

Talleres de Formación Matemática  
Barquisimeto, 9 al 14 de octubre, 2000

# Taller de Álgebra y Combinatoria

José H. Nieto  
(LUZ)

Roy Quintero  
(ULA-Trujillo)



# Prefacio

Estas notas constituyen el material de apoyo para un Taller de veinte horas de duración sobre Álgebra y Combinatoria, dirigido a estudiantes de Licenciatura en Matemáticas. El único prerrequisito necesario es estar familiarizado con los rudimentos de la Teoría de Grupos.

El material está organizado en tres capítulos. El primero es esencialmente el texto de un *notebook* de *Mathematica*, y está dirigido a mostrar cómo las herramientas computacionales simbólico-gráficas pueden ser usadas en la enseñanza y aprendizaje del Álgebra, en particular de la Teoría de Grupos.

En el segundo capítulo se estudia el concepto de *acción* de un grupo sobre un conjunto, el cual juega un rol central en muchas ramas de la matemática y sus aplicaciones. El tercer capítulo se ocupa de la *Teoría de Polya*, que trata de la enumeración de configuraciones bajo la acción de grupos.

A lo largo del texto hay numerosos *Ejercicios*, destinados a poner a prueba la comprensión del material tratado y a suministrar ejemplos. Es absolutamente *imprescindible* resolver estos ejercicios antes de continuar avanzando en el texto.

Al final de los capítulos 2 y 3 hay también una lista de *Problemas*, naturalmente de mayor dificultad que los ejercicios. En un Apéndice se incluyen las soluciones.



# Índice General

<b>1</b>	<b>Teoría de Grupos y <i>Mathematica</i></b>	<b>1</b>
1.1	Introducción . . . . .	1
1.2	Ejemplos de grupos usando <i>Mathematica</i> . . . . .	7
1.3	Producto de grupos, grupo cociente y homomorfismo de grupos . . . . .	11
1.4	Principales comandos de <i>Mathematica</i> empleados . . . . .	14
<b>2</b>	<b>Acción de un grupo sobre un conjunto</b>	<b>17</b>
2.1	Preliminares . . . . .	17
2.2	Acción de grupos . . . . .	18
2.3	Algunas aplicaciones . . . . .	22
2.3.1	Teorema de Cauchy . . . . .	22
2.3.2	Teoremas de Sylow . . . . .	23
2.4	Problemas . . . . .	25
<b>3</b>	<b>Enumeración bajo acción de grupos</b>	<b>27</b>
3.1	El Lema de Cauchy-Frobenius-Burnside . . . . .	28
3.2	La Acción de Polya . . . . .	29
3.2.1	Ejemplo: coloración del cubo con $r$ colores . . . . .	30
3.2.2	Aplicación: identidades con números de Stirling . . . . .	31
3.3	El Teorema de Polya . . . . .	32
3.4	Enumeración de grafos no isomorfos . . . . .	34
3.5	Problemas . . . . .	37
<b>A</b>	<b>Soluciones a los Problemas</b>	<b>39</b>
	<b>Bibliografía</b>	<b>43</b>
	<b>Índice de Materias</b>	<b>45</b>



# Capítulo 1

## Teoría de Grupos y *Mathematica*

### 1.1 Introducción

El presente capítulo cubre algunas nociones básicas sobre Teoría de Grupos que luego serán necesarias para el entendimiento de los siguientes capítulos. La intención fundamental es despertar el interés de estudiantes y profesores en el uso de herramientas simbólico-gráficas como complemento para el aprendizaje-enseñanza del material teórico de un curso introductorio de Teoría de Grupos. Específicamente se emplearán algunas partes del libro-paquete de *Mathematica* denominado *Exploring Abstract Algebra with Mathematica* [6], de Allen C. Hibbard y Kenneth M. Levasseur. En realidad para esta primera parte se requiere de un laboratorio de computación donde se haya instalado previamente *Mathematica*, preferiblemente la versión 3.0 o mayor y el paquete de álgebra abstracta antes mencionado. No se requiere un conocimiento previo de *Mathematica* para su desarrollo, pero sí un conocimiento básico general de las nociones de Teoría de Grupos consideradas. Para aquellas personas realmente motivadas y con expectativas mayores recomendamos la lectura y desarrollo de los laboratorios del libro-paquete indicado, debemos mencionar que el mismo cubre también otras áreas relevantes del Álgebra Abstracta como la Teoría de Anillos, incluyendo Cuerpos Finitos y Polinomios entre otras. También se incluye una Guía del Usuario donde se explican los diferentes comandos de *Mathematica* usados a lo largo del libro o laboratorio y sus potencialidades. Sin más preámbulo comencemos pues por recordar que existen diversas formas de introducir la noción general de grupo, una de ellas surge a partir del estudio de las simetrías de

un polígono regular, por ejemplo un triángulo equilátero.

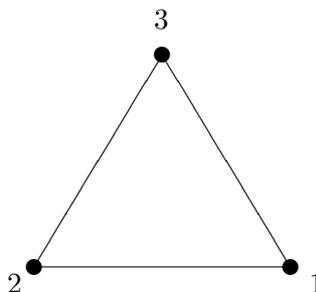
Primeramente se requiere la activación de la siguiente célula (para esto debe colocar el cursor sobre la célula y pulsar conjuntamente Shift y Enter),

```
Needs["AbstractAlgebra`Master`"];
SwitchStructureTo[Group];
```

Consideremos un triángulo equilátero con sus vértices identificados o etiquetados con los números 1, 2 y 3. Para verlo evalúe la célula:

```
triángulo = ShowFigure[3, {1, 2, 3}, "D"];
```

Aparecerá un triángulo como el siguiente (en la pantalla los vértices estarán diferenciados por colores):



Intentemos mover el triángulo de forma que después del movimiento parezca que el mismo no ha sido movido excepto por una nueva ordenación de las etiquetas de los vértices. Por ejemplo, dibuje una línea imaginaria que pase por el vértice 3 y sea perpendicular al lado opuesto, entonces refleje el triángulo. Para ello evalúe la siguiente célula:

```
Show[triángulo, Epilog -> {Blue, Line[{{0, -1.5}, {0, 2.0}}]}];
```

(De ahora en adelante, en general, no mostraremos el resultado de la evaluación, que puede ser visto en el computador).

Después de reflejar el triángulo a través de la línea azul, obtenemos el resultado siguiente (evalúe):

```
ShowPermutation[{1 -> 2, 2 -> 1, 3 -> 3}]
```

Esta reflexión es un ejemplo de una transformación geométrica llamada *simetría*. Observe que ha habido cambios en la ubicación de los vértices: el vértice 1 y el vértice 2 intercambiaron sus posiciones, y el vértice 3 mantuvo

su ubicación. Esta simetría induce una *permutación* de los vértices. Una manera de representar esta permutación en *Mathematica* es

$$\{1 \rightarrow 2, 2 \rightarrow 1, 3 \rightarrow 3\}$$

Denotemos esta primera permutación por  $p[1]$  (evalúe la célula)

```
Clear[p]
p[1] = {1 → 2, 2 → 1, 3 → 3}
```

¿Existirán otras simetrías (permutaciones) del triángulo equilátero? Seguramente que sí hay otras. Denotemos las restantes por  $p[2]$ ,  $p[3]$ , etc. Cada vez que descubra una permutación, debe escribir  $p[k] = \{1 \rightarrow x, 2 \rightarrow y, 3 \rightarrow z\}$ . donde usted proporciona valores apropiados de  $k, x, y, z$ . Por ejemplo,  $p[2]$  podría ser

$$p[2] = \{1 \rightarrow 2, 2 \rightarrow 3, 3 \rightarrow 1\}$$

Para comprobar que  $p[2]$  es realmente una permutación válida y apreciar el efecto geométrico que provoca en el triángulo evalúe la célula

```
ShowPermutation[p[2]]
```

Observe que  $\{1 \rightarrow 2, 2 \rightarrow 3, 3 \rightarrow 1\}$  también puede ser determinada considerando únicamente las segundas coordenadas de cada regla de asignación  $k \rightarrow x$ , ya que las primeras coordenadas son siempre las mismas para toda permutación.

Veamos ahora la última permutación en forma de matriz, para ello evalúe la siguiente célula

```
PermutationMatrix[{1 → 2, 2 → 3, 3 → 1}]
```

Note que cada columna representa una regla de la forma  $k \rightarrow x$ . Así que, la lista  $\{2, 3, 1\}$  puede ser usada para representar a  $p[2]$ . Por tanto, uno podría escribir

$$p[2] = \{2, 3, 1\}$$

y entonces

```
ShowPermutation[p[2]]
```

nos daría el mismo resultado.

Siguiendo este procedimiento usted debería obtener todas las posibles simetrías del triángulo (en forma de permutación). ¿Cuántas permutaciones ha encontrado incluyendo p[1] y p[2]? Escribalas por favor (para producir el símbolo  $\rightarrow$  presione las teclas Esc, -, >, Esc).

Ahora estamos interesados en saber si existe algún tipo de interrelación entre las simetrías del triángulo. Por ejemplo, supongamos que primero aplicamos la simetría dada por la permutación p[1] y luego aplicamos la simetría dada por p[2]. ¿Cuál será la apariencia final de la figura? ¿Habrá alguna permutación que coincida con este “producto”? Usaremos la función `MultiplyPermutations` para hacer esto. Veamos como trabaja este comando, para ello evalúe las células siguientes para recordar las definiciones de p[1] y p[2].

```
p[1]
p[2]
```

y luego la célula

```
producto = MultiplyPermutations[p[2], p[1], Mode→Textual]
```

Esto produce la permutación que es el producto de p[1] seguida por p[2]. Veamos qué efecto tiene la permutación resultante sobre el triángulo. Para ello evalúe la célula:

```
ShowPermutation[producto]
```

El resultado es una simetría del triángulo. ¿Qué pasará si invertimos el orden de aplicación de las permutaciones anteriores? La siguiente célula nos da la respuesta.

```
MultiplyPermutations[p[1], p[2], Mode→Textual]
```

Simplemente el resultado es diferente. En este caso es muy común, en Matemática, decir que el producto considerado no es conmutativo.

Ahora construyamos una tabla de “multiplicación” con todos los productos posibles de permutaciones. Esta debería disponerse, por ejemplo, de la siguiente forma

	p[1]	p[2]	p[3]	...
p[1]				
p[2]				
p[3]			x	
...				

La fila superior y la columna de la izquierda nos indican cuáles elementos están interactuando. El cuerpo de la tabla es llenado multiplicando las entradas de las filas por las entradas de las columnas. Por ejemplo, la entrada  $X$  situada en la fila 3 columna 2 puede ser obtenida (si previamente hemos definido quién es  $p[3]$ ) mediante la evaluación de la célula.

`MultiplyPermutations[p[3], p[2]]`

Si al intentar llenar la tabla encuentra un producto que no está en su lista original, quizás sea mejor volver atrás y hacer una revisión de ella. Eventualmente su lista debería terminar (piense un poco sobre las diferentes posibles simetrías del triángulo), y el resultado del producto de cualquier par de permutaciones debería ser otra permutación ya listada. En este caso, los miembros en el cuerpo de la tabla deberían consistir solamente de los elementos listados en la fila superior (o columna izquierda). Decimos entonces que el conjunto de elementos (simetrías del triángulo, representadas por permutaciones en este caso) es cerrado bajo este producto.

Cuando consideramos la adición de números reales, tenemos  $r + 0 = 0 + r = r$  para todo número real  $r$ . ¿Ocurrirá una situación análoga con las permutaciones estudiadas y el producto dado anteriormente? Es decir, ¿existirá una permutación  $p[j]$  que satisfaga la ecuación

`MultiplyPermutations[p[i], p[j]] =`  
`MultiplyPermutations[p[j], p[i]] = p[i]`

para toda  $p[i]$ ? Si la respuesta es afirmativa, ¿cómo se define  $p[j]$ ? En realidad existe y actúa dejando cada vértice en su posición inicial, es decir, deja al triángulo inalterado y usualmente es llamada identidad.

Por otra parte, si recordamos bien para cada  $r$  real existe un elemento (real)  $-r$  que satisface  $r + (-r) = (-r) + r = 0$ , siendo 0 la identidad aditiva de los reales. Queremos saber si dada una permutación cualquiera  $p[i]$  existe otra permutación  $p[j]$  tal que

`MultiplyPermutations[p[i], p[j]] =`  
`MultiplyPermutations[p[j], p[i]]`

y que esto a su vez sea igual a la identidad encontrada anteriormente. Si es así, decimos que  $p[j]$  es un (el) inverso de  $p[i]$ . Usando la tabla construida previamente, verifique que cada simetría (permutación) tiene un inverso. Por favor liste los elementos y sus correspondientes inversos. ¿Tiene alguna observación que hacer?

Otra vez recurriendo a la suma de números reales, recuerde que  $(a + b) + c = a + (b + c)$  para  $a$ ,  $b$ , y  $c$  cualesquiera. Esta ecuación dice que la suma de reales es asociativa. La siguiente pregunta es: ¿será el producto de permutaciones asociativo? En otras palabras, ¿será cierto que

$$\text{MultiplyPermutations}[p[i], \text{MultiplyPermutations}[p[j], p[k]]] = \text{MultiplyPermutations}[\text{MultiplyPermutations}[p[i], p[j]], p[k]]$$

para  $i$ ,  $j$ , y  $k$  cualesquiera? Si asumimos que usted encontró seis permutaciones, y que fueron definidas como  $p[1]$ ,  $p[2]$ , ...,  $p[6]$ , la siguiente célula permite chequear la asociatividad de la multiplicación de permutaciones, ¡pruebe!

```
assoc = True;
Do[Temp = MultiplyPermutations[
p[i], MultiplyPermutations[p[j], p[k]]] ===
MultiplyPermutations[
  MultiplyPermutations[p[i], p[j]], p[k]];
  assoc = And[assoc, temp], {i, 6}, {j, 6}, {k, 6}];
assoc
```

Observe que hay 216 posibles pruebas, ¿por qué? Después de efectuarlas debería concluir que efectivamente la multiplicación de permutaciones es asociativa.

Finalmente juntemos los diferentes aspectos considerados. Ciertamente la colección de las seis simetrías del triángulo equilátero con el producto de una transformación seguida por otra (que hemos representado por medio de permutaciones con la multiplicación de ellas estudiada) es un ejemplo de un conjunto con una operación binaria que cumple una lista de propiedades y que comúnmente es denominado grupo. Una definición formal de grupo es: dado un conjunto  $G$  y una operación  $*$ , decimos que  $G$  es un *grupo* si satisface las condiciones siguientes:

1. El conjunto es cerrado bajo la operación, es decir,  $g * h$  está en  $G$  para todo  $g$  y  $h$  en  $G$ .
2. Entre los elementos existe una identidad, es decir, existe  $e$  en  $G$  tal que  $e * g = g * e = g$  para todo  $g$  en  $G$ .
3. Cada elemento tiene un inverso, es decir, para todo  $g$  en  $G$  existe  $h$  en  $G$  tal que  $g * h = h * g = e$ .
4. La operación es asociativa, es decir,  $f * (g * h) = (f * g) * h$  para todo  $f$ ,  $g$  y  $h$  en  $G$ .

Si adicionalmente tenemos que  $g*h = h*g$  para todo  $g$  y  $h$  en  $G$ , decimos que  $G$  es *conmutativo* o *abeliano*.

De acuerdo a lo estudiado hasta aquí tenemos que el conjunto de las seis simetrías (permutaciones) del triángulo equilátero con la operación seguir una transformación por otra (multiplicación de permutaciones) es un ejemplo de un grupo no abeliano. ¿Por qué?

Este grupo usualmente es denotado por  $S_3$  (nosotros momentáneamente lo simbolizaremos con  $G$ ) y los elementos que lo constituyen pueden ser vistos activando:

```
G = Symmetric[3]
```

Si además queremos una tabla que incluya y nos permita apreciar todos los posibles productos de permutaciones, se requiere la activación de la siguiente célula

```
CayleyTable[G, Mode → Visual]
```

(se verá la tabla de multiplicación o *Tabla de Cayley* de  $S_3$ ).

## 1.2 Ejemplos de grupos usando *Mathematica*

Comencemos con un ejemplo de un conjunto que tiene asociada una operación, pero que no es grupo. En efecto, considere

```
Clear[G]
G = FormGroupoid[{1, 2, 3, 5, 8}, Plus, "+"]
```

El conjunto  $G$  no es cerrado bajo la operación  $+$ . El siguiente comando en modo textual, nos ilustra la no clausura de  $G$  cuando el resultado es falso.

```
ClosedQ[G, Mode → Textual]
```

Si en lugar del modo textual empleamos el visual, el comando `ClosedQ` muestra los productos de la tabla en casillas amarillas si ellos pertenecen al conjunto, y en casillas rojas en caso contrario.

Ahora presentaremos algunos ejemplos de grupos que son considerados tradicionales en la literatura, e importantes por su naturaleza y trascendencia en la Matemática a lo largo del tiempo. También mostraremos algunos comandos de *Mathematica* que nos permitirán observar ciertas propiedades relevantes en cada caso. Entre ellos podemos mencionar  $\mathbb{Z}_n$ , el grupo de los

enteros bajo la suma mod  $n$ ,  $U_n$ , el grupo de las unidades mutiplicativas de  $\mathbb{Z}_n$  (en este caso recuerde que la operación es la multiplicación mod  $n$ ), el grupo diédrico  $D_n$ , los grupos cíclicos y el grupo 4 de Klein. Comencemos escogiendo aleatoriamente un  $\mathbb{Z}_n$  con  $n$  entre 2 y 30.

```
Clear [G]
Clear [n]
n = Random[Integer, {2, 30}]
G = Z[n]
```

Calculemos los diferentes órdenes de los elementos de  $\mathbb{Z}_n$  (el *orden* de un elemento  $g$  de un grupo es el menor entero positivo  $k$  tal que  $g^k = e$ ). El siguiente comando nos construye una tabla que muestra el orden de cada elemento e inmediatamente la frecuencia de los órdenes calculados. ¡Verifíquelo!

```
ShowGroupOrders[Z[n]]
```

Veamos ahora un ejemplo relativo a  $U_n$ . Exactamente, consideraremos la posibilidad de que un subconjunto de un grupo sea un grupo cuando usamos la misma operación del grupo original (en este caso decimos que el subconjunto es un *subgrupo* del grupo inicial). Comencemos por elegir aleatoriamente un  $U_n$  con  $n$  entre 6 y 23.

```
Clear [G]
n = Random[Integer, {6, 23}]
G = U[n]
```

Ahora escogemos aleatoriamente otro entero positivo  $m$ , menor que  $n$ , para luego seleccionar  $m$  elementos de  $G$  y así formar un subconjunto que llamaremos  $H$ .

```
m = Random[Integer, {1, Floor[N[√n]]}]
H = RandomElements[G, m, Replacement → False]
```

La primera pregunta es, ¿será este conjunto un subgrupo de  $G$ ?, y si la respuesta es negativa, ¿cómo podemos construir uno a partir de él?

Emplee el siguiente comando para responder a la primera pregunta.

```
SubgroupQ[H, G]
```

Simplemente saber si es verdadero o falso que  $H$  es subgrupo de  $G$  es de valor limitado. Nos gustaría saber también como hacer que  $H$  se convierta en un subgrupo (agregando elementos de  $G$  si es necesario). Observemos la Tabla de Cayley de  $G$  enfocándonos sobre los elementos de  $H$ .

```
SubgroupQ[H, G, Mode → Visual]
```

Note que las casillas rojas contienen elementos de  $G$  que no pertenecen a  $H$ . ¿Qué pasa si modificamos  $H$  incluyendo algunos o todos los elementos que son productos de elementos de  $H$  y que no pertenecen a  $H$ , es decir, elementos que aparecen en casillas rojas? Mediante la variable llamada `ElementosAgregados` agregue los elementos mencionados entre llaves, que desee adjuntar a  $H$  para ver si de esta forma se transforma en un subgrupo de  $G$ .

```
ElementosAgregados = {};
H = Union[Join[H, ElementosAgregados]]
SubgroupQ[H, G, Mode → Visual];
```

Repita este procedimiento, es decir, agregue nuevos elementos, escogiendo entre aquellos que aparecen en casillas rojas si existen, a la variable `ElementosAgregados`, tantas veces como sea necesario hasta lograr que se convierta en subgrupo. Usted sabrá cuando parar en el momento en que no aparezcan casillas rojas.

Intente nuevamente

```
Clear[G]
n = Random[Integer, {6, 23}];
G = U[n]

m = Random[Integer, {1, Floor[N[√n]]}]
H = RandomElements[G, m, Replacement → False]
SubgroupQ[H, G, Mode → Visual];

ElementosAgregados = {};
H = Union[Join[H, ElementosAgregados]]
SubgroupQ[H, G, Mode → Visual];
```

Una vez que usted se sienta seguro sobre cómo extender  $H$  hasta hacerlo un subgrupo, puede pedir a *Mathematica* hacer esa parte y entonces concentrarse en otras cosas. Llamaremos al nuevo subgrupo de  $G$  formado a partir del conjunto  $H$  la *clausura* de  $H$  en  $G$  y para obtenerlo usaremos el comando `Closure`. Escojamos un nuevo grupo

```
Clear[G]
n = Random[Integer, {6, 23}];
G = U[n]
```

```
m = Random[Integer, {1, Floor[N[√n]]}]
H = RandomElements[G, m, Replacement → False]
SubgroupQ[H, G, Mode → Visual];
```

La clausura de  $H$  en  $G$  la determinamos activando la célula

```
Closure[G, H]
```

Los siguientes dos comandos son variaciones pequeñas del mismo

```
Closure[G, H, ReportIterations → True]
```

muestra el número de iteraciones necesarias para determinar la clausura, y

```
Closure[G, H, Mode → Visual]
```

simplemente muestra la misma información, pero visualmente. Estos gráficos pueden ser animados, si se desea. Para ello, presione dos veces (double-click) sobre cualquiera de los gráficos y ajuste el movimiento con las teclas flechas.

Ejemplos de otros grupos son dados a través de los comandos siguientes. Empecemos con el grupo diédrico

```
Dihedral[4, Mode → Visual]
```

Si desea una tabla que muestre los diferentes productos del grupo diédrico de orden 8, considere la célula

```
CayleyTable[Dihedral[4], Mode → Visual]
```

El grupo genérico cíclico de orden 6 se obtiene mediante el comando

```
Cyclic[6]
```

Pero si prefiere un símbolo diferente como generador y al mismo tiempo representarlo gráficamente, active la célula

```
CyclicGroup[10, Generator → "α", Mode → Visual]
```

Para concluir esta sección, construyamos el grupo 4 de Klein

```
Klein4
```

y su respectiva tabla

```
CayleyTable[Klein4, Mode → Visual]
```

### 1.3 Producto de grupos, grupo cociente y homomorfismo de grupos

En esta penúltima sección presentaremos algunas nociones bien conocidas a través de algunos comandos de *Mathematica*. Empecemos con el concepto de producto directo de dos grupos. Definamos dos grupos iniciales, por ejemplo

```
G1 = U[10]
G2 = Z[4]
```

¿Cómo podemos combinarlos para formar un nuevo grupo donde ambos  $G_1$  y  $G_2$  puedan ser vistos como “subgrupos” en cierto sentido? Del Algebra Lineal sabemos lo que significa representar vectores como pares ordenados y entonces usar la adición componente a componente, así que es posible que podamos implementar una estrategia parecida.

Lo que haremos es formar pares ordenados de la forma  $(x, y)$ , donde  $x$  es obtenido de  $G_1$  y  $y$  es obtenido de  $G_2$ . Al conjunto de todos estos pares ordenados se le puede dotar de una estructura de grupo considerando la operación definida por  $(x, y)(a, b) = (xa, yb)$ , donde la operación efectuada en la primera componente del lado derecho toma lugar en  $G_1$  y la efectuada en la segunda componente toma lugar en  $G_2$ . Llamaremos a este grupo el *producto directo* de  $G_1$  y  $G_2$  y lo denotaremos por  $G_1 \times G_2$ . El siguiente comando nos determina el producto directo

```
G = DirectProduct[G1, G2]
```

Como hemos podido apreciar anteriormente, el estudio de la tabla de Cayley de un grupo puede revelar información significativa.

```
CayleyTable[G, Mode → Visual];
```

Nuestro objetivo ahora es construir el *grupo cociente* de un grupo por un subgrupo. Recordemos que para esto es necesario calcular las diferentes co-classes (clases laterales izquierdas y derechas). Comencemos con un ejemplo conocido. Supongamos que partimos de cierto grupo  $G$ , digamos el grupo diédrico de orden 8,  $D_4$ .

```
Clear[G]
G = Dihedral[4]
```

Ahora consideremos un subgrupo de  $G$ , digamos  $H = \{1, \text{Rot}^2\}$ , consistente de la identidad y la rotación de  $180^\circ$  (visto  $D_4$  como el conjunto de las simetrías del cuadrado)

$$H = \{1, \text{Rot}^2\}$$

Recordemos que la coclase izquierda de  $H$  en  $G$  que contiene a  $g$  se denota por  $gH$  y es el conjunto  $\{g * h | h \in H\}$ , Similarmente se define la coclase derecha de  $H$  en  $G$  que contiene a  $g$ , y es denotada por  $Hg$ . Para calcular las diferentes coclases que contienen el elemento  $\text{Rot}^{2**\text{Ref}}$ , usaremos los siguientes comandos

```
LeftCoset[G, H, Rot2**Ref]
RightCoset[G, H, Rot2**Ref]
```

Ahora emplearemos el comando que sigue para visualizar mejor la coclase izquierda (igual a la coclase derecha) que contiene a  $\text{Rot}^{2**\text{Ref}}$ ,

```
LeftCoset[G, H, Rot2**Ref, Mode → Visual]
```

El siguiente comando nos muestra una tabla consistente de una columna (la izquierda) con los elementos de  $G$  seguida por las coclases izquierdas y derechas en las columnas central y derecha respectivamente. En efecto

```
TableForm[
  Map[{#, LeftCoset[G, H, #], RightCoset[G, H, #]} &,
  Elements[G]], TableDepth → 2,
  TableHeadings → {None, {"g", "gH", "Hg\ n"}}]
```

Como se puede observar en la tabla resultante, cada coclase izquierda coincide con su respectiva coclase derecha, así que el subgrupo  $H$  es *normal* en  $G$ . Por tanto, podemos calcular el grupo cociente  $G/H$ , mediante

```
QuotientGroup[G,H]
```

Una presentación muy buena del grupo cociente se consigue mediante la célula

```
CayleyTable[QuotientGroup[G,H], Mode → Visual, Output
→ Graphics]
```

Para finalizar esta sección introduzcamos algunos ejemplos que involucren la noción de *homomorfismo* de grupos. Recordemos que un homomorfismo de un grupo  $(G, *)$  en un grupo  $(H, \#)$  es una función de  $G$  en  $H$  que preserva las operaciones. Esto es,  $f : G \rightarrow H$  es un homomorfismo si para todos los valores de  $x$  y  $y$  en  $G$  se cumple

$$f(x * y) = f(x) \# f(y)$$

Los homomorfismos nos proveen de otra herramienta útil para explorar propiedades de grupos. Revisamos la noción de preservación de una operación mediante dos funciones del grupo de los enteros módulo 12 en el grupo de los enteros módulo 6. Usaremos la función `FormMorphoid` para crearlas. La primera función suma 3 a cada elemento de  $\mathbb{Z}_{12}$  y entonces toma el residuo módulo 6. La segunda suma 6 antes de tomar el residuo módulo 6.

```
f = FormMorphoid[Mod[#1 + 3, 6] &, Z[12], Z[6]]
```

```
g = FormMorphoid[Mod[#1 + 6, 6] &, Z[12], Z[6]]
```

A continuación veremos si la función  $f$  preserva las operaciones entre los grupos para un par específico de elementos, digamos 3 y 11. Para ello considere el comando

```
PreservesQ[f, {3, 11}, Mode → Visual]
```

Las operaciones no son preservadas porque  $5 = f(3 + 11) \neq f(3) + f(11) = 2$ . Por este simple ejemplo concluimos que  $f$  no es homomorfismo. Veamos qué pasa con  $g$

```
PreservesQ[g, {3, 11}, Mode → Visual]
```

Con el par (3, 11)  $g$  actúa como un homomorfismo. Pero en realidad, ¿satisface  $g$  esta propiedad para todos los pares de  $\mathbb{Z}_{12}$ ? Usaremos el comando `MorphismQ` para probar todos los pares. Efectivamente

```
MorphismQ[g, Mode → Visual]
```

nos dice que sí. Si  $g$  es reemplazada por  $f$  en la anterior célula, el color amarillo de las casillas cambia a blanco indicando lo contrario.

```
MorphismQ[f, Mode → Visual]
```

Finalmente para concluir esta sección calculemos el Núcleo de  $g$  usando el comando

```
Kernel[g, Mode → Visual]
```

y su Imagen activando la célula

```
Image[g]
```

Como dijimos previamente los homomorfismos pueden ser empleados para explorar propiedades de grupos. Por ejemplo considere la siguiente tabla

```
TableForm[
Table[x = RandomElement[Z[12]]; xinv = GroupInverse[Z[12], x];
gxinv = g[xinv]; gx = g[x]; invgx = GroupInverse[Z[6], g[x]];
{x, xinv, gxinv, gx, invgx}, {6}],
TableHeadings
→ {None, {"x", "x-1", "g(x-1)", "g(x)", "g(x)-1\n"}}]
```

x	x <sup>-1</sup>	g(x <sup>-1</sup> )	g(x)	g(x) <sup>-1</sup>
6	6	0	0	0
3	9	3	3	3
5	7	1	5	1
8	4	4	2	4
11	1	1	5	1
6	6	0	0	0

Detenidamente compare las columnas tercera y quinta, ¿tiene alguna observación que hacer al respecto?, ¿cuál?

De esta forma concluimos esta tercera sección. Lo invitamos a leer la siguiente sección si necesita alguna explicación más detallada sobre los comandos de *Mathematica* utilizados en estas primeras tres secciones. En caso contrario vaya directamente al capítulo 2.

## 1.4 Principales comandos de *Mathematica* empleados

Si usted desea saber más sobre como usar los comandos (o funciones) de *Mathematica* empleados a lo largo de este capítulo, escriba '?' seguido por el nombre del comando. A continuación se listan algunos de los principales comandos usados en las diferentes secciones-laboratorio que podrían ser útiles posteriormente.

?Needs

?SwitchStructureTo

?ShowPermutation

?Clear

?PermutationMatrix  
?MultiplyPermutations  
?Mode  
?Textual  
?Random  
?Symmetric  
?ShowGroupOrders  
?ClosedQ  
?DirectProduct  
?Closure  
?LeftCoset  
?RightCoset  
?QuotientGroup  
?FormMorphoid  
?PreservesQ  
?MorphismQ  
?Kernel  
?Image



## Capítulo 2

# Acción de un grupo sobre un conjunto

### 2.1 Preliminares

En esta sección recordaremos algunas definiciones básicas y fijaremos la notación utilizada en el resto de estas notas. También se mencionan algunos resultados elementales que serán usados más adelante. Al lector que no esté familiarizado con alguno de estos conceptos le recomendamos consultar una obra general sobre álgebra abstracta, como por ejemplo [5] o [7].

El conjunto de los enteros no negativos lo denotaremos  $\mathbb{N}$ . Si  $n \in \mathbb{N}$  entonces  $\mathbb{N}_n = \{i \in \mathbb{N} : 1 \leq i \leq n\} = \{1, 2, \dots, n\}$ . Al número de elementos de un conjunto (finito)  $A$  lo denotaremos  $|A|$ .

Si  $H$  es un subgrupo de un grupo  $G$ , las *coclases izquierdas* de  $H$  son los conjuntos  $aH = \{ah : h \in H\}$ , con  $a \in G$ . Al conjunto de estas coclases lo denotaremos  $G/H$ . El *índice* (izquierdo) de  $H$  en  $G$  es el cardinal de  $G/H$ , y lo denotaremos  $(G : H)$ . Si  $G$  es finito entonces se cumple que  $|G| = |H| \cdot (G : H)$ . Si  $K$  y  $H$  son subgrupos de  $G$  y  $K \subset H$  entonces  $(G : K) = (G : H)(H : K)$ .  $H$  es un subgrupo *normal* de  $G$  si  $aHa^{-1} = H$  para todo  $a \in G$ . En este caso  $G/H$  tiene una estructura natural de grupo con la operación  $(aH)(bH) = (ab)H$ . Si  $H$  es un subgrupo de  $G$ , el subgrupo  $N(H) = \{g \in G : gHg^{-1} = H\}$  se denomina *normalizador* de  $H$  y tiene la propiedad de ser el mayor subgrupo de  $G$  en el cual  $H$  es normal. El elemento identidad de un grupo  $G$  será denotado por lo general con la letra  $e$ , o bien  $e_G$  si es necesario identificar al grupo.

Si  $G$  y  $K$  son grupos, una aplicación  $f : G \rightarrow K$  es un *homomorfismo* si

$f(ab) = f(a)f(b)$  para todo  $a, b \in G$ . Un homomorfismo se dice que es un *monomorfismo* si es inyectivo, un *epimorfismo* si es sobre y un *isomorfismo* si es biyectivo. Si existe un isomorfismo entre  $G$  y  $K$  escribiremos  $G \approx K$ . El *núcleo* o *kernel* de un homomorfismo  $f : G \rightarrow K$  se define como  $\ker(f) = \{g \in G : f(g) = e_K\}$  y es siempre un subgrupo normal de  $G$ . Además  $\ker(f) = \{e\}$  si y sólo si  $f$  es un monomorfismo. Si  $f : G \rightarrow K$  es un epimorfismo entonces  $G/\ker(f) \approx K$ . Si  $H$  y  $K$  son subgrupos de  $G$  y  $H \subset N(K)$  entonces  $HK = KH$  es un subgrupo y se tiene que  $H/(H \cap K) \approx HK/K$ .

Las biyecciones de un conjunto  $A$  sobre sí mismo, con la composición como operación, forman un grupo que llamaremos *grupo de permutaciones de  $A$*  o *grupo simétrico sobre  $A$*  y denotaremos  $S(A)$  o  $S_A$ . En particular  $S_n$  denotará el grupo de permutaciones del conjunto  $\mathbb{N}_n = \{1, 2, \dots, n\}$ . Si  $a_1, a_2, \dots, a_k$  son elementos distintos de  $\mathbb{N}_n$  entonces el *ciclo*  $\sigma = (a_1, a_2, \dots, a_k)$  se define como la permutación de  $\mathbb{N}_n$  tal que  $\sigma(a_i) = a_{i+1}$  para  $i = 1, \dots, k-1$ ,  $\sigma(a_k) = a_1$  y que deja fijo cualquier otro elemento. Cada elemento de  $S_n$  se puede representar como un producto de ciclos disjuntos, de manera única excepto por el orden (ya que los ciclos sin elementos comunes conmutan).

## 2.2 Acción de grupos

**Definición 2.1.** Sea  $G$  un grupo,  $e$  su elemento identidad y  $A$  un conjunto. Una *acción* de  $G$  sobre  $A$  es una aplicación  $\phi : G \times A \rightarrow A$  tal que:

1.  $\phi(e, x) = x, \quad \forall x \in A$ .
2.  $\phi(g, \phi(h, x)) = \phi(gh, x), \quad \forall g, h \in G, \forall x \in A$ .

Se acostumbra simplificar la notación escribiendo  $gx$  en lugar de  $\phi(g, x)$ . Entonces las condiciones 1 y 2 pueden reformularse así:

1.  $ex = x, \quad \forall x \in A$ .
2.  $g(hx) = (gh)x, \quad \forall g, h \in G, \forall x \in A$ .

Cuando se está en presencia de esta situación se dice que  $G$  *actúa* (por la izquierda) sobre  $A$ , y también que  $A$  es un  *$G$ -conjunto*.

Dada una acción de  $G$  sobre  $A$  es posible definir una relación de equivalencia  $\sim$  en  $A$  del siguiente modo:

$$x \sim y \text{ si existe } g \in G \text{ tal que } y = gx$$

La condición 1 nos asegura que  $\sim$  es reflexiva. También es transitiva pues si  $x \sim y$  e  $y \sim z$  entonces existen elementos  $g, h \in G$  tales que  $y = gx$ ,  $z = hy$  de donde  $z = h(gx) = (hg)x$  y por lo tanto  $x \sim z$ . Finalmente,  $\sim$  es simétrica pues si  $y = gx$  y  $h = g^{-1}$  es el elemento inverso de  $g$  en  $G$  entonces  $hy = h(gx) = (hg)x = ex = x$ .

**Definición 2.2.** Las clases de equivalencia determinadas por la relación  $\sim$  se llaman *órbitas*.

La órbita de un elemento  $x \in A$  es igual al conjunto  $Gx = \{gx : g \in G\}$ , que también denotaremos  $\text{orb}(x)$  o sencillamente  $\bar{x}$ . El conjunto  $A$  es la unión disjunta de todas las órbitas.

Al conjunto cociente de  $A$  por la relación  $\sim$  (es decir al conjunto de todas las órbitas) lo denotaremos  $A/\sim$  o más simplemente  $\bar{A}$ .

La acción de  $G$  sobre  $A$  es *transitiva* si cualquier par de elementos de  $A$  son equivalentes, es decir si dados  $x, y \in A$  existe  $g \in G$  tal que  $y = gx$ . En este caso hay una sola órbita, el propio conjunto  $A$ .

**Ejercicio 2.1.** Sea  $A = \mathbb{R}^2$  el plano cartesiano y  $G$  el conjunto de las rotaciones alrededor del origen. Con la composición como operación,  $G$  es un grupo. Si  $g \in G$  y  $P \in A$  definamos  $gP$  como el resultado de aplicar la rotación  $g$  al punto  $P$ . Verifique que ésta es una acción de  $G$  sobre  $A$ . ¿Cuáles son las órbitas?

**Ejercicio 2.2.** Sea  $A = \mathbb{R}^2$  el plano cartesiano y  $G$  el conjunto de todos los movimientos rígidos de  $A$ , que forman grupo con la composición. Si  $g \in G$  y  $P \in A$  definamos  $gP$  como el resultado de aplicar  $g$  al punto  $P$ . Verifique que ésta es una acción transitiva de  $G$  sobre  $A$ .

**Ejercicio 2.3.** Sea  $G$  un grupo cualquiera. Pruebe que la propia operación binaria de  $G$ , como aplicación de  $G \times G$  en  $G$ , constituye una acción transitiva de  $G$  sobre sí mismo. Esta acción es llamada *traslación*.

**Ejercicio 2.4.** Sea  $G$  un grupo cualquiera y  $A = 2^G$  el conjunto potencia de  $G$  (es decir la familia de todos los subconjuntos de  $G$ ). Pruebe que

$$gX = \{gx : x \in X\}, \quad g \in G, \quad X \subset G,$$

define una acción de  $G$  sobre  $A$ . Si  $H$  es un subgrupo de  $G$ , muestre que la acción anterior puede restringirse a una acción de  $G$  sobre el conjunto de las coclases izquierdas de  $H$ .

**Ejercicio 2.5.** Sea  $G$  un grupo cualquiera. Pruebe que  $\phi : G \times G \rightarrow G$  definida mediante  $\phi(g, x) = gxg^{-1}$  es una acción de  $G$  sobre sí mismo. A esta acción se le llama *conjugación*, y a las órbitas *clases conjugadas*.

**Ejercicio 2.6.** Por analogía con el ejercicio anterior defina una acción de conjugación de un grupo  $G$  sobre su conjunto potencia. Muestre que esta acción puede restringirse a una acción de  $G$  sobre el conjunto de todos sus subgrupos.

**Proposición 2.1.** Sea  $G$  un grupo que actúa sobre un conjunto  $A$ . Para cada  $g \in G$  definamos una función  $g^* : A \rightarrow A$  mediante  $g^*(x) = gx$ ,  $\forall x \in A$ . Entonces  $g^* \in S_A$  y la aplicación  $\theta : G \rightarrow S_A$  que a cada  $g \in G$  le hace corresponder  $g^*$  es un homomorfismo de grupos,

*Demostración.* Si  $e$  es el elemento identidad de  $G$  entonces obviamente  $e^*$  es  $\text{Id}_A$ , la aplicación identidad en  $A$ . Además si  $g, h \in G$  y  $x \in A$  entonces  $(gh)^*(x) = (gh)x = g(hx) = g^*(h^*(x)) = (g^* \circ h^*)(x)$ . En otras palabras,  $(gh)^* = g^* \circ h^*$ . Si  $h = g^{-1}$  es el elemento inverso de  $g$  en  $G$  se tiene que  $g^* \circ h^* = h^* \circ g^* = e^* = \text{Id}_A$ , y por lo tanto  $h^*$  es la aplicación inversa de  $g^*$ . De aquí resulta en particular que  $g^*$  es una biyección de  $A$  en  $A$ , es decir un elemento del grupo  $S(A)$ . La aplicación  $\theta : G \rightarrow S_A$  que a cada  $g \in G$  le hace corresponder  $g^*$  es un homomorfismo de grupos, ya que  $\theta(gh) = (gh)^* = g^* \circ h^* = \theta(g) \circ \theta(h)$ .  $\square$

Al homomorfismo  $\theta$  de la Proposición anterior le llamaremos *homomorfismo inducido* por la acción de  $G$  sobre  $A$ . Diremos que una acción es *efectiva* si su homomorfismo inducido es inyectivo, En este caso el grupo  $G$  puede identificarse con un subgrupo de  $S_A$ .

**Ejercicio 2.7.** Sean  $A$  un conjunto,  $f : A \rightarrow A$  una función tal que  $f^n = \text{Id}_A$  y  $G = \{e, g, g^2, \dots, g^{n-1}\}$  un grupo cíclico de orden  $n$ . Pruebe que existe una única acción de  $G$  sobre  $A$  tal que  $g^* = f$ .

**Ejercicio 2.8.** Dado un homomorfismo  $\varphi : G \rightarrow S(A)$  pruebe que existe una única acción de  $G$  sobre  $A$  cuyo homomorfismo inducido es  $\varphi$ .

**Ejercicio 2.9.** Sea  $A$  el conjunto de vértices de un polígono regular de  $n$  lados y  $D_n$  el grupo de movimientos rígidos que dejan el polígono invariante ( $D_n$  tiene  $2n$  elementos:  $n$  rotaciones y  $n$  simetrías axiales). Pruebe que si  $n \geq 3$  entonces  $D_n$  es isomorfo a un subgrupo de  $S_n$ .

**Ejercicio 2.10.** Considere la acción de un grupo  $G$  por traslación sobre sí mismo (vea el Ejercicio 2.3), Pruebe que es efectiva, y deduzca el Teorema de Cayley: *Todo grupo es isomorfo a un subgrupo de un grupo de permutaciones.*

**Ejercicio 2.11.** Sea  $G$  un grupo y  $\phi$  la conjugación definida en el Ejercicio 2.5, Pruebe que si  $g \in G$  entonces  $g^*$  es un automorfismo de  $G$ . Caracterice el núcleo del homomorfismo inducido.

**Definición 2.3.** El *estabilizador* de un elemento  $x \in A$  es el conjunto  $G_x$  de elementos de  $G$  que dejan fijo a  $x$ . En otras palabras:

$$G_x = \{g \in G : gx = x\}.$$

Es claro que  $G_x$  es un subgrupo de  $G$ , ya que si  $g, h \in G_x$  entonces  $gx = hx = x$ , de donde

$$(gh^{-1})x = (gh^{-1})hx = (gh^{-1}h)x = gx = x$$

y por lo tanto  $gh^{-1} \in G_x$ .

**Ejercicio 2.12.** Si  $G$  actúa sobre  $A$ ,  $g \in G$  y  $x \in A$  pruebe que  $G_{gx} = gG_xg^{-1}$  (en particular, los estabilizadores de elementos de una misma órbita son subgrupos conjugados).

Si  $G$  actúa sobre sí mismo por conjugación y  $x \in G$  entonces  $G_x$  es el subgrupo formado por los  $g \in G$  tales que  $gxg^{-1} = x$ , o sea por los elementos que conmutan con  $x$ . Este subgrupo es conocido como el *centralizador* de  $x$  y se denota  $C(x)$ . También recibe el nombre de *normalizador* de  $x$  (notación:  $N(x)$ ). La intersección de todos los centralizadores está formada por los elementos que conmutan con todos los demás. Este subgrupo se denomina *centro* de  $G$  y lo denotaremos  $Z(G)$ .

Si consideramos la acción de  $G$  por conjugación sobre la familia de todos sus subconjuntos, el estabilizador de  $H \subset G$  es un subgrupo de  $G$  llamado el *normalizador* de  $H$ , y denotado  $N(H)$ .

**Ejercicio 2.13.** Pruebe que si  $H$  es un subgrupo de  $G$  entonces  $N(H)$  es el mayor subgrupo de  $G$  en el cual  $H$  es normal.

**Proposición 2.2.** Si el grupo  $G$  actúa sobre el conjunto  $A$  y  $x$  es un elemento cualquiera de  $A$ , entonces existe una biyección entre la órbita de  $x$  y el conjunto de las coclases izquierdas de  $G_x$ .

*Demostración.* Sea  $G/G_x$  el conjunto de las coclases izquierdas de  $G_x$ . Definamos una función  $f : G/G_x \rightarrow \text{orb}(x)$  mediante  $f(hG_x) = hx$ . La función  $f$  está bien definida, ya que si  $kG_x = hG_x$  entonces  $k = hg$ , para algún  $g \in G_x$ . y por tanto  $kx = (hg)x = h(gx) = hx$ . Obviamente  $f$  es sobre. y también es inyectiva pues si  $f(h_1G_x) = f(h_2G_x)$  entonces  $h_1x = h_2x$  y  $h_2^{-1}h_1x = x$ , de donde  $h_2^{-1}h_1 \in G_x$  y  $h_1G_x = h_2G_x$ .  $\square$

Los dos corolarios siguientes son inmediatos.

**Corolario 2.3.** *Si  $G$  actúa sobre  $A$ ,  $x \in A$  y  $G_x$  tiene índice finito ( $G : G_x$ ) entonces*

$$|\bar{x}| = (G : G_x).$$

**Corolario 2.4.** *Si  $G$  es finito y actúa sobre  $A$  entonces para cualquier  $x \in A$  se tiene*

$$|\bar{x}| = \frac{|G|}{|G_x|}.$$

**Proposición 2.5 (Ecuación de clases).** *Sea  $G$  un grupo finito que actúa por conjugación sobre sí mismo. Sea  $S$  un sistema de representantes distintos de las clases conjugadas (es decir un conjunto que tiene exactamente un elemento de cada clase conjugada). Entonces*

$$|G| = \sum_{x \in S} (G : G_x).$$

*Si  $S'$  es un sistema de representantes distintos de las clases conjugadas que constan de más de un elemento, entonces*

$$|G| = |Z(G)| + \sum_{x \in S'} (G : G_x).$$

*Demostración.* La primera igualdad es inmediata, ya que cada sumando  $(G : G_x)$  en el miembro derecho representa el número de elementos de una órbita. La segunda igualdad se obtiene observando que las órbitas unitarias son las de la forma  $\{z\}$ , con  $z \in Z(G)$ . Por lo tanto su contribución total a la sumatoria en la primera igualdad es  $|Z(G)|$ .  $\square$

## 2.3 Algunas aplicaciones

### 2.3.1 Teorema de Cauchy

**Teorema 2.6.** *Sea  $G$  un grupo finito y  $p$  un divisor primo de  $|G|$ . Entonces  $G$  tiene un subgrupo de  $p$  elementos.*

*Demostración.* (según McKay, [8])

Sea  $A = \{(x_1, x_2, \dots, x_p) : x_i \in G, x_1 x_2 \cdots x_p = e\}$ . Es claro que  $|A| = |G|^{p-1}$ , ya que para obtener un elemento de  $A$  se pueden escoger arbitrariamente las primeras  $p - 1$  componentes, luego de lo cual la última queda

determinada como el inverso del producto de las  $p - 1$  anteriores. Sea ahora  $C = \{e, \sigma, \sigma^2, \dots, \sigma^{p-1}\}$  un grupo cíclico con  $p$  elementos y hagámoslo actuar sobre  $A$  de manera tal que

$$\sigma(x_1, x_2, \dots, x_p) = (x_2, x_3, \dots, x_p, x_1)$$

(cf. Ejercicio 2.7). Como  $C$  no tiene subgrupos propios, el número de elementos de cada órbita solamente puede ser 1 o  $p$ . Si una órbita contiene una sola  $p$ -upla  $x$  entonces, al ser  $x$  invariante por rotaciones, todas sus componentes deben ser iguales, es decir, debe ser de la forma  $x = (a, a, \dots, a)$  con  $a^p = e$ . Sea  $r$  el número de estas órbitas unitarias, y sea  $s$  el número de órbitas con  $p$  elementos. Entonces  $|A| = |G|^{p-1} = r + sp$ , y como  $p$  divide a  $|G|$  concluimos que  $p|r$ . En particular hay más de una órbita unitaria, y por lo tanto hay algún elemento  $b \neq e$  en  $G$  tal que  $b^p = e$ . El subgrupo generado por  $b$  tiene exactamente  $p$  elementos.  $\square$

### 2.3.2 Teoremas de Sylow

Sea  $p$  un número primo. Un  $p$ -grupo es un grupo finito cuyo orden es una potencia de  $p$ . Un  $p$ -subgrupo de un grupo finito es un subgrupo cuyo orden es una potencia de  $p$ . Un  $p$ -subgrupo de Sylow de un grupo finito  $G$  es un subgrupo cuyo orden es igual a la máxima potencia de  $p$  que divide a  $|G|$ .

**Teorema 2.7.** *Si  $G$  es un grupo finito y  $p$  un divisor primo de  $|G|$  entonces  $G$  contiene un  $p$ -subgrupo de Sylow.*

*Demostración.* Si  $|G| = p$  entonces basta tomar  $H = G$ . Supongamos entonces  $|G| > p$  y procedamos por inducción, suponiendo el resultado verdadero para grupos con menos elementos que  $G$ .

Si  $G$  posee un subgrupo propio  $H$  de índice coprimo con  $p$  entonces, como  $p||G| = |H|(G : H)$ , se deduce que  $p||H|$  y por la hipótesis inductiva  $H$  debe contener un  $p$ -subgrupo de Sylow  $K$ . Este  $K$  debe ser también  $p$ -subgrupo de Sylow de  $G$ , ya que la mayor potencia de  $p$  que divide a  $|H|$  es la misma que divide a  $|G|$ .

Por el contrario si todos los subgrupos propios de  $G$  tienen índice divisible entre  $p$  entonces por la Proposición 2.5 tenemos

$$|G| = |Z(G)| + \sum_{x \in S'} (G : G_x),$$

y como todos los términos  $(G : G_x)$  que aparecen en la sumatoria son múltiplos de  $p$ , al igual que  $|G|$ , concluimos que  $p$  divide a  $|Z(G)|$ . El Teorema 2.6

nos asegura ahora la existencia de un subgrupo  $H$  de  $Z(G)$  de orden  $p$ . Este  $H$  es claramente un subgrupo normal de  $G$ . Consideremos ahora  $G/H$ . Si  $p^k$  es la mayor potencia de  $p$  que divide a  $|G|$  entonces  $p^{k-1}$  divide a  $|G/H|$ , y por la hipótesis inductiva existe un  $p$ -subgrupo de Sylow  $K'$  de  $G/H$ . Si  $f : G \rightarrow G/H$  es el epimorfismo canónico (es decir la aplicación definida por  $f(a) = aH$ ) entonces  $K = f^{-1}(K')$  es un subgrupo de  $G$  que contiene a  $H$ , y como la restricción de  $f$  a  $K$  es un epimorfismo sobre  $K'$  con núcleo  $H$ , se tiene que  $K/H \approx K'$  y por tanto  $|K| = |H| \cdot |K/H| = p \cdot p^{k-1} = p^k$ .  $\square$

**Teorema 2.8.** *Sea  $G$  un grupo finito y  $p$  un divisor primo de  $|G|$ . Entonces:*

- (a) *Todo  $p$ -subgrupo de  $G$  está contenido en un  $p$ -subgrupo de Sylow.*
- (b) *Todos los  $p$ -subgrupos de Sylow de  $G$  son conjugados.*
- (c) *El número de  $p$ -subgrupos de Sylow de  $G$  es congruente con 1 módulo  $p$ .*

*Demostración.*

(a) Sea  $H$  un  $p$ -subgrupo de  $G$  de orden  $p^k > 1$ . Sea  $A$  el conjunto de los  $p$ -subgrupos de Sylow de  $G$  y consideremos la acción de  $G$  sobre  $A$  por conjugación. Como el estabilizador de cualquier  $L \in A$  contiene a  $L$ , el número de elementos de cualquier órbita debe ser coprimo con  $p$ . Ahora bien, si  $\mathcal{O}$  es una de las órbitas, consideremos la acción de  $H$  (por conjugación) sobre ella. Como el índice de cualquier subgrupo propio de  $H$  es una potencia de  $p$ , alguna de las órbitas de  $\mathcal{O}$  bajo  $H$  debe consistir de un único elemento  $K$ . Entonces  $H$  debe estar contenido en el normalizador de  $K$ . De aquí se sigue que  $HK$  es un subgrupo y además  $H/(H \cap K) \approx HK/K$ . De aquí se deduce que  $|HK|$  es una potencia de  $p$ , pero como  $K \subset HK$  y  $G$  no contiene  $p$ -grupos de orden mayor que  $K$ , debe ser  $HK = K$ . Por lo tanto  $H \subset HK = K$ .

(b) Dados dos  $p$ -subgrupos de Sylow  $H$  y  $L$ , el razonamiento anterior aplicado a  $H$  y la órbita de  $L$  muestra que existe un subgrupo  $K$  conjugado de  $L$  tal que  $H \subset K$ . Pero como  $H$  y  $K$  son del mismo orden resulta  $H = K$ , o sea que  $H$  es conjugado de  $L$ .

(c) Consideremos la acción por conjugación de un  $p$ -subgrupo de Sylow  $H$  sobre el conjunto  $A$  de todos los  $p$ -subgrupos de Sylow. Si  $\{K\}$  es una órbita con un solo elemento, el argumento que usamos para la parte (a) muestra que  $H = K$ . Por lo tanto hay una única órbita unitaria, a saber  $\{H\}$ , y las demás tienen un número de elementos múltiplo de  $p$ .  $\square$

## 2.4 Problemas

- 2.1 Sea  $G$  un grupo y  $H$  un subgrupo, y considere la acción de  $G$  sobre el conjunto  $G/H$  de las coclases izquierdas de  $H$ , definida mediante  $g(aH) = (ga)H$ . Sea  $\theta$  el homomorfismo inducido por esta acción. Pruebe que  $\ker(\theta)$  es el mayor subgrupo normal de  $G$  contenido en  $H$ . Deduzca que si  $|G| \nmid (G : H)!$  entonces  $H$  contiene un subgrupo normal no trivial.
- 2.2 Sea  $G$  un grupo finito y  $H$  un subgrupo de índice igual al menor divisor primo de  $|G|$ . Pruebe que  $H$  es normal (en particular, todo subgrupo de índice 2 es normal).
- 2.3 Pruebe que todo grupo de orden 99 contiene un subgrupo normal de orden 11.
- 2.4 El número de particiones de un conjunto de  $n$  elementos en exactamente  $k$  clases (disjuntas y no vacías) se denomina *número de Stirling de segunda especie* y lo denotaremos  $\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$ . Pruebe que si  $p$  es primo y  $1 < k < p$  entonces  $p \mid \left\{ \begin{smallmatrix} p \\ k \end{smallmatrix} \right\}$ .
- 2.5 El número de permutaciones de un conjunto de  $n$  elementos que se descomponen en producto de exactamente  $k$  ciclos disjuntos se denomina *número de Stirling de primera especie* y lo denotaremos  $\left[ \begin{smallmatrix} n \\ k \end{smallmatrix} \right]$ . Pruebe que si  $p$  es primo y  $1 < k < p$  entonces  $p \mid \left[ \begin{smallmatrix} p \\ k \end{smallmatrix} \right]$ .
- 2.6 Pruebe que todo grupo de orden  $pq$ , donde  $p$  y  $q$  son primos,  $p < q$  y  $p \nmid (q - 1)$ , es necesariamente abeliano.



## Capítulo 3

# Enumeración bajo acción de grupos

### Introducción

A veces al contar configuraciones es deseable considerar algunas de ellas como equivalentes. Por ejemplo supongamos que queremos pintar un cubo con dos colores, digamos rojo y azul, pintando cada cara de un solo color. Como hay dos colores posibles para cada cara y el cubo tiene seis caras, llegamos a la conclusión de que existen  $2^6 = 64$  maneras de pintar el cubo. Pero este resultado supone que las seis caras del cubo pueden distinguirse unas de otras, como en efecto sucede si están numeradas o si el cubo está montado en una posición fija que nos permita reconocer cada cara por su orientación. Si en cambio podemos mover el cubo y rotarlo y las caras no se distinguen entre sí excepto por su color, entonces el número de coloraciones se reduce bastante. En efecto, las seis coloraciones que tienen una cara roja y las otras cinco azules se vuelven indistinguibles. Asimismo las  $\binom{6}{2} = 15$  coloraciones con dos caras rojas y las demás azules se reducen a solamente dos: una en la cual las dos caras rojas son adyacentes y otra en la cual esas caras son opuestas. Prosiguiendo con este análisis se ve fácilmente que hay solamente diez coloraciones *esencialmente diferentes*.

**Ejercicio 3.1.** Completar el análisis de las coloraciones de las caras del cubo con dos colores.

El problema anterior se complica considerablemente si aumentamos el número de colores disponibles o si sustituimos el cubo por, digamos, un dodecaedro regular. En la teoría de grafos se presentan numerosos problemas

de este tipo, por ejemplo el de determinar el número de grafos no isomorfos con un número dado de vértices y aristas. En las ciencias naturales también se presentan situaciones semejantes, por ejemplo en la enumeración de compuestos químicos.

En general, supongamos que un grupo de permutaciones actúa sobre un conjunto de configuraciones y que consideramos a dos configuraciones *equivalentes* cuando una permutación del grupo lleva una en la otra. En este capítulo estudiaremos el problema de contar el número de configuraciones *no equivalentes*. Los resultados fundamentales de esta teoría fueron obtenidos en primer lugar por J. H. Redfield (ver [14]), pero pasaron desapercibidos durante varios años hasta que Polya (ver [13]), de Bruijn y otros los redescubrieron y enriquecieron.

### 3.1 El Lema de Cauchy-Frobenius-Burnside

Sea  $G$  un grupo que actúa sobre un conjunto  $A$ . Si  $g \in G$  entonces al subconjunto de  $A$  formado por los puntos fijos de  $g^*$  lo denotaremos  $A_g$ . En símbolos:

$$A_g = \{x \in A : gx = x\}.$$

Observemos que  $x \in A_g$  si y sólo si  $g \in G_x$ .

**Proposición 3.1.** *Sea  $G$  un grupo finito que actúa sobre un conjunto  $A$ , y sea  $Y$  un grupo aditivo. Supongamos que  $p : A \rightarrow Y$  es una función tal que  $p(gx) = p(x)$ ,  $\forall g \in G, \forall x \in A$  (en otras palabras,  $p$  es constante en cada órbita). Sea  $\bar{p} : \bar{A} \rightarrow Y$  la única función tal que  $\bar{p}(\bar{x}) = p(x)$ ,  $\forall x \in A$ . Entonces:*

$$\sum_{X \in \bar{A}} \bar{p}(X) = \frac{1}{|G|} \sum_{g \in G} \sum_{x \in A_g} p(x).$$

*Demostración.*

$$\begin{aligned} \sum_{g \in G} \sum_{x \in A_g} p(x) &= \sum_{x \in A} \sum_{g \in G_x} p(x) = \sum_{x \in A} |G_x| p(x) = \sum_{X \in \bar{A}} \sum_{x \in X} |G_x| p(x) \\ &= \sum_{X \in \bar{A}} \sum_{x \in X} (|G|/|\bar{x}|) \bar{p}(\bar{x}) = |G| \sum_{X \in \bar{A}} \bar{p}(X). \end{aligned}$$

□

**Lema 3.2 (Cauchy-Frobenius-Burnside).** *Si  $G$  es un grupo finito que actúa sobre un conjunto  $A$  entonces el número de órbitas de  $A$  viene dado por:*

$$|\bar{A}| = \frac{1}{|G|} \sum_{g \in G} |A_g|$$

*Demostración.* Basta tomar en la Proposición anterior  $Y = \mathbb{Z}$  (los enteros) y como  $p : A \rightarrow Y$  la función constante  $p(x) = 1, \forall x \in A$ .  $\square$

## 3.2 La Acción de Polya

**Definición 3.1.** Sean  $D$  y  $C$  dos conjuntos,  $G$  un subgrupo de  $S(D)$  y  $A = C^D$  el conjunto de todas las funciones de  $D$  en  $C$ . La *acción de Polya* de  $G$  sobre  $A$  es la acción  $\phi : G \times A \rightarrow A$  definida por  $\phi(g, f) = f \circ g^{-1}$ .

**Ejercicio 3.2.** Verifique que  $\phi$  es realmente una acción.

Si pensamos en los elementos de  $D$  como objetos a colorear y en los elementos de  $C$  como colores, entonces los elementos de  $A$  son las diferentes *coloraciones* o maneras de pintar los elementos de  $D$ , cada uno con un solo color. En lo sucesivo utilizaremos este lenguaje.

**Proposición 3.3.** *Sean  $D$  y  $C$  dos conjuntos finitos y  $G$  un subgrupo del grupo de permutaciones de  $D$ . Consideremos la acción de Polya de  $G$  sobre  $A = C^D$ . Entonces el número de órbitas viene dado por*

$$\frac{1}{|G|} \sum_{g \in G} |C|^{\lambda(g)}$$

siendo  $\lambda(g)$  el número de factores en la descomposición de  $g$  en producto de ciclos disjuntos.

*Demostración.* Por el Lema (3.2) el número de órbitas es  $(1/|G|) \sum_{g \in G} |A_g|$ . Ahora bien,  $A_g$  está constituido por todas las coloraciones  $f : D \rightarrow C$  tales que  $f \circ g^{-1} = f$ . Afirmamos que  $f \circ g^{-1} = f$  si y sólo si  $f$  asigna el mismo color a todos los elementos de cada ciclo de  $g$ . En efecto, supongamos que  $f \circ g^{-1} = f$  y sea  $(d_1, \dots, d_t)$  un ciclo de  $g$ . Entonces  $g(d_i) = d_{i+1}$  para  $1 \leq i < t$  y  $g(d_t) = d_1$ . En consecuencia,  $f(d_i) = f(g^{-1}(d_{i+1})) = f(d_{i+1})$  para  $1 \leq i < t$  y  $f(d_t) = f(g^{-1}(d_1)) = f(d_1)$ . Recíprocamente si  $f$  es una coloración constante en cada ciclo de  $g$ , puesto que el elemento  $g^{-1}(d)$  está en el mismo ciclo que  $d$  para todo  $d \in D$ , tendremos que  $f(g^{-1}(d)) = f(d)$ . Esto significa que hay tantos elementos en  $A_g$  como formas de asignar un color de  $C$  a cada ciclo de  $g$ , y este número es precisamente  $|C|^{\lambda(g)}$ .  $\square$

### 3.2.1 Ejemplo: coloración del cubo con $r$ colores

El resultado recién demostrado nos permite resolver con toda generalidad el problema planteado al principio de este capítulo. El grupo de rotaciones del cubo está constituido por 24 rotaciones, que clasificaremos en 5 tipos:

1. La identidad.
2. Rotaciones de  $120^\circ$  y  $240^\circ$  alrededor de las diagonales del cubo. Como hay cuatro diagonales, hay 8 rotaciones de este tipo.
3. Rotaciones de  $90^\circ$  y  $270^\circ$  alrededor de los 3 ejes que pasan por los centros de caras opuestas del cubo. Son 6 rotaciones.
4. Rotaciones de  $180^\circ$  alrededor de los mismos ejes que las del tipo anterior. Son 3 rotaciones.
5. Rotaciones de  $180^\circ$  alrededor de los ejes que pasan por los puntos medios de aristas opuestas. Hay 6 rotaciones de este tipo.

Cada una de estas rotaciones induce una permutación de las seis caras del cubo que se descompone en ciclos de la manera siguiente:

1. La identidad se descompone en seis 1-ciclos.
2. Estas rotaciones se descomponen en dos 3-ciclos cada una.
3. Estas, en dos 1-ciclos y un 4-ciclo (total: tres ciclos cada una.)
4. Estas, en dos 1-ciclos y dos 2-ciclos. (total: cuatro ciclos cada una.)
5. Estas, en tres 2-ciclos cada una.

La información anterior nos permite afirmar que el número de coloraciones del cubo, no equivalentes por rotación, viene dado por la fórmula

$$\frac{1}{24}(r^6 + 8r^2 + 6r^3 + 3r^4 + 6r^3) = \frac{1}{24}r^2(r^4 + 3r^2 + 12r + 8),$$

la cual nos permite construir la tabla siguiente:

número de colores	número de coloraciones no equivalentes
1	1
2	10
3	57
4	240
5	800
6	2226
7	5390
8	11712
9	23355
10	43450
20	2690800
30	30490050

### 3.2.2 Aplicación: identidades con números de Stirling

Tomemos  $D = \mathbb{N}_n$  y  $C = \mathbb{N}_k$ . Entonces  $|C^D| = k^n$ . Usaremos la convención  $0^0 = 1$ , de modo que la igualdad anterior es válida incluso si  $n$ ,  $k$  o ambos son nulos. Si  $x$  es un número real y  $n \in \mathbb{N}$  entonces definimos  $x^n = x(x-1) \cdots (x-n+1)$  (*factorial inferior*) y  $x^{\bar{n}} = x(x+1) \cdots (x+n-1)$  (*factorial superior*). Por convención  $x^0 = x^{\bar{0}} = 1$ . Denotaremos mediante  $\text{Part}(n, k)$  el conjunto de todas las particiones de  $\mathbb{N}_n$  con exactamente  $k$  bloques (disjuntos y no vacíos) y mediante  $\text{Perm}(n, k)$  el conjunto de todas las permutaciones de  $\mathbb{N}_n$  que se descomponen en producto de exactamente  $k$  ciclos disjuntos. Definamos el *número de Stirling sin signo de primera especie*  $\left[ \begin{smallmatrix} n \\ k \end{smallmatrix} \right]$  como  $|\text{Perm}(n, k)|$  (para otra definición combinatoria equivalente vea [12]) y el *número de Stirling de segunda especie*  $\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$  como  $|\text{Part}(n, k)|$ . Entonces se tiene:

**Proposición 3.4.**

$$x^{\bar{n}} = \sum_{k=0}^n \left[ \begin{smallmatrix} n \\ k \end{smallmatrix} \right] x^k. \tag{3.1}$$

*Demostración.* (Según [10]) Sea  $x \in \mathbb{N}$  y consideremos la acción de Polya de  $S_n$  sobre  $C^D$ . Dos coloraciones son equivalentes si y sólo si cada color es utilizado el mismo número de veces en cada una de ellas. Por lo tanto las órbitas pueden ponerse en correspondencia con las combinaciones con repetición de  $x$  colores tomados de  $n$  en  $n$ , que son  $\binom{x+n-1}{n}$ . Por otra parte las coloraciones que quedan fijas bajo una permutación  $g \in S_n$  son aquellas

que asignan el mismo color a los elementos de cada ciclo de  $g$ . Si denotamos mediante  $\lambda(g)$  el número de ciclos de  $g$  entonces estas coloraciones son  $x^{\lambda(g)}$ . Aplicando el Lema de Cauchy-Frobenius-Burnside resulta entonces que:

$$\binom{x+n-1}{n} = \frac{1}{n!} \sum_{g \in S_n} x^{\lambda(g)}.$$

Pero para cada  $k$  desde 0 hasta  $n$  hay  $\begin{bmatrix} n \\ k \end{bmatrix}$  permutaciones  $g \in S_n$  con  $\lambda(g) = k$ . Agrupando los términos correspondientes en la igualdad anterior y multiplicando ambos miembros por  $n!$  obtenemos (3.1), que queda así probada para todo  $x$  entero. Por lo tanto, en virtud del Teorema de Identidad de Polinomios, (3.1) es una identidad polinomial.  $\square$

**Ejercicio 3.3.** Probar que

$$x^n = \sum_{k=0}^n (-1)^{n-k} \begin{bmatrix} n \\ k \end{bmatrix} x^k.$$

El Ejercicio precedente nos permite expresar los polinomios  $x^n$  como combinaciones lineales de las potencias de  $x$ , con los números de Stirling de primera especie como coeficientes. A la inversa, las potencias de  $x$  pueden expresarse como combinaciones lineales de los  $x^n$  con los números de Stirling de segunda especie como coeficientes (vea el Problema 2.4).

### 3.3 El Teorema de Polya

**Definición 3.2.**  $G$  un subgrupo de  $S_n$ . El polinomio

$$P_G(x_1, \dots, x_n) = \frac{1}{|G|} \sum_{g \in G} x_1^{\lambda_1(g)} \dots x_n^{\lambda_n(g)}$$

se llama *polinomio indicador de ciclos* de  $G$ .

**Definición 3.3.** Sean  $D = \mathbb{N}_n$  y  $C = \mathbb{N}_r$ . El *peso* de una coloración  $f \in C^D$  es el monomio en las variables  $x_1, \dots, x_r$  dado por

$$p(f) = \prod_{d \in D} x_{f(d)}.$$

**Teorema 3.5 (Polya).** Sean  $D = \mathbb{N}_n$ ,  $C = \mathbb{N}_r$  y  $G$  un subgrupo de  $S_n$ . Consideremos la acción de Polya de  $G$  sobre  $C^D$ . Sean  $\psi_k$ ,  $k = 1, \dots, n$ , las funciones simétricas  $\psi_k(x_1, \dots, x_r) = x_1^k + \dots + x_r^k$ . Entonces

$$\sum_{\bar{f} \in \bar{A}} \bar{p}(\bar{f}) = P_G(\psi_1(x_1, \dots, x_r), \dots, \psi_n(x_1, \dots, x_r)).$$

*Demostración.* Sea  $Y = \mathbb{Q}[x_1, x_2, \dots, x_r]$  el anillo de los polinomios en  $r$  variables con coeficientes racionales. El peso de una coloración es una función  $p : C^D \rightarrow Y$ . Es claro que  $p(f)$  es un monomio de grado total  $n$  y que el exponente de  $x_k$  en  $p(f)$  corresponde al número de puntos de  $D$  pintados con el color  $k$  en la coloración  $f$ . Observemos además que  $p(gf) = p(f)$ , para todo  $g \in G$  y  $f \in C^D$ . En efecto,

$$p(gf) = \prod_{d \in D} x_{gf(d)} = \prod_{d \in D} x_{f(g^{-1}(d))}$$

pero como  $g$  es una biyección de  $D$  en  $D$ , cuando  $d$  toma todos los valores en  $D$  lo mismo hace  $g^{-1}(d)$  y el segundo producto es igual al primero. Esto significa que estamos en condiciones de aplicar la Proposición (3.1) a la acción de Polya de  $G$  sobre  $C^D$ , y obtenemos:

$$\sum_{\bar{f} \in \bar{A}} \bar{p}(\bar{f}) = \frac{1}{|G|} \sum_{g \in G} \sum_{f \in A_g} p(f).$$

Ahora bien, como vimos en la demostración de la Proposición 3.3  $f \in A_g$  si y sólo si  $f$  asigna el mismo color a los elementos de cada ciclo de  $g$ . Por lo tanto si  $g \in G$  se descompone en  $\lambda$  ciclos  $c_1, \dots, c_\lambda$  de longitudes  $a_1, \dots, a_\lambda$  y si  $f$  asigna el color  $i_j$  a los elementos del ciclo  $c_j$  entonces  $p(f)$  será de la forma  $x_{i_1}^{a_1} \cdots x_{i_\lambda}^{a_\lambda}$ . Más aún,  $p$  establece una correspondencia biyectiva entre los monomios del tipo antedicho y las coloraciones  $f \in A_g$ . Por consiguiente:

$$\begin{aligned} \sum_{f \in A_g} p(f) &= \sum x_{i_1}^{a_1} \cdots x_{i_\lambda}^{a_\lambda} \\ &= (x_1^{a_1} + \cdots + x_r^{a_1})(x_1^{a_2} + \cdots + x_r^{a_2}) \cdots (x_1^{a_\lambda} + \cdots + x_r^{a_\lambda}) \\ &= \psi_{a_1} \psi_{a_2} \cdots \psi_{a_\lambda} = \prod_{k=1}^n \psi_k(x_1, \dots, x_r)^{\lambda_k(g)}, \end{aligned}$$

ya que cada  $\psi_k$  aparece en el producto  $\psi_{a_1} \psi_{a_2} \cdots \psi_{a_\lambda}$  tantas veces como ciclos de longitud  $k$  aparezcan en la descomposición de  $g$ , es decir  $\lambda_k(g)$ . La demostración se concluye sumando para  $g \in G$ .  $\square$

**Observaciones y comentarios:**

1. Poniendo en el Teorema de Polya  $x_1 = x_2 = \cdots = x_r = 1$  se obtiene como caso particular la proposición (3.3).
2. Para otros enfoques de la Teoría de Polya vea [3, 9, 15].

**Ejemplo 3.1.** El análisis de las rotaciones del cubo realizado en el ejemplo anterior nos permite escribir el polinomio indicador de ciclos de inmediato:

$$P_G(x_1, x_2, x_3, x_4, x_5, x_6) = \frac{1}{24}(x_1^6 + 8x_3^2 + 6x_1^2x_4 + 3x_1^2x_2^2 + 6x_2^3)$$

Supongamos que se va a colorear el cubo con dos colores, digamos rojo y azul. Calculando  $P_G(\psi_1, \dots, \psi_6)$  con  $\psi_1 = x + y$ ,  $\psi_2 = x^2 + y^2$ ,  $\psi_3 = x^3 + y^3$ ,  $\psi_4 = x^4 + y^4$ , resulta el polinomio

$$x^6 + x^5y + 2x^4y^2 + 2x^3y^3 + 2x^2y^4 + xy^5 + y^6$$

(hemos usado  $x, y$  en lugar de  $x_1, x_2$  para aligerar la notación) El término  $2x^3y^3$  por ejemplo, nos dice que hay dos coloraciones con tres caras pintadas de rojo y las otras tres de azul.

### 3.4 Enumeración de grafos no isomorfos

A continuación haremos un resumen de las definiciones y conceptos básicos que necesitaremos de la teoría de grafos. El lector no familiarizado con esta teoría puede consultar [1] o [4]. Un *grafo* es un par  $G = (V, A)$  donde  $V$  es un conjunto finito no vacío y  $A$  es un conjunto de pares (desordenados) de elementos distintos de  $V$ . Los elementos de  $V$  se llaman *vértices* y los de  $A$  *aristas*. Se llama *extremos* de una arista a los dos vértices que le pertenecen. Dos vértices distintos son *adyacentes* si son extremos de una misma arista. Un vértice y una arista son *incidentes* si el primero es un extremo de la segunda. El *grado* de un vértice  $v \in V$  es el número de aristas incidentes con  $v$ . Lo denotaremos mediante  $\rho(v)$ . El grafo  $G = (V, A)$  es *completo* si todos sus pares de vértices distintos son adyacentes. La notación  $K_n$  se usa para designar el grafo completo de  $n$  vértices. Es claro que un grafo de  $n$  vértices es completo si y sólo si tiene  $n(n-1)/2$  aristas. Dos grafos son *isomorfos* si existe una aplicación biyectiva entre sus conjuntos de vértices que preserve la relación de adyacencia.

La teoría de Polya puede ser usada para determinar el número de grafos no isomorfos con un número de vértices y aristas dado. En efecto, a cada coloración de las aristas del grafo completo  $K_n$  con dos colores, digamos rojo y azul, le podemos hacer corresponder el grafo cuyos vértices son los mismos de  $K_n$  y cuyas aristas son las coloreadas de rojo. Es claro que cualquier grafo de  $n$  vértices puede ser obtenido de esta manera a partir de una bicoloración de  $K_n$ . Observemos sin embargo que la correspondencia descripta no es inyectiva, ya que coloraciones diferentes pueden dar lugar

a grafos isomorfos. Entonces dos coloraciones de  $K_n$  darán lugar a grafos isomorfos cuando ambas difieran en una permutación de las aristas de  $K_n$  inducida por una permutación de sus vértices. En símbolos, si  $K_n = (V, A)$  y  $f : A \rightarrow (r, a)$  es una coloración de  $A$  con dos colores  $r$  y  $a$ , el grafo correspondiente a  $f$  es  $G_f = (V, A_f)$  siendo  $A_f = \{e \in A : f(e) = r\}$ . Dos coloraciones  $f$  y  $g$  dan lugar a grafos isomorfos si existe una permutación  $\sigma$  de  $V$  tal que  $\{u, v\} \in A_f$  si y sólo si  $\{\sigma(u), \sigma(v)\} \in A_g$ . Esto equivale a decir que  $f(\{u, v\}) = g(\{\sigma(u), \sigma(v)\})$ ,  $\forall u, v \in V$ , o más simplemente  $f = g \circ \bar{\sigma}$  siendo  $\bar{\sigma}$  la permutación de  $A$  inducida por  $\sigma$ , a saber  $\bar{\sigma}(\{u, v\}) = \{\sigma(u), \sigma(v)\}$ ,  $\forall u, v \in V, u \neq v$ .

Sea  $G$  el grupo de las permutaciones de  $A$  inducidas por permutaciones de  $V$ . Entonces la acción de Polya de  $G$  sobre las bicoloraciones de  $K_n$  induce una relación de equivalencia bajo la cual dos coloraciones son equivalentes si y sólo si les corresponden grafos isomorfos. El número de grafos no isomorfos de  $n$  vértices será entonces igual al número de órbitas, y puede obtenerse a partir del lema de Cauchy-Frobenius-Burnside. El teorema de Polya permite, más aún, calcular el número de grafos no isomorfos con  $n$  vértices y  $m$  aristas. Pero para aplicar el teorema de Polya es necesario conocer como se descompone en ciclos cada elemento del grupo  $G$ . Sea  $\sigma$  una permutación del conjunto de vértices  $V$  con  $\lambda_i$  ciclos de longitud  $i$ , para  $i = 1, 2, \dots, n$ . Sea  $\alpha = \{u, v\}$  una arista de  $K_n$ . Consideraremos varios casos:

1) Si  $u$  y  $v$  pertenecen a un mismo ciclo de  $\sigma$  de longitud impar  $2k + 1$  entonces la arista  $\alpha$  pertenece a un ciclo de  $\bar{\sigma}$  de longitud  $2k + 1$ , a saber  $\{u, v\}, \{\sigma(u), \sigma(v)\}, \dots, \{\sigma^{2k}(u), \sigma^{2k}(v)\}$ . Puesto que las  $\binom{2k+1}{2} = (2k+1)k$  aristas cuyos extremos son vértices del ciclo  $\sigma$  se agrupan en ciclos disjuntos de longitud  $2k + 1$  concluimos que hay  $k$  de estos ciclos. Por lo tanto cada ciclo de longitud impar  $2k + 1$  en  $\sigma$  da origen a  $k$  ciclos de longitud  $2k + 1$  en  $\bar{\sigma}$ .

2) Si  $u$  y  $v$  pertenecen a un mismo ciclo de  $\sigma$  de longitud par  $2k$  entonces la arista  $\alpha$  puede estar en un ciclo de  $\bar{\sigma}$  de longitud  $2k$  o bien en uno de longitud  $k$ . Por ejemplo si consideramos el ciclo  $(1\ 2\ 3\ 4)$  entonces las aristas  $\{1, 2\}, \{2, 3\}, \{3, 4\}$  y  $\{1, 4\}$  pertenecen al 4-ciclo  $(\{1, 2\}\ \{2, 3\}\ \{3, 4\}\ \{1, 4\})$ , pero las aristas  $\{1, 3\}$  y  $\{2, 4\}$  pertenecen al 2-ciclo  $(\{1, 3\}\ \{2, 4\})$ . En general es fácil ver que el  $2k$ -ciclo  $(v_1, \dots, v_{2k})$  dará origen a un  $k$ -ciclo  $(\{v_1, v_{k+1}\}\ \{v_2, v_{k+2}\}\ \dots\ \{v_k, v_{2k}\})$  y a  $k - 1$   $2k$ -ciclos.

3) Si  $u$  pertenece a un  $r$ -ciclo de  $\sigma$  y  $v$  a un  $s$ -ciclo entonces la arista  $\{u, v\}$  estará en un ciclo de  $\bar{\sigma}$  de longitud igual al mínimo común múltiplo de  $r$  y  $s$ . En efecto para que se cumpla que  $\{\sigma^t(u), \sigma^t(v)\} = \{u, v\}$  debe ser

$\sigma^t(u) = u$  y  $\sigma^t(v) = v$  (no puede ser  $\sigma^t(u) = v$  y  $\sigma^t(v) = u$  ya que  $u$  y  $v$  están en ciclos disjuntos). Por lo tanto debe cumplirse que  $r|t$  y  $s|t$ , lo cual implica  $\text{m.c.m.}(r, s)|t$ . El número de ciclos disjuntos en los cuales se dividen las  $rs$  aristas con un vértice en cada ciclo será entonces  $rs/\text{m.c.m.}(r, s) = \text{m.c.d.}(r, s)$  (máximo común divisor de  $r$  y  $s$ ).

Como consecuencia del análisis anterior podemos afirmar que en la descomposición de  $\bar{\sigma}$  en producto de ciclos disjuntos tendremos:

1.  $\lambda_r(r-1)/2$   $r$ -ciclos, para cada  $r$  impar entre 1 y  $n$ .
2.  $\lambda_r \frac{r}{2}$ -ciclos y  $\frac{r}{2} - 1$   $r$ -ciclos para cada  $r$  par entre 1 y  $n$ .
3.  $\lambda_r \lambda_s \text{m.c.d.}(r, s)$   $\text{m.c.m.}(r, s)$ -ciclos para cada par de números distintos  $r, s$  entre 1 y  $n$ , y  $r \binom{\lambda_r}{2}$   $r$ -ciclos, para cada  $r$  entre 1 y  $n$  (ya que existen  $\lambda_r \lambda_s$  maneras de escoger un  $r$ -ciclo y un  $s$ -ciclo, si  $r \neq s$ , y  $\binom{\lambda_r}{2}$  maneras de escoger un par de  $r$ -ciclos distintos)

Si aplicamos el Teorema de Polya (3.5) para dos colores, dando a la variable  $x_1$  el valor 1 y recordando que el número de permutaciones con  $\lambda_i$  ciclos de longitud  $i$  para  $i = 1, \dots, n$  es

$$K(\lambda_1, \dots, \lambda_n) = \frac{n!}{1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n} \lambda_1! \lambda_2! \dots \lambda_n!}$$

resulta la siguiente:

**Proposición 3.6.** *El número de grafos no isomorfos con  $n$  vértices y  $m$  aristas es igual al coeficiente de  $x^m$  en el polinomio que se obtiene sumando, para cada solución de la ecuación diofántica  $1\lambda_1 + 2\lambda_2 + \dots + n\lambda_n = n$  un término de la forma:*

$$\frac{1}{n!} K(\lambda_1, \dots, \lambda_n) [w_1^{0\lambda_1} w_3^{1\lambda_3} \dots] [(w_1 w_2^0)^{\lambda_2} (w_2 w_4^1)^{\lambda_4} (w_3 w_6^2)^{\lambda_6} \dots] \\ [w_1^{1\binom{\lambda_1}{2}} w_2^{2\binom{\lambda_2}{2}} w_3^{3\binom{\lambda_3}{2}} \dots] \prod_{r \neq s} w_{\text{mcm}(r,s)}^{\lambda_r \lambda_s \text{mcd}(r,s)}$$

siendo  $w_k$  el polinomio  $1 + x^k$ .

Excepto para pequeños valores de  $n$  el cálculo manual del número de grafos no isomorfos utilizando la última Proposición es imposible, y se requiere la ayuda del computador. En [11] puede verse una tabla obtenida de esta manera. que muestra el número de grafos no isomorfos con  $n$  vértices y  $m$  aristas para  $1 \leq n \leq 11$ .

### 3.5 Problemas

- 3.1 ¿De cuántas maneras se puede pintar un tablero cuadrado de  $2 \times 2$  con  $r$  colores, pintando cada casilla de un color y considerando equivalentes las coloraciones que difieren en una rotación del tablero?
- 3.2 ¿De cuántas maneras se pueden marcar con una X ocho de las dieciséis casillas de un tablero cuadrado de  $4 \times 4$ , considerando equivalentes las configuraciones que se obtienen unas de otras por rotaciones o simetrías del cuadrado?
- 3.3 Determine el número de coloraciones de las caras de un poliedro regular (tetraedro, cubo, octaedro, dodecaedro e icosaedro) con  $r$  colores, no equivalentes por rotaciones.

3.4 Pruebe que

$$x^n = \sum_{k=0}^n \binom{n}{k} x^k$$

- 3.5 Calcule el número de grafos no isomorfos con 5 vértices y  $m$  aristas, para  $m = 0, 1, \dots, 10$ , usando la Proposición 3.6.
- 3.6 (N. G. de Bruijn, [2])

Sea  $G$  un subgrupo de  $S(D)$  y  $H$  un subgrupo de  $S(C)$ . Considere la acción de  $G \times H$  sobre  $A = C^D$  definida así:

$$(g, h)f = h \circ f \circ g^{-1} \quad \forall (g, h) \in G \times H, \forall f \in A$$

Pruebe que si  $C$  y  $D$  son finitos y  $|D| = n$  entonces el número de órbitas viene dado por la fórmula siguiente:

$$|\overline{A}| = \frac{1}{|G||H|} \sum_{g \in G} \sum_{h \in H} \prod_{k=1}^n \left( \sum_{i|k} i \lambda_i(h) \right)^{\lambda_k(g)}$$

siendo  $\lambda_i(\sigma)$  el número de ciclos de longitud  $i$  en la descomposición de la permutación  $\sigma$  en producto de ciclos disjuntos.



## Apéndice A

# Soluciones a los Problemas

### Capítulo 2

2.1 Sea  $K = \ker(\theta)$ . Entonces  $g \in K$  si y sólo si  $gaH = aH$  para todo  $a \in G$ . Si esto ocurre, poniendo  $a = e$  se deduce que  $g \in H$  y por lo tanto  $K \subset H$ . Además  $K$  es normal por ser el núcleo de un homomorfismo. Si  $J$  es cualquier otro subgrupo normal de  $G$  contenido en  $H$  y  $j \in J$ , entonces para cualquier  $a \in G$  se tiene  $a^{-1}ja \in J \subset H$  y por lo tanto  $a^{-1}jaH = H$  y  $jaH = aH$ , lo que prueba que  $j \in K$ . Por tanto  $J \subset K$ .

Ahora bien, si  $\theta$  fuese un monomorfismo entonces  $G$  sería isomorfo a un subgrupo de  $S(G/H)$  y por lo tanto  $|G|$  debería dividir a  $|S(G/H)| = (G : H)!$ . Si esto no ocurre concluimos que  $K \neq \{e\}$  y por lo tanto  $H$  contiene un subgrupo normal no trivial.

2.2 Consideremos la misma acción del problema anterior y sea  $K$  el núcleo del homomorfismo inducido. Entonces  $(G : K) = |G/K|$  es un múltiplo de  $|G : H| = p$  y debe dividir a  $|G|$  y a  $|S_p| = p!$ . Pero como  $p$  es el menor divisor primo de  $|G|$  esto sólo puede suceder si  $(G : K) = p$ , de donde se concluye que  $K = H$ .

2.3 Un grupo de orden 99 debe contener un subgrupo  $H$  de orden 11 por el Teorema de Sylow. Pero como  $99 \nmid 9!$ , por el ejercicio anterior  $H$  debe ser normal.

2.4 Sea  $A$  el conjunto de las particiones de  $\{1, 2, \dots, p\}$  en  $k$  clases. Sea  $\sigma = (1, 2, \dots, n) \in S_p$  y  $G$  el grupo cíclico de orden  $p$  generado por  $\sigma$ . Hay una acción natural de  $G$  sobre  $A$ , a saber la dada por

$$g\{B_1, B_2, \dots, B_k\} = \{g(B_1), g(B_2), \dots, g(B_k)\}.$$

El número de elementos de una órbita sólo puede ser 1 o  $p$ . Pero una órbita unitaria debería tener todos los bloques del mismo tamaño, lo cual es imposible porque en ese caso  $k$  sería un divisor de  $p$ . Por lo tanto  $p \parallel |A| = \left\{ \begin{smallmatrix} p \\ k \end{smallmatrix} \right\}$ .

- 2.5 Proceda por analogía con el problema precedente, definiendo una acción de un grupo cíclico de orden  $p$  sobre el conjunto de las permutaciones de  $\{1, 2, \dots, p\}$  que se descomponen en producto de  $k$  ciclos disjuntos.
- 2.6 por el Teorema de Sylow sabemos que existe un subgrupo  $H$  de orden  $p$ . Si  $H$  no fuese normal entonces su clase conjugada tendría  $(G : N(H)) = (G : H) = q$  elementos. Pero como  $p \nmid (q - 1)$  esto no puede ser. Por lo tanto  $H$  es normal y es el único  $p$ -subgrupo de Sylow de  $G$ . Por lo tanto  $H$  contiene todos los elementos de orden  $p$  que hay en  $G$  (exactamente  $p - 1$ ). Sea  $h$  uno de ellos. Como  $H \subset C(h)$ , el centralizador  $C(h)$  debe ser  $H$  o  $G$ . Pero en el primer caso la clase conjugada de  $h$  tendría  $q$  elementos, todos ellos de orden  $p$ , lo cual es imposible pues  $q > p$ . Por lo tanto  $C(h) = G$  y se sigue que  $H \subset Z(G)$ . De aquí y del hecho de que  $G/H$  es cíclico se deduce fácilmente que  $G$  es abeliano.

### Capítulo 3

- 3.1 En total hay  $r^4$  coloraciones. Las invariantes bajo una rotación de  $90^\circ$  son únicamente aquellas que asignan un mismo color a las cuatro casillas. Son por lo tanto  $r$ . Las invariantes bajo la rotación de  $180^\circ$  son las que asignan el mismo color a las dos casillas de cada diagonal, y son  $r^2$ . De acuerdo con (3.3) resulta entonces que el número de coloraciones no equivalentes por rotaciones es  $(r^4 + 2r + r^2)/4$ .
- 3.2 El número total de configuraciones es  $\binom{16}{8} = 12870$ . El grupo de simetrías del cuadrado  $D_4$  tiene 8 elementos. Si fijamos un sistema de coordenadas con origen en el centro del tablero y ejes paralelos a los lados entonces las configuraciones invariantes bajo una rotación de  $90^\circ$  quedan caracterizadas por las dos cruces que deben tener en el primer cuadrante. Por lo tanto son  $\binom{4}{2} = 6$ . Lo mismo puede decirse para la rotación de  $270^\circ$ . Las invariantes bajo la rotación de  $180^\circ$  quedan caracterizadas por la posición de las cuatro cruces que deben tener en el semiplano superior. Por lo tanto son  $\binom{8}{4} = 70$ . Un razonamiento análogo se aplica a las simetrías de ejes  $Ox$  y  $Oy$ . Las configuraciones invariantes bajo la simetría de eje  $y = x$  quedan caracterizadas por el

número de cruces que tengan en la diagonal (que puede ser 0, 2 o 4) y por la disposición de la mitad de las cruces restantes en el semiplano  $y > x$ . Por lo tanto su número es  $\binom{6}{4} + \binom{4}{2}\binom{6}{3} + \binom{6}{2} = 150$ . Lo mismo puede decirse para la simetría de eje  $y = -x$ . En definitiva, aplicando el Lema de Cauchy-Frobenius-Burnside el número buscado resulta ser:

$$\frac{1}{8}(12870 + 2 \cdot 6 + 3 \cdot 70 + 2 \cdot 150) = 1674$$

3.3 De modo similar a lo hecho en el texto para el cubo se obtienen los siguientes resultados para los demás poliedros regulares:

$$\begin{aligned} \text{tetraedro:} & \quad (r^4 + 11r^2)/12 \\ \text{octaedro:} & \quad (r^8 + 17r^4 + 6r^2)/24 \\ \text{dodecaedro:} & \quad (r^{12} + 15r^6 + 44r^4)/60 \\ \text{icosaedro:} & \quad (r^{20} + 15r^{10} + 20r^8 + 24r^4)/60 \end{aligned}$$

3.4 Supongamos que  $x \in \mathbb{N}$ . El miembro izquierdo es igual al número de coloraciones de  $\mathbb{N}_n$  con  $x$  colores. Pero estas coloraciones se pueden clasificar según el número de colores efectivamente utilizados. Las que emplean exactamente  $k$  colores se pueden obtener particionando  $\mathbb{N}_n$  en  $k$  clases y asignando un color diferente a cada clase, lo cual puede hacerse de  $x^k$  maneras. Sumando en  $k$  se obtiene que la identidad a probar se cumple para todo  $x \in \mathbb{N}$  y por tanto, en virtud del Teorema de Identidad de Polinomios, es una identidad polinomial.

3.5

$$\begin{aligned} w_1^{10} + 10w_1^4w_2^3 + 20w_1^2w_3^3 + 30w_2w_4^2 + 15w_1^2w_2^4 + 20w_1w_3w_6 + 24w_5^2 \\ = 1 + x + 2x^2 + 4x^3 + 6x^4 + 6x^5 + 6x^6 + 4x^7 + 2x^8 + x^9 + x^{10}. \end{aligned}$$

3.6 De acuerdo con el Lema de Cauchy-Frobenius-Burnside el número de órbitas es:

$$\frac{1}{|G||H|} \sum_{g \in G} \sum_{h \in H} |\{f \in C^D : h \circ f \circ g^{-1} = f\}|$$

Ahora bien, supongamos que  $f \in C^D$ ,  $g \in G$ ,  $h \in H$ ,  $h \circ f \circ g^{-1} = f$ , que  $d \in D$  pertenezca a un  $k$ -ciclo de  $g$  y que su imagen  $c = f(d)$  esté en un  $i$ -ciclo de  $h$ . Entonces:

$$h^k(c) = h^k(f(d)) = (h^k \circ f \circ g^{-k})(g^k(d)) = f(d) = c$$

y por lo tanto  $i$  divide a  $k$ . Recíprocamente, dados  $g \in G$  y  $h \in H$  si seleccionamos un representante en cada  $k$ -ciclo de  $g$  (para  $k = 1, \dots, |D|$ )

y le hacemos corresponder un elemento de  $C$  que pertenezca a un ciclo de  $h$  cuya longitud divida a  $k$ , se ve sin dificultad que la correspondencia puede ser extendida de modo único a una función  $f \in C^D$  tal que  $h \circ f \circ g^{-1} = f$ . Puesto que al representante de un  $k$ -ciclo de  $g$  se le pueden asignar según este criterio  $\sum_{i|k} i\lambda_i(h)$  colores, resulta que:

$$|\{f \in C^D : h \circ f \circ g^{-1} = f\}| = \left( \sum_{i|k} i\lambda_i(h) \right)^{\lambda_k(g)}$$

con lo cual queda probado el resultado.

# Bibliografía

- [1] Bollobas, B., *Graph theory*, Springer-Verlag, New York-Berlin-Heidelberg-Tokyo, 1979.
- [2] Bruijn, N. G. de, *Generalization of Polya's fundamental theorem in enumeration combinatorial analysis*, Indagationes Math. **21** (1959), 59–69.
- [3] González, G., *Función de Möbius y teoría de Polya*, Notas de Matemática y computación Num. 2, F.E.C., Universidad del Zulia, Maracaibo, Venezuela, 1987.
- [4] Harary, F. *Graph theory*, Addison-Wesley, Reading, 1969.
- [5] Herstein, I. N., *Algebra moderna*, Trillas, México, 1976 (traducción del original *Topics in algebra*, Blaisdell, Waltham, 1964.)
- [6] Hibbard, A. C., Levasseur, K. M., *Exploring Abstract Algebra with Mathematica*, Springer-Verlag, New York, 1988.
- [7] Lang, S. *Algebra*, Addison-Wesley, Reading, 1965.
- [8] McKay, J. H. *Another Proof of Cauchy's Group Theorem*, American Mathematical Monthly, **66**(2), (1959), p. 119.
- [9] Merris, R., *Polya's Counting Theorem Via Tensors*, American Mathematical Monthly, **88**(3) (1981), 179–185.
- [10] Nieto, J. H., *Números de Stirling y Acción de Grupos*, Ciencia **8**(2) (2000), 188–190.
- [11] Nieto, J. H., *Teoría Combinatoria*, EdiLUZ, Maracaibo, 1996.
- [12] Nieto, J. H., *Extremos en sucesiones*, Divulg. Mat., **2**(1), 1994, 5–9.

- [13] Polya, G., *Kombinatorische Anzahlbestimmungen für Gruppen, Graphen, und chemische Verbindungen*, Acta Mathematica **68** (1937), 145–254.
- [14] Redfield, J. H., *The theory of group-reduced distributions*, American Journal of Mathematics **49** (1927), 433–455.
- [15] Rodríguez, J., *Polya theory and tableaux*, Notas de Matemática No. 67, Universidad de los Andes, Mérida, Venezuela 1984.

# Índice de Materias

- acción, 18
  - de Polyá, 29
  - efectiva, 20
  - transitiva, 19
- Bruijn, N. G. de, 28, 37
- Burnside, W., 29
- Cauchy, A. L., 22, 29
- Cayley, A., 7, 20
- centralizador, 21
- centro, 21
- clase conjugada, 20
- clausura, 9
- coloraciones, 29
- conjugación, 20
- ecuación de clases, 22
- estabilizador, 21
- Frobenius, G., 29
- $G$ -conjunto, 18
- grafo, 34
- grupo, 6
  - abeliano, 7
  - cociente, 11
  - conmutativo, 7
  - de permutaciones, 18
  - simétrico, 18
- homomorfismo, 12
- Mathematica*, 1
- McKay, J. H., 22
- normalizador, 21
- números de Stirling, 25, 31
- órbita, 19
- orden, 8
- permutación, 3
- peso, 32
- polinomio indicador de ciclos, 32
- Polyá, G., 28
- producto directo, 11
- Redfield, J. H., 28
- simetría, 2
- Stirling, J.
  - números de, 25, 31
- subgrupo, 8
  - de Sylow, 23
  - normal, 12, 17
- Sylow, L., 23
- Tabla de Cayley, 7
- Teorema
  - de Cauchy, 22
  - de Cayley, 20
  - de Polyá, 32
  - de Sylow, 23, 24
- traslación, 19