g_2H podemos formar el conjunto $\{h_1 * h_2 \; / \; h_1 \in g_1H \wedge h_2 \in g_2H\}$. Si operamos $g_1H * g_2H = (g_1 * g_2)H$ que es otra clase. Por tanto el grupo de clases es cerrado. El neutro sería la caja H puesto que gHH=gH para cualquier g que escojamos. Además el inverso de gH es $g^{-1}H$. Por último, vemos que $(g_1H * g_2H) * g_3H = g_1H * Hg_2 * g_3H = g_1H * Hg_3 * g_2H$, por ser G asociativo. Queda probado pues, que el conjunto de las clases de equivalencia, forma un grupo.

Teorema 1.29. *Si definimos [G:H]=nº de cajas=índice, tenemos: H<G* $\wedge [G : H] = 2 \Rightarrow H \lhd G$.

Demostración. Por un lado tenemos que g$\notin$H $\Rightarrow$ gH= H^c. Por otro lado, si tomamos la otra relación de equivalencia, a partir de g$\notin$H obtenemos Hg=H^c. Uniendo estos dos ejemplos, donde mantenemos H como una mitad en ambos, tenemos Hg=gH. Por tanto H es un subgrupo normal □