Grupos

Un *grupo* es un conjunto G con una operación • que asocia a cada par de elementos a,b de G otro elemento de G, denotado por a•b, con las siguientes propiedades:

1. Para todos a,b,c en G, (a•b)•c=a•(b•c) (asociatividad)
2. Existe un e en G tal que para todo a en G, a•e=e•a=a (neutro)
3. Para cada a en G existe un a' en G tal que a•a'=a'•a=e (inversos)

Ejemplos:

- Los enteros, con la suma.
- Los racionales distintos de 0, con el producto.
- Z_n: los enteros modulo n, con la suma (mod n).
- Z_p*: Z_p-{0} los enteros modulo un primo p, sin el 0, con el producto (mod p).
- Las funciones biyectivas de R en R, con la composición
- Las matrices reales de nxn con determinante no 0, con el producto de matrices.
- Las isometrías del plano, con la composición

Cada grupo finito esta descrito por su "tabla de multiplicación", aquí estan las tablas de multiplicación de dos grupos distintos con 4 elementos (Z_4 y $Z_2 x Z_2$):

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Observar que si una tabla viene de un grupo, entonces en cada renglón y en cada columna deben aparecer todos los elementos del grupo. Esto es porque en un grupo las ecuaciones
ax = b y **xa = b** siempre tienen soluciones y las soluciones son únicas

Un **subgrupo** de un grupo (G,•) es un subconjunto H de G tal que (H,•) es un grupo (con la misma operación).

Ejemplos:

- Los números enteros forman un subgrupo del grupo de los números racionales con la suma.
- Las matrices con determinante 1 forman un subgrupo del grupo de las matrices invertibles de nxn.
- Las isometrías que preservan orientación forman un subgrupo del grupo de las isometrías del plano (pero las que invierten orientación no forman un subgrupo).

El **producto** de dos grupos G y G' es el grupo G x G' formado por las parejas (a,b) con $a \in G$ y $b \in G'$ con la multiplicación definida coordenada a coordenada, es decir,

$$G \times G' = \{(a,b) / a \in G, b \in G'\} \text{ y } (a,b)x(c,d) = (a \bullet c, b \circ d)$$

donde • es la multiplicación en G y ○ es el la multiplicación en G'

Ejemplo. Si Z_2 y Z_3 son los enteros modulo 2 y modulo 3 (con la suma) entonces $Z_2 \times Z_3$ es un grupo con 6 elementos: (0,0), (1,0), (0,1), (1,1), (0,2) y (1,2) que se suman coordenada a coordenada, la primera modulo 2 y la segunda modulo 3.

Si G y G' son dos grupos, un **homomorfismo** de G a H es una función $\varphi : G \to G'$ que preserva productos, es decir, $\varphi(a \bullet b) = \varphi(a) \circ \varphi(b)$.
Un **isomorfismo** es un homomorfismo biyectivo. Decimos que dos grupos son **isomorfos** si existe un isomorfismo entre ellos.

Ejemplos:

- Z_p^* es isomorfo a Z_{p-1}: un isomorfismo de Z_{p-1} a Z_p^* esta dado por la funcion $x \to 2^x$.
- Si m y n son primos relativos entonces $Z_m \times Z_n$ es isomorfo a Z_{mxn}:
  Podemos definir $\varphi : Z_m \times Z_n \to Z_{mxn}$ como $\varphi(a,b) = na+mb$. Esto es un homomorfismo de grupos ya que $\varphi((a,b)+(c,d)) = \varphi(a+c,b+d) = n(a+c)+m(b+d) = na+mb+nc+md = \varphi(a,b) +\varphi(c,d)$.
  Falta ver que si (m.n)=1 entonces φ es biyectiva, asi que es un isomorfismo (tarea).
- Si G es un grupo y a es un elemento fijo de G, entonces la **conjugación** por a, definida como por $\varphi_a(g)=aga^{-1}$ es un isomorfismo de G: φ_a es un homomorfismo porque
  $\varphi_a(xy) = axya^{-1} = ax(a^{-1}a)ya^{-1} = (axa^{-1})(aya^{-1}) = \varphi_a(x)\,\varphi_a(y)$
  y φ_a es biyectiva ya que tiene inversa (la conjugación por a^{-1})

El **orden** de un grupo finito G es el número de elementos en el grupo, y se denota por |G|.

Lema. Si G es un grupo finito y H es un subgrupo de G entonces |H| divide a |G|.

Demostracion. Si H es un subgrupo de G, entonces para cada g en G el conjunto gH={ gh / h∈H } es un subconjunto de G con la misma cardinalidad que H.
Los subconjuntos de la forma gH para algún g en G se llaman *clases laterales* de H. Veamos que dos clases laterales solo pueden ser iguales o ser ajenas (o sea que no pueden intersectarse a medias).
Si la clase gH intersecta a la clase g'H entonces gh = g'h' para algunas h, h' ∈ H.
Ahora, si gh'' ∈ gH entonces $gh'' = g(hh^{-1})h'' = (gh)(h^{-1}h'') = (g'h')(h^{-1}h'') = g'(h'h^{-1}h'') \in g'H$
por lo tanto gH ⊂ g'H. De la misma manera se muestra que gH ⊂ g'H y por lo tanto g'H = gH
Asi que las clases laterales dan una *partición* de G en subconjuntos de la misma cardinalidad que H.
Asi que la cardinalidad de G es un múltiplo de la cardinalidad de H. ◙

Corolario. El orden de cada elemento de un grupo G divide al orden de G.

Demostracion. Si g es un elemento de G entonces las potencias de g forman un subgrupo H de G. El orden de H es la primera potencia de g que es trivial, que es el orden de g. Y por el lema anterior el orden de H divide al orden de G. ◙

El **índice** de un subgrupo es el numero de veces que el subgrupo cabe en el grupo
(si el grupo es finito, el índice es el orden del grupo dividido por el orden del subgrupo)

Ejemplo. El grupo Z_{12} tiene un subgrupo isomorfo a Z_4, formado por los elementos {0,3,6,9}.
Como el orden del grupo es 12 y el orden del subgrupo es 4, el índice del subgrupo es 3.

Problemas.

1. Muestra que existen exactamente 2 grupos no isomorfos con 4 elementos.
   ¿Cuantos grupos no isomorfos con 5 elementos existirán?

2. Muestra que $Z_m \times Z_n$ y Z_{mxn} son isomorfos si y solo si m y n son primos relativos.
   Hint: ⇒ Si (m.n)>1 ve que todos los elementos de $Z_m \times Z_n$ tienen orden menor que mxn.
   ⇐ Si (m.n)=1 usa el homomorfismo dado en los ejemplos, y ve que hay un elemento que va al 1.

3. Si G es un grupo y a es cualquier elemento de G, muestra que la función
   $\varphi_a : G \to G$ dada por $\varphi_a(g)=aga^{-1}$ es un isomorfismo.

Grupos de simetrías

Las simetrías de una figura plana son las isometrías del plano que la dejan invariante.
Las simetrías de una figura plana forman un grupo.

¿Como son los grupos de simetrías de las figuras del plano?

$\mathbf{Z}_2$

(id,reflexión)

Z_2

(id, rotación)

$Z_2 \times Z_2$

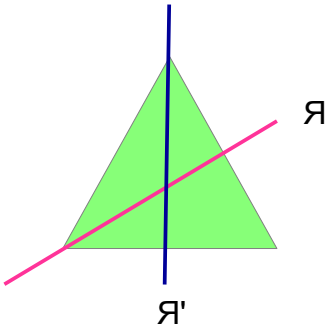
(id, rotación, 2 reflexiones)

Z_4

(id, 3 rotaciones)

¿Habrá una figura en el plano cuyo grupo de simetrías sea $Z_2 \times Z_3$? ¿Y $Z_3 \times Z_3$?

Ejemplo. El grupo de simetrías de un triángulo equilátero tiene 6 simetrías: 3 rotaciones (incluyendo a la identidad) y 3 reflexiones, si Я y son las reflexiones en las rectas mostradas, entonces Я'○Я es la rotación de 120° y Я○Я' es la rotación de -120°.
Así que todas las isometrías del triángulo estan generadas por las reflexiones Я y Я', pero el grupo no es conmutativo asi que no puede ser isomorfo a Z2 x Z3.



De manera similar, el grupo de isometrías de un polígono regular de n lados tiene 2n elementos: n rotaciones (incluyendo a la identidad) y n reflexiones.
Este grupo esta generado por una rotación R con ángulo $^{2\pi}/_{n}$ y una reflexión en una recta r: todas las rotaciones son múltiplos de R y todas la reflexión en otra recta r' se obtiene rotando para llevar r; a r, reflejando en r y regresando r a r' asi que todas las reflexiones son de la forma $R^n \circ Я \circ R^n$ donde Я es una reflexión fija.
El grupo también esta generado por 2 reflexiones en rectas que formen un ángulo π/n.
Pero este grupo *no es conmutativo* si n>2 ya que 2 refexiones en rectas que forman un ángulo distinto de π no conmutan.

A este grupo se le conoce como el grupo diédrico de orden n, y se le denota por D_n.

¿Como serán los grupos de simetrías de todas las figuras del plano?

Es intuitivamente claro que si F es una figura del plano, entonces las simetrías de F deberían dejar fijo al menos un punto: el centro de gravedad de F. Pero si pensamos un poco surgen dudas: ¿que es el centro de gravedad? ¿Todas las figuras planas tienen centro de gravedad? ¿y donde esta? En el caso de los poligonos, hay otro punto cuya existencia es clara y que podemos calcular fácilmente usando coordenadas: el **centroide** de un conjunto finito de puntos p_1, p_2,p_3,..,p_n en $\mathbf{R}^2$ el punto $^1/_n\,(p_1+p_2+p_3+...+p_n)$ que es el *promedio* de los puntos.

El Teorema de Leonardo. Todo grupo finito G de isometrías de $\mathbf{R}^n$ tiene un punto fijo.

Demostracion. Sean g_1, g_2, g_3, ...g_n los elementos en G. Sea p *cualquier* punto de R^n, y sea x el centroide de sus imágenes bajo los elementos de G, es decir, $x = {}^1/_n\,(g_1(x)+g_2(x)+g_3(x)+...+g_n(x))$.
Las isometrías del plano son funciones afines, que preservan promedios, por lo que si g es cualquier elemento de G entonces

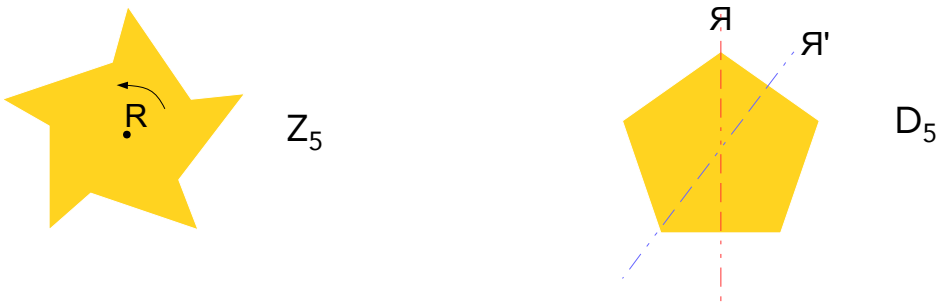
$$g(x) = g(\,{}^1/_n\,(g_1(p)+g_2(p)+g_3(p)+...+g_n(p))) = {}^1/_n\,(gg_1(p)+gg_2(p)+gg_3(p)+...+gg_n(p)).$$

Pero como G es un grupo, los productos g_ig_1,g_ig_2,g_ig_3,...,g_ig_m son todos los elementos de G, en otro orden. Por lo tanto

$$d(x) = {}^1/_n\,(gg_1(p)+gg_2(p)+gg_3(p)+...+gg_n(p)) = {}^1/_n\,(g_1(p)+g_2(p)+g_3(p)+...+g_n(p)) = x$$

■

Teorema. Los grupos finitos de isometrías del plano son cíclicos o diédricos.



Demostracion. Si G es un grupo finito de isometrías entonces por el teorema de Leonardo G fija un punto p y por lo tanto G consta de rotaciones con centro en p y/o reflexiones en rectas por p.

Caso 1. Si el grupo G contiene únicamente rotaciones, sea R la rotación en G con ángulo positivo mas pequeño. Si R' es otra rotación en G, entonces el ángulo φ' de R' debe ser un múltiplo entero del ángulo φ de R ya de otra manera, $\varphi'=n\varphi+\varphi''$ donde $0<\varphi''<\varphi'$ asi que la composición $R''= R^{-n}\circ R'$ seria una rotación con ángulo $\varphi''<\varphi$', contradiciendo nuestra elección de R.
Como R y R' tienen el mismo centro y el ángulo de rotación de R es un múltiplo del ángulo de rotación de R, entonces $R'=R^n$ para alguna n en Z. Asi que todas las rotaciones del grupo son potencias de R, lo que dice que G un grupo cíclico.

Caso 2. Si el grupo G contiene al menos 2 reflexiones, sean Я y Я' dos reflexiones en rectas que formen un ángulo mínimo θ. Entonces Я○Я' es una rotación con ángulo 2θ. Si R es una rotación en G con ángulo mínimo φ, entonces Я○Я' es una potencia de R (porque todas las rotaciones de G lo son) asi que 2θ es un múltiplo de φ.
Pero Я○R es una reflexión en una recta que forma un ángulo φ/2 con la recta de la reflexión Я, asi que θ ≤ φ /2 (porque θ es el ángulo mínimo entre 2 refexiones). Asi que 2θ= φ y Я○Я' = R.
Asi que las reflexiones Я y Я' generan al grupo, ya que la mitad de los elementos de G deben preservar orientación y por lo tanto son rotaciones, que son múltiplos de R, y al componer las rotaciones con Я obtenemos todas las reflexiones de G. La multiplicación del grupo queda determinada por las relaciones R^n = id y Я○R○Я = R^{-1}.

Caso 3. Si el grupo G solo contiene una reflexión Я. Si G contuviera una rotación R con ángulo θ, entonces R○Я seria otra reflexión en G)en una recta que forma un ángulo θ/2 con la primera).
Asi que G no puede contener rotaciones y G es isomorfo a Z_2. ◙

Problemas.

4. Da una figura en el plano cuyo grupo de simetrías sea $Z_3 \times Z_5$ y demuestra que no existe ninguna figura en el plano cuyo grupo de simetrías sea $Z_3 \times Z_6$.

5. Muestra que el grupo de simetrías del 37-agono regular esta generado por cualquier par de reflexiones, y también por cualquier rotación y cualquier reflexión. Muestra que esto no es cierto para el 39-agono regular.

6. Demuestra que dos rotaciones del plano conmutan solo cuando tienen el mismo centro, y que dos reflexiones conmutan solo cuando son en rectas perpendiculares o son iguales.

6. Muestra que en el grupo de isometrías del plano:

a. Los conjugados de una traslación son traslaciones a la misma distancia, quizás en otras direcciones

b. Los conjugados de una reflexión en una recta son reflexiones, quizás en otras rectas.

c. Los conjugados de una rotación son rotaciones, quizás con otros centros, pero con el mismo ángulo o con el ángulo opuesto.