Lectura 9: Elementos de la teoría de grupos

9.1. Subgrupos

Una de las posibilidades en cualquier estructura algebraica, es que el conjunto base contenga subconjuntos que cumplen con las misma propiedades. Hemos visto por ejemplo, que el subconjunto $\mathrm{O}_2(\mathbb{R})$ del grupo $\mathrm{E}(\mathbb{R}^2)$ es también un grupo, comparten la identidad y los inversos y esto no es un caso aislado, es una instancia de un concepto más general.

Definición 9.1. Sea G un grupo. Un subconjunto $H \subset G$, se dice *un subgrupo* si

1. $e \in H$.
2. H es cerrado bajo $*$.
3. Si x en un elemento de H, entonces x^{-1} también lo es.

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:

- El subconjunto $\{e\}$ de un grupo G, es un subgrupo, al cual se le denomina *el subgrupo trivial*.
- Como se discutió, el grupo ortogonal $\mathrm{O}_2(\mathbb{R})$ es un subgrupo del grupo euclidiano $\mathrm{E}(\mathbb{R}^2)$.
- 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.
- El grupo de las raíces de la unidad, Γ_m, es un subgrupo del grupo circular S^1.
- Si $F \subset E$, entonces $\mathcal{P}(F) \leq \mathcal{P}(E)$, considerando a $\mathcal{P}(E)$ junto a la diferencia simétrica.
- 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.
- El conjunto $\mathrm{SO}_2(\mathbb{R})$ de rotaciones sobre el origen, es un subgrupo del grupo ortogonal $\mathrm{O}_2(\mathbb{R})$. Al grupo $\mathrm{SO}_2(\mathbb{R}^2)$ 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.

Proposición 9.1. *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 $x - y \in H$. Esto es una sugerencia interesante, pues retomando el subgrupo $H_m \leq \mathbb{Z}$, tenemos $x \equiv y \mod m$ si y sólo si $x - y \in H_m$. Este enunciado sirve para definir una congruencia usando un subgrupo y aunque digno de mención, no tendremos tiempo de explorar el tema.

9.2. Grupos cíclicos

En nuestra discusión de las raíces m-ésimas de la unidad, se introdujo un concepto que nos permitió distinguir algunas propiedades que presentaba dicho conjunto: el orden. El orden en las raíces de la unidad es en realidad un caso particular de un concepto en la teoría de grupos.

Definición 9.2. Sea G un grupo y sea a un elemento cualquiera de éste. *El orden de a* es el menor entero positivo m de forma que $a^m = e$. Si dicho entero existe, decimos que *a tiene orden finito* y escribimos $\text{ord}(a) = m$, en caso contrario decimos que *a tiene orden infinito*.

En el caso del grupo de las raíces m-ésimas, la definición anterior coincide con la que se provee. La ventaja, por supuesto, es tener ahora un concepto que aplica a cualquier objeto que pertenezca a un grupo. Podemos considerar algunos ejemplos sencillos.

- En el grupo euclidiano del plano, la rotación $R_{2\pi/m}$ tiene orden m, mientras que las reflexiones tiene todas orden 2. Las translaciones, por otro lado, tienen orden infinito.
- Una permutación α sobre n elementos se dice una transposición si existe un par de enteros i y j de forma que $\alpha(i) = j$ y $\alpha(j) = i$, mientras para todo entero k distinto de i y j, $\alpha(k) = k$. Toda transposición tiene orden 2 en el grupo simétrico sobre n elementos.
- En general, una permutación α se dice es un m-ciclo, si existen enteros $i_1, i_2, \ldots, i_m$, todos distintos, tales que $\alpha(i_1) = i_2, \ldots, \alpha(i_{m-1}) = i_m$ y $\alpha(i_m) = i_1$; y si $i \neq i_k$ para todo k, entonces $\alpha(i) = i$. Un m-ciclo tiene orden m.

El objetivo de introducir el concepto de orden en las raíces m-ésimas, era distinguir algunos elementos que parecían contener más información del conjunto y este vuelve a ser el caso.

Definición 9.3. Sea G un grupo cualquiera y sea a un elemento de dicho grupo. Definimos *el subgrupo cíclico generado por a* como el subgrupo

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}.$$

Si además $G = \langle a \rangle$, decimos que G es *un grupo cíclico* y en ese caso a se dice *un generador*.

Aunque no hemos usado esa terminología para describirlos, ya conocemos varios grupos que resultan cíclicos:

- El grupo aditivo de los enteros, es cíclico y tiene como generador al entero 1, en símbolos $\mathbb{Z} = \langle 1 \rangle$. En particular este es un grupo cíclico de orden infinito.
- El grupo aditivo de los enteros módulo m, también es cíclico con generador $[1]_m$. En símbolos $\mathbb{Z}_m = \langle [1]_m \rangle$. Los enteros módulo m, constituyen un ejemplo de grupo cíclico de orden finito.
- Según el teorema 7.3, cualquier raíz m-ésima se puede escribir como

  $$\cos(2\pi k/m) + i \operatorname{sen}(2\pi k/m).$$

  Por la identidad de De Moivre, esto implica que la raíz primitiva

  $$\zeta = \cos(2\pi/m) + i \operatorname{sen}(2\pi/m)$$

  debe ser un generador del grupo formado por las raíces m-ésimas. En símbolos: $\Gamma_m = \langle \zeta \rangle$.
- En contraste, el grupo de unidades módulo 8, $\mathbb{Z}_8^* = \{[1]_8, [3]_8, [5]_8, [7]_8\}$, tiene la peculiaridad que sus elementos son también sus inversos. Esto implica que si $a \in \mathbb{Z}_8^*$, entonces

  $$a^m = \begin{cases} a & \text{si } m \text{ es impar} \\ [1]_8 & \text{si } m \text{ es par} \end{cases}$$

  mostrando que ningún elemento del grupo lo genera o en otras palabras, no es cíclico.

Lema 9.2. *Sea G un grupo cualquiera y sea a un elemento de orden m. Entonces, $a^n = e$ implica $m \mid n$.*

Demostración. Por el teorema de la división expresamos $n = qm + r$ con $0 \leq r < m$. En ese caso,

$$e = a^n = a^{qm+r} = a^{qm}a^r = a^r$$

pero si $r > 0$, entonces $r < \operatorname{ord}(a)$ lo cual es contradictorio por tanto $r = 0$ o en otras palabras $m \mid n$, como buscábamos. ∎

Teorema 9.3. *Sea G un grupo cíclico de orden m y sea a un generador de G. Entonces, a^k es un generador si y sólo si $(m, k) = 1$.*

Demostración. Supongamos que a^k es un generador, en ese caso $a \in \langle a^k \rangle$, entonces existe un entero s de forma que $a = a^{ks}$ o en otras palabras, $a^{ks-1} = e$. Ahora, según el lema 9.2, debemos tener que $m \mid (ks - 1)$, lo que implica que existe un entero t tal que $-mt + ks = 1$, implicando con esto que 1 es una combinación lineal de m y k. Como el máximo común divisor es la mínima combinación lineal positiva, entonces $(m, k) = 1$.

Supongamos ahora que $(m,k) = 1$. Por la identidad de Bézout, expresamos $1 = mt + ks$ y en ese caso

$$a = a^{mt+ks} = a^{mt}a^{ks} = a^{ks}$$

y en consecuencia $a \in \langle a^k \rangle$. Por hipótesis $G = \langle a \rangle$ obteniendo de esto $G \subset \langle a^k \rangle$ por lo que $G = \langle a^k \rangle$. Esto prueba el resultado. ■

Es interesante notar que el lema 9.2 contempla un caso general de la proposición 7.10; no sólo eso, si uno compara además las demostraciones, se debe notar que, en esencia, se usa el mismo argumento. No debe ser sorpresa que teorema 9.3 sea una generalización del teorema 7.11.

9.3. Homomorfismos

Como en el caso de anillos, las funciones que nos permiten comparar dos grupos resultan de nuevo los homomorfismos, aunque estos son de una clase especial y no deben confundirse con los que se introducen en la teoría de anillos.

Definición 9.4. Sean $(G, *_G)$ y $(H, *_H)$ grupos cualquiera. Una función $f\colon G \to H$ se dice *un homomorfismo de grupos* si

$$f(e_G) = e_H$$

y para cualesquiera elementos x y y de G,

$$f(x *_G y) = f(x) *_H f(y).$$

Como en el caso de anillos, expresar qué operación binaria se realiza, es demasiado quisquilloso. Una función definida de manera correcta, nos provee de la información suficiente para no caer en ambigüedades. Por eso se prefiere escribir la propiedad que define al homomorfismo omitiendo cualquier referencia a las operaciones binarias involucradas. Esto nos permite simplificar las propiedades de homomorfismo de grupo como

$$f(e) = e$$

y

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

Consideremos ahora algunos ejemplos.

- 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, determinada por $f(x) = e$.
- 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 $R^* \to S^*$ que es un homomorfismo entre los grupos de unidades.
- Sea Γ_m el grupo de las raíces m-ésimas de la unidad y tomemos $\mathbb{Z}_m$ como su grupo aditivo. Como cada raíz se puede expresar como ζ^k, para alguna raíz primitiva ζ y algún $0 \leq k < m$, la función $f\colon \Gamma_m \to \mathbb{Z}_m$ con regla de correspondencia $f(\zeta^k) = [k]_m$, es un homomorfismo.

Definición 9.5. 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. La prueba es un ejercicio (9.5).

Proposición 9.4. *Sea $f\colon G \to H$ un homomorfismo de grupos. Entonces,*

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

Por último, los homomorfimos se clasifican muy parecido a los anillos. De hecho, la definición de isomorfismo e inmersión son esencialmente las mismas.

Definición 9.6. Sea $f\colon G \to H$ un homomorfismo entre grupos. Decimos que:

- f es *una inmersión 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 una inmersión de grupos de G en H y se dice que G y H *son isomorfos* si existe un isomorfismo entre ellos.

Un isomorfismo de G en G, se dice *un automorfismo*. Por ejemplo, cada elemento a del grupo, induce un automorfismo $f_a\colon G \to G$ definido por

$$f_a(x) = axa^{-1}.$$

Quizá no sorprenda que los automorfismos forman un grupo bajo la composición, el cual se denota por $\mathrm{Aut}(G)$. Es importante notar que éste resulta un subgrupo del grupo de permutaciones de G. Además, la asignación $a \mapsto f_a$ resulta un homomorfismo de G en $\mathrm{Aut}(G)$.

9.4. Grupos de simetría

Vamos ahora a introducir un par de ejemplos en geometría que ilustran algunos conceptos de la teoría grupos. Para construirlos, usaremos una vez más el concepto de isometrías en el plano. Para introducir a estos grupos usaremos primero un caso particular.

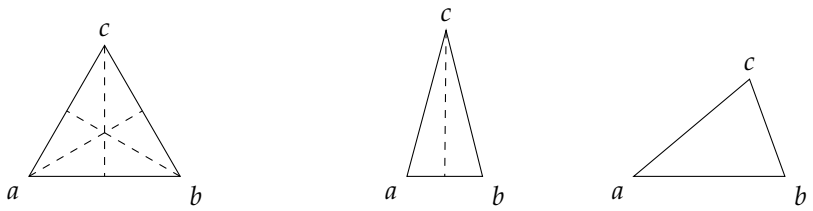

Figura 1: Algunas simetrías en los triangulos.

Sea $\triangle$ un triángulo con centro en el origen y vértices a, b y c y tomemos φ como una isometría. No es difícil observar que $\varphi(a)$, $\varphi(b)$ y $\varphi(c)$ son también los vértices de un triangulo y si asumimos además que $\varphi(\triangle) = \triangle$, entonces lo que único que realiza φ es permutar los vértices. Si consideremos el triangulo en cuestión como isósceles (donde la arista ac tiene la misma longitud que la arista bc), entonces la recta L que pasa por el origen y el vértice c, define la reflexión ρ_L que satisface $\rho_L(\triangle) = \triangle$; en particular, ρ_L transpone los vértices b y c. Si por otro lado, $\triangle$ es equilátero podemos tomar las rectas L_a, L_b y L_c de forma que L_i pase por el origen y el vértice i, y definir las reflexiones ρ_{L_i} que satisfacen todas $\rho_{L_i}(\triangle) = \triangle$; en particular transponen los vértices fuera de la recta L_i. Además, las rotaciones de $2\pi/3$ y $4\pi/3$ tienen el mismo efecto (sus imágenes son de nueva cuenta $\triangle$) y de igual forma, sólo permutan los vértices en sentido contrario a las manecillas del reloj. Podemos observar que cualquier isometría, al ser una permutación de los vértices del triángulo, debe ser una de las descritas anteriormente o la identidad. Esto se ilustra en la figura 1.

Definición 9.7. Para cualquier subconjunto $\Omega \subset \mathbb{R}^2$, definimos *el grupo de simetría de* Ω como el conjunto

$$\Sigma(\Omega) = \left\{ \varphi \in \mathrm{E}(\mathbb{R}^2) \mid \varphi(\Omega) = \Omega \right\},$$

junto a la composición como operación. Los elementos de $\Sigma(\Omega)$ se denominan *simetrías de* Ω.

Los ejemplos más interesantes resultan de tomar grupos de simetría de un polígono regular.

- Un 3-gono regular π_3, es un triangulo equilatero. Hemos discutido ya que el orden del grupo de simetrías de π_3 es 6. Este se puede observar en la figura 1.
- Supongamos π_4 como un cuadrado con centro en el origen y vértices v_0, v_1, v_2 y v_3. Es sencillo ver que una simetría φ de π_4 permuta los vértices y por tanto deben existir cuando más $4! = 24$ simetrías del cuadrado, sin embargo, no toda permutación deriva en una simetría. En efecto, si v_i y v_j son adyacentes, entonces $\|v_i - v_j\| = L$ pero $\|v_0 - v_2\| = \sqrt{2}L$ por lo que φ preserva adyacencia al preservar la distancia. Hay exactamente 8 isometrías con esta característica[1]: La identidad, tres rotaciones de $\pi/2$, π y $3\pi/2$ grados y cuatro reflexiones indicadas dos por los ejes y las restantes por las rectas que unen a v_0 y v_2 por un lado, y a v_1 y v_3 por el otro.

Teorema 9.5. *Sea π_m un polígono regular con centro en el origen. Entonces, el conjunto*

$$\Sigma_S(\pi_m) = \{ \varphi \in \mathrm{SO}(2) \mid \varphi(\pi_m) = \pi_m \},$$

es un subgrupo del grupo de simetría $\Sigma(\pi_m)$.

Demostración. Es evidente que el conjunto $\Sigma_S(\pi_m)$ es no vacío al pertenecer la identidad a éste. Ahora, supongamos que R_θ y R_η son rotaciones del conjunto $\Sigma_S(\pi_m)$. Sabemos que que $R_{-\eta}$ es la inversa de R_η y sabemos que

$$R_\theta \circ R_{-\eta} = R_{\theta-\eta},$$

permitiéndonos concluir que la función que resulta de la composición expresada es una rotación y en consecuencia $R_\theta \circ R_{-\eta} \in \Sigma_S(\pi_m)$. Según la proposición 9.1, lo anterior es suficiente para afirmar que $\Sigma_S(\pi_m)$ es un subgrupo como buscábamos. ■

[1] Lamentablemente la prueba está más allá de los alcances de nuestra discusión.

Corolario 9.6. *El grupo $\Sigma_S(\pi_m)$ es cíclico de orden m.*

Demostración. Sea $V = \{v_0, \ldots, v_{m-1}\}$ el conjunto de vértices del polígono π_m y sea $\rho = R_{2\pi/k}$ la rotación de $2\pi/k$ grados sobre el origen. Entonces,

$$\rho(v_i) = \begin{cases} v_{i+1} & \text{si } 0 \leq i < n-1 \\ v_0 & \text{si } i = n-1 \end{cases}.$$

Es inmediato que el orden de ρ es m. Además, con la definición de subgrupo cíclico, $\langle \rho \rangle \subset \Sigma_S(\pi_m)$, por lo que bastará probar la otra contención para alcanzar el resultado enunciado. Supongamos entonces que R_θ es una rotación en el conjunto $\Sigma_S(\pi_m)$, en ese caso de lo que podemos concluir $R_\theta(V) = V$, en particular $R_\theta(v_0) = v_k$ para algún $0 \leq k < n$. Sabemos que un polígono regular, en ángulo entre los vértices v_0 y v_k es $2\pi k/m$ por lo que debemos concluir $\theta = 2\pi k/m$. En ese caso, $R_\theta = \rho^k$ y en consecuencia $R_\theta \in \langle \rho \rangle$, lo que nos lleva a tener $\Sigma_S(\pi_m) \subset \langle \rho \rangle$. En conclusión $\Sigma_S(\pi_m) = \langle \rho \rangle$ y como ρ tiene orden m entonces $\Sigma_S(\pi_m)$ resulta un grupo cíclico de orden m. ■

Por último es interesante comentar que de acuerdo al corolario anterior podemos escribir cualquier rotación como ρ^k y sabemos también que cualquier raíz de la unidad se puede escribir como ζ^k para una raíz primitiva ζ. Es natural pensar que toda raíz define una rotación, lo cual matemáticamente se expresa asignando

$$\zeta^k \mapsto \rho^k.$$

No es difícil probar que esta asignación es un isomorfismo y por tanto el grupo $\Sigma_S(\pi_m)$ es isomorfo al grupo Γ_m. Desde el punto de vista algebraico, estos dos objetos son lo mismo por este motivo.

Ejercicios

Ejercicio 9.1. Muestra que una raíz m-ésima es primitiva si y sólo si es un generador del grupo Γ_m.

Ejercicio 9.2. Para un grupo cualquiera G y un elemento a en éste, muestra que el siguiente conjunto es en verdad un subgrupo de G como afirma la definición 9.3:

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}.$$

Ejercicio 9.3. Sea $E = \{\alpha, \beta\}$ un conjunto con dos elementos. Demuestra que el grupo formado por el conjunto $\mathcal{P}(E)$ y la diferencia simétrica es isomorfo al grupo de unidades módulo 8.

Ejercicio 9.4. Sea $\mathbb{Z}_m^+$ el grupo aditivo de $\mathbb{Z}_m$ y sea $\zeta = \cos(2\pi/m) + i\,\mathrm{sen}(2\pi/m)$. Sabemos que a cada raíz m-ésima de la unidad se le puede expresar como ζ^k, para algún entero $0 \leq k < m$. Si $f\colon \Gamma_m \to \mathbb{Z}_m^+$ es una función definida como $f(\zeta^k) = [k]_m$, demuestra lo siguiente:

1. f es un homomorfismo.
2. f es biyectiva.
3. Γ_m y $\mathbb{Z}_m^+$ son isomorfos.

Ejercicio 9.5. Prueba la proposición 9.4.

Ejercicio 9.6. Demuestra que el conjunto de automorfismos es un grupo.

Ejercicio 9.7. Sea $f\colon G \to H$ un homomorfismo de grupos. Demuestra que para todo elemento a del grupo, se cumple:

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

Sugerencia: Es muy parecido al caso de anillos.

Ejercicio 9.8. Sean G y H grupos de forma que G sea cíclico. Si G y H son isomorfos, demuestra que H es cíclico.

Ejercicio 9.9. 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.

Ejercicio 9.10. Sea π_4 un cuadrado. Muestra que el grupo de simetría $\Sigma(\pi_4)$, se puede sumergir en el grupo simétrico S_4.

Ejercicio 9.11. Sea π_n un polígono regular de n lados. Muestra que el grupo de simetría $\Sigma(\pi_n)$ se puede sumergir en el grupo simétrico S_n.

Ejercicio 9.12. Sea v un punto cualquiera en el plano y sea Ω un subconjunto de $\mathbb{R}^2$. Si

$$\Omega_v = \{x + v \mid x \in \Omega\}\,;$$

en otras palabras: Ω_v es la traslación del conjunto Ω al punto v, demuestra que los grupos de simetría $\Sigma(\Omega)$ y $\Sigma(\Omega_v)$ son isomorfos.

Ejercicio 9.13. Sea φ una isometría del plano y sea sea Ω un subconjunto de $\mathbb{R}^2$. Demuestra que los grupos de simetría $\Sigma(\Omega)$ y $\Sigma\left(\varphi(\Omega)\right)$ son isomorfos.

Referencias

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

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

Las notas anteriores juegan algunas veces a ser un simple resumen de lo que otros autores han presentado, otras menos a reinterpretarlo y en una cantidad ínfima de ocasiones intentan pobremente aumentalo. El único objectivo real al que sirven, es preparar el curso de Álgebra Superior II impartido en la carrera de Actuaría de la FES Acatlán. Su versión es, en consecuencia, susceptible a errores gramaticales, imprecisiones técnicas y cambios constantes.