1. El grupo simétrico, el grupo alternante y grupos simples

En lo que sigue nos proponemos estudiar algunas propiedades de los grupos simétricos. Por simplicidad trataremos de trabajar siempre con la siguiente presentación: el *grupo simétrico en n elementos* es

$$S_n = \{\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} : \sigma \text{ es biyectiva}\},$$

en donde se entiende que la operación de grupo es la composición de funciones. La notación que usamos en clase para las permutaciones identifica un elemento $\sigma \in S_n$ con la n-upla $(\sigma(1), \sigma(2), \ldots, \sigma(n))$. Así, por ejemplo si $\sigma, \eta \in S_4$ están dadas por $\sigma = (1, 2, 4, 3)$ y $\eta = (2, 4, 1, 3)$ se tiene que

$$\sigma\eta = (1, 2, 4, 3)(2, 4, 1, 3) = (2, 3, 1, 4).$$

Las permutaciones más sencillas son las llamadas *trasposiciones* y son precisamente las permutaciones que intercambian dos elementos dejando los demás fijos. La notación que usamos para la trasposición que intercambia i con j es $\tau_{i,j}$. Hacemos dos observaciones con respecto a esta notación. En primer lugar, está implícito que $i \neq j$, ya que el elemento $\tau_{i,i}$ correspondería a la permutación identidad $e = (1, 2, \ldots, n)$, la cual no es una trasposición (no intercambia nada de lugar). En segundo lugar, mencionemos que hay una cierta ambigüedad en la notación, pues $\tau_{i,j}$ tiene sentido en cualquier S_n tal que $i, j \leq n$. De todas formas preferimos dejarlo así en lugar de recargar la notación y tratar de usar el contexto para decidir qué es lo que tiene sentido.

Un primer resultado interesante dice que las trasposiciones son los elementos básicos con los cual se construyen todas las permutaciones.

Proposición 1. *Toda permutación es producto de trasposiciones. Es decir, para cada $\sigma \in S_n$ existen trasposiciones $\tau_1, \tau_2, \ldots, \tau_k \in S_n$ tales que $\sigma = \tau_1\tau_2 \cdots \tau_k$.*

La demostración de este resultado debería ser evidente: siempre se pueden reordenar los números $1, 2, \ldots, n$ en $\sigma(1), \sigma(2), \ldots, \sigma(n)$ intercambiándolos de a pares. Observemos sin embargo que no hay una única manera de hacerlo. Por ejemplo, si $i \neq j$,

$$e = \tau_{i,j}\tau_{i,j} = \tau_{i,j}\tau_{i,j}\tau_{i,j}\tau_{i,j} = \tau_{i,j}\tau_{i,j}\tau_{i,j}\tau_{i,j}\tau_{i,j}\tau_{i,j} = \ldots$$

(Por cierto, la inversa de una trasposición es ella misma.)

Ejercicio 1. Expresar como producto de trasposiciones las siguientes permutaciones.

1. $(2, 3, 4, 1), (3, 1, 4, 2) \in S_4$.
2. $(5, 3, 4, 2, 1) \in S_5$.

Si bien la manera de descomponer una permutación en trasposiciones no es única, se tiene un resultado muy importante que dice que, fija una permutación σ, la cantidad de trasposiciones usadas en cualquier descomposición de σ tiene siempre la misma paridad.

Teorema 2. *Sean $\sigma \in S_n$ una permutación cualquiera y $\tau_1, \tau_2, \ldots, \tau_k, \mu_1, \mu_2, \ldots, \mu_\ell \in S_n$ trasposiciones tales que $\sigma = \tau_1\tau_2\cdots\tau_k = \mu_1\mu_2\cdots\mu_\ell$. Entonces $\ell - k$ es un número par. Como consecuencia, tiene sentido definir el* signo *de la permutación σ como $\operatorname{sg}\sigma = (-1)^k \in \{-1, 1\}$.*

Ejercicio 2. Demostrar el teorema anterior usando el siguiente argumento. Consideremos la función $F : S_n \to \{-1, 1\}$ dada por

$$F(\sigma) = \prod_{i<j} \frac{j-i}{\sigma(j) - \sigma(i)}.$$

1. Probar que F es un morfismo de grupos. Es decir, para todas $\sigma, \eta \in S_n$ se tiene $F(\sigma\eta) = F(\sigma)F(\eta)$ (esta es la parte más complicada).
2. Probar que si τ es una trasposición entonces $F(\sigma) = -1$.
3. Usar los apartados anteriores para dar una demostración del teorema.

Corolario 3. *Para toda $\sigma \in S_n$ se tiene que*

$$\operatorname{sg}\sigma = \prod_{i<j} \frac{j-i}{\sigma(j) - \sigma(i)}.$$

Siguiendo este enfoque se suele distinguir entre las permutaciones *pares* y las permutaciones *impares*, según tengan signo 1 o -1 respectivamente. Más aún, el conjunto de todas las permutaciones pares de S_n forma un subgrupo llamado el *grupo alternante*

$$A_n = \{\sigma \in S_n : \operatorname{sg}\sigma = 1\}.$$

Ejercicio 3. Ya vimos en un ejercicio anterior que $\operatorname{sg} : S_n \to \{\pm 1\}$ es un morfismo de grupos. Mostar que $\ker \operatorname{sg} = A_n$ y por lo tanto A_n es un subgrupo normal de S_n. (Comparar con el hecho de que todo subgrupo de índice 2 es normal.)

Los grupos alternantes son muy importantes porque forman una de las tres familias infinitas de grupos finitos simples.

Definición 1. Un grupo G se dice *simple* si no posee subgrupos normales propios. Es decir, si $H \lhd G$ entonces $H = \{e\}$ o $H = G$.

Ejercicio 4.

1. S_n es simple si y sólo si $n = 1$ o $n = 2$.
2. $\mathbb{Z}_n$ es simple si y sólo si n es primo.
3. A_4 no es simple.
4. A_5 es simple.

Los grupos simples tienen la propiedad destacadas de no poseer cocientes (no triviales), es decir no se pueden formar nuevos grupos (más pequeños) a partir de ellos. Mencionamos el siguiente resultado sin incluir su demostración (la cual no es difícil, pero es un poco larga y requiere muchas cuentas).

Teorema 4. *A_n es simple para todo $n \geq 5$.*

Comentario. Además de los grupos alternantes A_n con $n \geq 5$, y de los grupos cíclicos $\mathbb{Z}_p$ con p primo, la otra familia infinita de grupos finitos simples son los llamados grupos de tipo Lie, que pueden visualizarse como ciertos grupos de matrices donde los coeficientes se toman en cuerpos finitos. La clasificación de los grupos finitos simples es uno de los problemas más difíciles de la matemática moderna y fue resuelto hace no muchos años. Además de estas tres familias, existen otros 26 grupos finitos simples llamados *esporádicos*, los cuales son extremadamente difíciles de describir. El problema con estos grupos no es tanto su tamaño (son grandes, sí) sino que son muy difíciles de representar. Por ejemplo, el más grande de los grupos esporádicos es el llamado *monster group* M (todos tienen nombres graciosos), el cual tiene orden menor que el grupo alternante A_{100} de orden

$$|A_{100}| = \frac{100!}{2} > 4 \times 10^{157}.$$

Pero A_n tiene la ventaja de que puede visualizarse dentro del grupo de simetrías de un conjunto de 100 elementos, que es número muy chico comparado con 10^{157}. Sin embargo, el objeto más chico del cual M es un grupo de simetrías tiene aproximadamente 200,000 dimensiones. Es por eso que los grupos esporádicos son tan complicados, y en realidad, primero los se los imaginaron y luego probaron su existencia.

1.1. Ciclos

Otro tipo muy sencillo de permutaciones son las que ciclan entre ciertos elementos de la siguiente forma. Se eligen k elementos (de entre n dados) y se les asigna un orden (total), un k-ciclo asigna al primer elemento el último lugar y a los demás los pasa un lugar para adelante. Luego de aplicar k-veces el mismo k-ciclo se llega a la configuración inicial. Por ejemplo, toda trasposición es un 2-ciclo. Otro ejemplo sería el *shift*

$$\sigma = (2, 3, \ldots, n, 1) \in S_n$$

que es un n-ciclo. Más precisamente, decimos que $\sigma \in S_n$ es un *k-ciclo* (o simplemente un *ciclo*) si existen $i_1, \ldots, i_k \in \{1, 2, \ldots, n\}$ todos distintos tales que

$$\begin{cases} \sigma(i) = i, & i \notin \{i_1, \ldots, i_k\} \\ \sigma(i_1) = i_k, & \\ \sigma(i_j) = i_{j-1}, & j \in \{2, \ldots, k\} \end{cases}$$

Usaremos la notación $C_{i_1,\ldots,i_k}$ para denotar el ciclo recién definido.

Ejercicio 5. 1. Probar que $C_{i_1,\dots,i_k} = C_{i_2,\dots,i_k,i_1}$.

2. Escribir $C_{i_1,\dots,i_k}$ como producto de trasposiciones.

3. Probar que $C_{i_1,\dots,i_k}$ conmuta con $C_{j_1,\dots,j_\ell}$ si y sólo si $\{i_1,\dots,i_k\} \cap \{j_1,\dots,j_\ell\} = \varnothing$. Dos ciclos de esta forma se llaman *disjuntos*. Concluir que si σ, η son dos ciclos disjuntos en S_n entonces $|\sigma\eta| = \text{mcm}(|\sigma|, |\eta|)$.

4. Probar que si $\sigma \in S_4$ no tiene puntos fijos (i.e., $\sigma(i) \neq i$ para todo i) entonces σ es un 4-ciclo o el producto de dos trasposiciones disjuntas. Concluir que $|\sigma| \leq 4$ para toda $\sigma \in S_4$.

5. ¿Cuál es el máximo orden posible de un elemento en S_5, S_6, S_7?

2. Producto semidirecto

A continuación presentamos un método un poco más sofisticado para construir nuevos grupos a partir de grupos conocidos. Recordemos las construcciones que vimos hasta ahora.

Grupo cociente Si G es un grupo y $H \lhd G$ entonces G/H es un grupo tal que $G \to G/H$ es un epimorfismo de grupos. En algún sentido G/H es un grupo "más chico" que G, pero no necesariamente se lo puede visualizar dentro de G (como subgrupo).

Producto directo Si G y H son dos grupos, entonces $G \times H$ es un grupo definiendo las operaciones coordenada a coordenada: para todos $g_1, g_2 \in G$, $h_1, h_2 \in H$,

$$(g_1, h_1)(g_2, h_2) := (g_1 g_2, h_1 h_2).$$

Observar que los subgrupos $G \times \{e_H\}$, $\{e_G\} \times H$ de $G \times H$ son normales e isomorfos a G y H respectivamente. Es decir, el producto directo $G \times H$ es un grupo más grande que G y H que los contiene como subgrupos. Si bien los productos directos son muy importantes para tratar de entender la estructura general de los grupos, como construcción algebraica no son muy interesantes porque la estructura de grupo de $G \times H$ está completamente determinada por las estructuras de grupos de G y H (es decir, no aparece información nueva). Esto tiene que ver con la forma en la que G y H están incluidos en $G \times H$. Es decir,

$$\frac{G \times H}{G} \simeq H, \qquad \frac{G \times H}{H} \simeq G$$

El siguiente resultado nos da un criterio para decidir cuándo un grupo es el producto directo de dos subgrupos.

Proposición 5. *Sean K un grupo y G, H dos subgrupos de K tales que*

1. $G \lhd K$, $H \lhd K$,

2. $K = GH$,

3. $G \cap H = \{e\}$.

Entonces K *es isomorfo a* $G \times H$.

Ejercicio 6. 1. Demostrar la Proposición anterior usando el siguiente argumento. Recordemos que GH es el subgrupo de K generado por $G \cup H$, es decir, sus elementos son de la forma $k_1 k_2 \cdots k_m$ donde los k_i son elegidos en G o en H. Usando las condiciones de normalidad, verificar que si $g \in G$ y $h \in H$ entonces $gh = hg$. Luego, como $K = GH$ cualquier elemento $k \in K$ se puede escribir de forma única como $k = gh$ con $g \in G$, $h \in H$ (¿por qué?). Finalmente concluir que la asignación $k \mapsto (g, h)$ es un isomorfismo de grupos de K en $G \times H$.

2. Demostrar la siguiente generalización de la proposición anterior. Sean G un grupo y $G_1, \ldots, G_k$ subgrupos de G tales que

   a) $G_i \lhd G$ para todo i,

   b) $G = G_1 G_2 \cdots G_k$,

   c) $G_i \cap (G_1 \cdots G_{i-1} G_{i+1} \cdots G_k) = \{e\}$

   Entonces $G \simeq G_1 \times G_2 \times \cdots \times G_k$ (con el producto definido coordenada a coordenada).

3. Cuando G y H son grupos abelianos y los presentamos con la notación aditiva, el producto directo se llama *suma directa* y se denota $G \oplus H$. Probar que si m y n son coprimos, entonces $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \oplus \mathbb{Z}_n$.

Estudiemos la siguiente generalización del producto directo. Supongamos que K es un grupo y que G, K son dos subgrupos tales que $G \lhd K$, $K = GH$ y $G \cap H = \{e\}$. O sea, son casi las mismas hipótesis que en la Proposición 5 salvo que en este caso requerimos que solamente uno de los subgrupos sea normal. Observemos que, a diferencia del caso del producto directo, ahora no podemos asegurar que $gh = hg$ para todos $g \in G$, $h \in H$, pero sí podemos escribir $hg = hgh^{-1}h$ y como G es normal $hgh^{-1} \in G$. Luego para cada $g \in G$, $h \in H$ existe $g' \in G$ tal que $hg = g'h$. Usando que $K = GH$ tenemos que todo elemento $k \in K$ se escribe como $k = gh$ y está expresión es única pues $G \cap H = \{e\}$. En efecto, si $gh = g'h'$, sigue que $g^{-1}g' = h'h^{-1} \in G \cap H$, de donde se tiene que $g = g'$ y $h = h'$. Luego hay una biyección entre K y $G \times H$. Notar que esta correspondencia no es un isomorfismo de grupos si H no es normal. Analicemos un poco más cómo es el producto en G. Llamemos $\varphi_h : G \to G$ a la conjugación en G por el elemento $h \in H$, es decir, $\varphi_h(g) = hgh^{-1}$ que es la función que usamos antes para escribir

$$hg = \varphi_h(g)h.$$

Si ahora queremos calcular el producto entre $k_1, k_2 \in K$, podemos escribir $k_1 = g_1 h_1$, $k_2 = g_2 h_2$, con $g_1, g_2 \in G$, $h_1, h_2 \in H$ y tenemos que

$$k_1 k_2 = g_1 h_1 g_2 h_2 = g_1 \varphi_{h_1}(g_2) h_1 h_2.$$

Es decir, la componente según G de k_1k_2 es $g_1\varphi_{h_1}(g_2)$ y la componente según H es h_1h_2.

Todavía podemos decir un poco más. Observemos que para cada $h \in H$, φ_h es un *automorfismo* de G, es decir $\varphi_h : G \to G$ es un isomorfismo de grupos. Más aún, la asignación $\varphi : H \to \mathrm{Aut}(G)$ es un morfismo de grupos, o sea, $\varphi_{h_1h_2} = \varphi_{h_1} \circ \varphi_{h_2}$. En este caso se dice que K es el *producto semidirecto* de G con H y se lo suele denotar por $G \rtimes H$. Otras notaciones frecuentes son $G \rtimes_\varphi H$ y $G \times_\varphi H$. Regla mnemotécnica: el símbolo $\rtimes$ en $G \rtimes H$ nos indica que G es normal en K (o sea, $G \lhd K$). También sería válida la construccuón $H \ltimes G$ (¿qué automorfismos se usarían en este caso?).

Antes de seguir, precisemos un poco las definiciones anteriores.

Ejercicio 7. Continuamos con las hipótesis anteriores.

1. Probar que
$$\mathrm{Aut}(G) = \{f : G \to G : f \text{ es isomorfismo de grupos}\}$$
es un grupo con la composición.

2. Probar que para todo $h \in H$, $\varphi_h \in \mathrm{Aut}(G)$ y que $\varphi : H \to \mathrm{Aut}(G)$ es un morfismo de grupos

3. Probar que si $g_0 \in G$ entonces $g \mapsto g_0 g g_0^{-1}$ es un automorfismo de G. Estos automorfismos se llaman *automorfismos interiores*. Notar que φ_h definido como antes no necesariamente es un automorfismo interior, porque en principio estamos conjugando por el elemento $h \in H$ que no está en G.

4. Calcular $\mathrm{Aut}(G)$ para $G = \mathbb{Z}, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_5, \mathbb{Z}_6$.

A continuación damos la construcción recíproca, a veces llamada *producto semidirecto externo*.

Proposición 6. *Sean G, H dos grupos y $\varphi : H \to \mathrm{Aut}(G)$ un morfismo de grupos. Definimos en el producto cartesiano de G con H la operación*

$$(g_1, h_1)(g_2, h_2) = (g_1\varphi_{h_1}(g_2), h_1h_2).$$

Probar que esta operación define una estructura de grupo en $G \times H$. Al grupo obtenido lo llamamos el φ-producto semidirecto de G por H y lo denotamos por $G \rtimes_\varphi H$.

Ejercicio 8.

1. Demostrar la proposición anterior. Para probar la asociatividad (antes la teníamos gratis) tendremos que usar que φ es un morfismo. ¿Quién es el elemento neutro en $G \rtimes_\varphi H$? ¿Quién es el inverso de (g, h)?

2. Probar que si $\varphi : H \to \mathrm{Aut}(G)$ es el morfismo trivial $\varphi_h = \mathrm{Id}_G$ para todo $h \in H$, entonces $G \rtimes_\varphi H = G \times H$, es decir, la estructura de producto semidirecto coincide con la estructura de producto directo.

Ejercicio 9. 1. Probar que el grupo afín de la recta

$$\mathrm{Aff}(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \mid f(x) = ax + b,\ a, b \in \mathbb{R},\ a \neq 0\}$$

es el producto semidirecto de las traslaciones $f_b(x) = x+b$ y las dilataciones $f_a(x) = ax$, $a \neq 0$. ¿Cuál de estos dos es el subgrupo normal?

2. Generalizar para el grupo afín del plano $\mathrm{Aff}(\mathbb{R}^2)$.

Ejercicio 10. Encontrar todo los grupos de orden 6, salvo isomorfismo, usando el siguiente argumento. Sea K un grupo con 6 elementos.

1. Probar que K tiene un elemento g de orden 3 y un elemento h de orden 2. Llamemos $G = \langle g \rangle \simeq \mathbb{Z}_3$ y $H = \langle h \rangle \simeq \mathbb{Z}_2$.

2. Probar que $G \lhd K$.

3. Por un ejercicio anterior, $\mathrm{Aut}(G) \simeq \mathbb{Z}_2$, luego hay sólo dos posibilidades para un morfismo de gruos $\varphi : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$: $\varphi = \mathrm{Id}$ o φ es la inversión. Concluir que en el primer caso tenemos que $G \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_2 \simeq \mathbb{Z}_6$ y en el segundo $G \simeq S_3$.

Ejercicio 11. Encontrar todos los grupos de orden 14 y 15 salvo isomorfismo.