NOTAS DE TRABAJO, 12

TEORÍA DE GRUPOS

Estructura de grupos finitos

Pascual Jara Martínez

Departamento de Álgebra. Universidad de Granada

Granada, 2001–2021

Primera redacción: 2001.
Segunda redacción: Octubre 2014.
Tercera redacción: Octubre 2017.
Cuarta redacción: Septiembre 2020.

Introducción general

La teoría elemental de grupos trata de la definición y propiedades de grupos y de las consecuencias elementales de estas propiedades sobre la estructura de los grupos (Teorema de Lagrange), así como del estudio de construcciones sencillas de grupos. Trata también de mostrar los primeros ejemplos de grupos y construcciones sobre los mismos, en especial el cociente y el producto directo de una familia de grupos.

Mediante el uso de grupos como operadores o transformaciones de conjuntos (geométricos o no), obtenemos una gran variedad de ejemplos de grupos. Citaremos entre otros los grupos simétricos y subgrupos de ellos como los diédricos, alternados, etc., y los grupos de matrices que pueden ser vistos como grupos de movimientos de espacios vectoriales o de espacios afines.

Dejamos para un segundo bloque el estudio de las acciones de un grupo sobre un conjunto, los teoremas de Sylow y los grupos solubles y grupos simples. Asimismo, en este curso, haremos un estudio en profundidad de la estructura de grupos finitos de orden pequeño, utilizando productos semidirectos; y utilizaremos el algoritmo de Todd–Coxeter para identificar cada grupo finito con un subgrupo de un grupo de permutaciones.

En esta segunda parte dedicada a la teoría de grupos hacemos una aproximación al estudio de su estructura. La primera parte trata de resultados generales sobre series de composición y grupos solubles, y se prueba el Teorema de Abel sobre la simplicidad del grupo alternado A_n para n mayor o igual que 5. Pasamos posteriormente al estudio de grupos como grupos de operadores; una consecuencia directa de esta teoría son los teoremas de Sylow. La tercera parte la dedicamos al estudio y clasificación de algunos grupos finitos. la herramienta fundamental para este estudio son los teoremas de Sylow. Además, teniendo en cuenta que los grupos estudiados son de orden pequeño, el producto semidirecto de grupos nos ayuda enormemente en la descripción de la mayor parte de los grupos estudiados.

Índice general

Introducción general I

I Estructura de grupos finitos 1

Introducción 3

I Grupos 5
1 Definición de grupo . . . 5
2 Grupos simétricos I . . . 13
3 Subgrupos . . . 16
4 Ejercicios propuestos . . . 20

II Homomorfismos de grupos 37
5 Homomorfismos de grupos . . . 37
6 Subgrupos normales y grupos cocientes . . . 41
7 Grupos cíclicos . . . 54
8 Grupos simétricos II . . . 58
9 Ejercicio propuestos . . . 62

III Presentación de un grupo 87
10 Presentaciones de un grupo. . . . 87
11 Ejercicios propuestos . . . 110

IV Grupos libres 129
12 Grupos libres . . . 129
13 Ejercicios propuestos . . . 140

V Series de composición. Grupos solubles. Teorema de Abel 147
14 Series de composición . . . 147
15 Teorema de Schreier . . . 150
16 Grupos solubles . . . 152
17 Subgrupo derivado . . . 154
18 Teorema de Abel . . . 157
19 Ejercicios Propuestos . . . 160

VI Producto directo de grupos 161
20 Producto directo finito de grupos . . . 161
21 Producto directo de una familia de grupos . . . 163
22 Producto directo interno . . . 166

23 Ejercicios Propuestos 169

VII Grupos de operadores. Teoremas de Sylow 173
24 Grupos de operadores 174
25 Teoremas de Sylow 187
26 Ejercicios propuestos 199

VIII Producto semidirecto de grupos 217
27 Productos semidirectos 218
28 Aplicaciones. Ejemplos de grupos 222

Bibliography 243

Index 245

Parte I

Estructura de grupos finitos

Introducción

ESCRIBIR!!!!!

Capítulo I

Grupos

1 Definición de grupo 5
2 Grupos simétricos I 13
3 Subgrupos 16
4 Ejercicios propuestos 20

Introducción.

1. Definición de grupo

Sea G un conjunto, una **operación binaria** en G es una aplicación

$$* : G \times G \longrightarrow G.$$

Cuando $x, y \in G$, el elemento $*(x, y)$ se nota, generalmente, por $x * y$, ó por xy.
Ya conocemos ejemplos de operaciones binarias;

Ejemplos. 1.1.
(1) En el conjunto $\mathbb{N}$ de los números naturales la suma y el producto son operaciones binarias. También son operaciones binarias en $\mathbb{Z}$ la suma y el producto de números enteros.
(2) Si X es un conjunto, en $\mathscr{P}(X)$, la unión y la intersección son ejemplos de operaciones binarias.
(3) En el conjunto $\mathbb{R}$ de los números reales la suma y el producto son operaciones binarias.

Un **monoide** es un conjunto no vacío G junto con una operación binaria $*$ que verifica las siguientes propiedades:

(I) **Propiedad asociativa.** Para todo $a, b, c \in G$ se verifica: $a * (b * c) = (a * b) * c$.
(II) **Existencia de elemento neutro.** Existe un elemento $e \in G$ tal que para todo $a \in G$ se verifica: $a * e = a = e * a$.

Lema. 1.2.
Sea $(G,*)$ *un monoide, existe un único elemento neutro en* G*.*

DEMOSTRACIÓN. Supongamos que e y e_1 son elementos neutros, entonces tenemos: $e = e * e_1 = e_1$. □

En este caso podemos escribir también que $(G,*,e)$ es un monoide.

Ejemplo. 1.3.
(1) El conjunto $\mathbb{N}$ de los números naturales con la suma y con elemento neutro 0 es un monoide.
(2) El conjunto $\mathbb{N}$ de los números naturales con el producto y con elemento neutro 1 es un monoide.
(3) También son monoides $(\mathbb{Z},+,0)$ y $(\mathbb{Z},\times,1)$.
(4) Si X es un conjunto, entonces $(\mathscr{P}(X),\cup,\varnothing)$ y $(\mathscr{P}(X),\cap,X)$ son monoides.
(5) También son monoides $(\mathbb{R},+,0)$ y $(\mathbb{R},\times,1)$.

Un **grupo** es un conjunto no vacío G junto con una operación binaria $*$ que verifica las siguientes propiedades:

(I) **Propiedad asociativa.** Para todo $a,b,c \in G$ se verifica: $a*(b*c) = (a*b)*c$.
(II) **Existencia de elemento neutro.** Existe un elemento $e \in G$ tal que para todo $a \in G$ se verifica: $a*e = a = e*a$.
(III) **Existencia de elemento simétrico.** Para todo $a \in G$ existe un elemento $a' \in G$ verificando: $a*a' = e = a'*a$.

Según lo anterior, si G es un conjunto no vacío y $*$ es una operación binaria, verificando las propiedades anteriores, diremos que el par $(G,*)$ es un **grupo**, para así hacer referencia a la operación que se está considerando en G. Cuando la operación $*$ se da por supuesta, y no es necesario destacarla, se dice simplemente que G es un grupo.
Una palabra en cuanto a notación, para $a,b \in G$, recordemos que el elemento $a*b$ se representa también por ab.

Otra propiedad que puede verificar una operación binaria $*$ en un conjunto G es la siguiente:
(IV) **Propiedad conmutativa.** Para todos $a,b \in G$ se verifica: $a*b = b*a$.

Si $(G,*)$ es un grupo que verifica la propiedad (IV), se dice que $(G,*)$ es un **grupo conmutativo** ó un **grupo abeliano**.

Lema. 1.4.
Sea G *un grupo, se verifican las siguientes propiedades:*
(1) Existe un único elemento neutro.
(2) Para cada elemento de G *existe un único elemento simétrico.*

DEMOSTRACIÓN. (1). Ver Lema (1.2.).
(2). Supongamos que b y c son elementos simétricos de $a \in G$, tenemos:

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c.$$

□

Ejemplos. 1.5.
(1) El conjunto $\mathbb{Z}$ de los números enteros con la operación suma es un grupo abeliano.
(2) El conjunto $\mathbb{R}^\times$ de los números reales no nulos con la operación producto es un grupo abeliano.
(3) El conjunto $\mathbb{R}^+$ de los números reales positivos no nulos con la operación producto es un grupo abeliano.
(4) El conjunto $\mathrm{GL}_2(\mathbb{R})$ de las matrices del tipo

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R})$$

verificando $ad - bc \neq 0$, con la operación producto de matrices, es un grupo no abeliano.
(5) Si X es un conjunto (no vacío), y llamamos $S(X)$ al conjunto de todas las aplicaciones biyectivas de X en X, entonces $S(X)$, junto con la composición de aplicaciones, es un grupo no abeliano.
(6) Si G es un grupo y X un conjunto, en el conjunto, $\mathrm{Apl}(X, G) = G^X$, de las aplicaciones de X a G, se define una operación binaria: $(f * g)(x) = f(x) * g(x)$, para cada $x \in X$. Entonces G^X es un grupo con esta operación. El simétrico de $f \in G^X$ es f', definido $f'(x) = f(x)'$, para cada $x \in X$. Observa que si $X = \emptyset$, entonces $G^X = G^\emptyset = \{\emptyset\}$ es un conjunto unitario,y si $X = \{1, 2\}$, entonces G^X se identifica con el producto cartesiano $G \times G$.

Lema. 1.6.
Sea G un conjunto no vacío con una operación binaria $\star$. La operación $\star$ verifica las propiedades (I), (II) *y* (III) *de la definición de grupo si, y sólo si, verifica las propiedades* (I), (II*b*) *y* (III*b*), *donde:*

(II*b*) ***Existencia de elemento neutro a la derecha.*** *Existe un elemento $e \in G$ tal que para todo $a \in G$ se verifica: $a * e = a$.*
(III*b*) ***Existencia de elemento simétrico a la derecha.*** *Para todo $a \in G$ existe un elemento $a' \in G$ verificando: $a * a' = e$.*

DEMOSTRACIÓN. (⇒). Es evidente.
(⇐). (I). Se verifica por la hipótesis.
(III). Tenemos que probar que $a'a = e$ para cada $a \in G$, se tiene:

$$\begin{aligned} a'a = (a'a)e &= (a'a)(a'(a')') \\ = ((a'a)a')(a')' &= (a'(aa'))(a')' \\ = (a'e)(a')' &= a'(a')' = e. \end{aligned}$$

(II). Tenemos que probar que $ea = a$ para cada $a \in G$, se tiene:

$$ea = (aa^{-1})a = a(a^{-1}a) = ae = a.$$

□

En los ejemplos de grupos que se va a estudiar las operaciones binarias se notan, usualmente, por "+", ó por "·".

La operación "+" se llama **suma**;

- el elemento neutro se llama **cero** y se representa por 0;
- el elemento simétrico del elemento $a \in G$ se llama **opuesto** de a, y se representa por $-a$.

La operación "·" se llama **producto**;

- el elemento $a \cdot b$, para $a, b \in G$, se representa también por ab;
- el elemento neutro se llama **uno**, y se representa por 1 ó por e;
- el elemento simétrico del elemento $a \in G$ se llama **inverso** de a y se representa por a^{-1}.

Por comodidad utilizaremos como operación el producto, y al elemento neutro lo notaremos por e, aunque en los ejercicios utilicemos 1.

Con los siguientes resultados se tiene más información sobre los inversos y, en general, sobre la aritmética de los grupos.

Lema. 1.7.
Sea G un grupo, y $a, b \in G$ elementos arbitrarios de G, se verifica:
(1) $(a^{-1})^{-1} = a$.
(2) $(ab)^{-1} = b^{-1}a^{-1}$.

DEMOSTRACIÓN. (1). Ya que $a^{-1}a = e$, tenemos que a es el inverso de a^{-1}, luego se tiene $a = (a^{-1})^{-1}$.
(2). Basta considerar el siguiente desarrollo:

$$(ab)(b^{-1}a^{-1}) = ((ab)b^{-1})a^{-1} = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e,$$

entonces se tiene:

$$b^{-1}a^{-1} = (ab)^{-1}.$$

□

Lema. 1.8.
*En todo grupo G se verifica la **propiedad cancelativa**, esto es; para todos $a, b, c \in G$ se tiene que $ac = bc$ implica $a = b$.*

DEMOSTRACIÓN. Supongamos que para $a, b, c \in G$ se verifica $ac = bc$, desarrollando tenemos:

$$a = a(cc^{-1}) = (ac)c^{-1} = (bc)c^{-1} = b(cc^{-1}) = be = b.$$

□

Lema. 1.9.
Sea G un conjunto no vacío en el que existe una operación binaria verificando la propiedad asociativa. Son equivalentes:

(a) G es un grupo.
(b) Para cada par de elementos $a, b \in G$ las ecuaciones $aX = b$ y $Xa = b$ tienen solución en G, esto es; existen elementos c y d de G tales que $ac = b$ y $da = b$.

DEMOSTRACIÓN. (a) ⇒ (b). Si G es un grupo y $a, b \in G$, entonces una solución de $aX = b$ es: $a^{-1}b$, y una solución de $Xa = b$ es: ba^{-1}.
(b) ⇒ (a). Llamamos e_a a una solución de la ecuación $aX = a$, entonces para todo $b \in G$ tenemos que $Xa = b$ tiene una solución, llamémosla x, entonces:

$$be_a = (xa)e_a = x(ae_a) = xa = b,$$

luego e_a es también una solución de la ecuación $bX = b$, y por tanto e_a es un elemento neutro a la derecha. Para simplificar, llamemos e al e_a. Para cada $a \in G$ la ecuación $aX = e$ tiene una solución, luego cada elemento $a \in G$ tiene un inverso a la derecha. Por lo tanto, por el Lema (1.6.), G es un grupo. □

Sea G un grupo, para cada elemento $a \in G$ se define:

(I) $a^0 = e$.
(II) $a^{n+1} = aa^n$, para todo $n \in \mathbb{N}$.
(III) $a^{-m} = (a^m)^{-1}$, para todo $m \in \mathbb{N}$.

Sea G un grupo y $a_1, \ldots, a_n \in G$, definimos $a_1 \cdots a_n$ como cualquier producto de los elementos $a_1, \ldots, a_n$ en no importa qué orden de los paréntesis. Por ejemplo, si $n = 4$, entonces $a_1a_2a_3a_4$ es uno cualquiera de los siguientes productos:

$$((a_1a_2)a_3)a_4; \quad (a_1a_2)(a_3a_4); \quad a_1(a_2(a_3a_4)).$$

Para que esto tenga sentido, es necesario probar el siguiente resultado:

Lema. 1.10.
Sea G un grupo y $a_1, \ldots, a_n \in G$, entonces todos los elementos que pueden definir $a_1 \ldots a_n$ son iguales y para cada $1 \leq r \leq n$, se verifica:

$$(a_1 \cdots a_r)(a_{r+1} \cdots a_n) = a_1 \cdots a_n.$$

DEMOSTRACIÓN. Si $n = 1, 2, 3$, entonces el resultado es cierto. Supongamos que $n > 3$, y que el resultado es cierto para listas de menos de n elementos; entonces se verifica para $1 \leq r < n$:

$$\begin{aligned}(a_1 \cdots a_r)(a_{r+1} \cdots a_n) &= (a_1(a_2 \cdots a_r))(a_{r+1} \cdots a_n) \\ &= a_1((a_2 \cdots a_r)(a_{r+1} \cdots a_n)) \\ &= a_1(a_2 \cdots a_n).\end{aligned}$$

Ahora bien, cualquier elemento que puede definir $a_1 \cdots a_n$ es un producto de la forma

$$(a_1 \cdots a_r)(a_{r+1} \cdots a_n),$$

con $1 \leq r < n$, y por tanto todos ellos son iguales. □

Corolario. 1.11.
Sea G un grupo, $a \in G$ y $n, m \in \mathbb{Z}$, entonces se verifica:
(1) $a^{n+m} = a^n a^m$.
(2) $(a^n)^m = a^{nm}$.

DEMOSTRACIÓN. (1). Si n, $m \in \mathbb{N}$, el resultado es consecuencia del Lema (1.10.). Si $n, m \notin \mathbb{N}$, entonces tenemos:

$$a^{n+m} = (a^{-m-n})^{-1} = (a^{-m}a^{-n})^{-1} = (a^{-n})^{-1}(a^{-m})^{-1} = a^n a^m.$$

Si $n \in \mathbb{N}$, $m \notin \mathbb{N}$, entonces llamamos $h = n + m$; si $h \in \mathbb{N}$, entonces $n = h + (-m)$, y por tanto tenemos

$$a^n = a^{h+(-m)} = a^h a^{-m} = a^h (a^m)^{-1},$$

luego $a^n a^m = a^h = a^{n+m}$; si $h \notin \mathbb{N}$, entonces tenemos $-h + n = -m$, ya que todos son números naturales, se verifica $a^{-m} = a^{-h+n} = a^{-h}a^n$, y por tanto $a^n a^m = a^h = a^{n+m}$.
(2). Si $n, m \in \mathbb{N}$, el resultado es una consecuencia inmediata del Lema (1.10.). Para los demás casos el resultado se sigue del hecho siguiente: para cada $n \in \mathbb{N}$ se verifica $a^{-n} = (a^{-1})^n$; para probar este hecho consideremos la relación:

$$a^n (a^{-1})^n = e,$$

este resultado se obtiene por inducción sobre n aplicando la parte (1) de este Corolario; si $n = 1$ el resultado es cierto; supongamos que $n > 1$ y que el resultado es cierto para todo número natural menor ó igual que n, entonces se verifica:

$$a^{n+1}(a^{-1})^{n+1} = (aa^n)((a^{-1})^n a^{-1}) = a((a^n(a^{-1})^n)a^{-1}) = aa^{-1} = e.$$

□

Como consecuencia de este Corolario, para cada elemento a de un grupo G, y para cualesquiera $n, m \in \mathbb{Z}$ se verifica $a^n a^m = a^m a^n$.

Sea G un grupo, si G tiene un número finito de elementos, entonces G se llama un **grupo finito**, en caso contrario G se llama **grupo infinito**. Cuando G es un grupo finito, se llama **orden** de G al número de elementos de G, y se representa por $|G|$.

Para un grupo finito G la operación binaria se puede representar por medio de una tabla de dos entradas. Los siguientes ejemplos de grupos finitos están dados por las tablas de sus operaciones binarias.

Sea $G = \{0, 1\}$, en G se consideran las operaciones binarias dadas por las tablas:

	0	1
0	0	1
1	1	0

	0	1
0	1	0
1	0	1

Sea $G = \{0, 1, 2\}$, en G se considera la operación binaria dada por la tabla:

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Sea $G = \{0, 1, 2, 3\}$, en G se consideran las operaciones binarias dadas por las tablas:

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Si G_1 y G_2 son grupos, podemos definir en el producto cartesiano $G_1 \times G_2$ una nueva operación:

$$(a_1, a_2) * (b_1, b_2) = (a_1 * b_1, a_2 * b_2)$$

para cada $a_1, a_2 \in G_1$ y $b_1, b_2 \in G_2$.

Lema. 1.12.
Si G_1 y G_2 son grupos, entonces $G_1 \times G_2$ es un grupo, que es abeliano si, y sólo si, G_1 y G_2 son abelianos.

Ver Ejercicio (4.15.).

2. Grupos simétricos I

Dado un conjunto X, el conjunto $S(X) = \{f : X \longrightarrow X \mid f \text{ biyectiva}\}$, junto con la composición, es un grupo. Si el conjunto X es finito, con n elementos, entonces el grupo $S(X)$ se representa por S_n, y se llama el n–ésimo **grupo simétrico**; cada elemento de $S(X)$ se llama una **permutaciones** de X. Ver Ejemplo (1.5.).

Ejemplo. 2.1.
Supongamos que $n = 5$, y que $\sigma \in S_5$ está definido por

$$\sigma(1) = 2,\ \sigma(2) = 3,\ \sigma(3) = 1,\ \sigma(4) = 5,\ \sigma(5) = 4.$$

Para simplificar, representaremos a σ por

$$\sigma = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,1\,5\,4 \end{pmatrix}.$$

Otro elemento de S_5 es

$$\tau = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,4\,5\,1 \end{pmatrix}$$

A partir de aquí podemos calcular los productos $\sigma\tau$ y $\tau\sigma$, los cuales, como podemos comprobar, no son iguales.

$$\tau\sigma = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,4\,5\,1 \end{pmatrix} \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,1\,5\,4 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,4\,2\,1\,5 \end{pmatrix}.$$

$$\sigma\tau = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,1\,5\,4 \end{pmatrix} \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,4\,5\,1 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,1\,5\,4\,2 \end{pmatrix}.$$

Luego, como era de esperar, S_5 no es un grupo abeliano. Tenemos que S_n es un grupo abeliano solamente para $n = 0$, 1 ó 2, para el resto de los números naturales n se tiene que S_n es un grupo no abeliano.

La permutación τ anterior podemos representarla gráficamente de la siguiente forma:

$$(1\,2\,3\,4\,5).$$

A una permutación de este tipo la llamamos **permutación cíclica** ó un **ciclo**. Otro ejemplo de ciclo es la permutación $\tau\sigma$, en este caso tenemos $\tau\sigma = (1\ 3\ 2\ 4)$. Mientras que la permutación σ es el producto de dos ciclos: $\sigma = (1\,2\,3)(4\,5)$.
Una definición más precisa de ciclo es la siguiente: una permutación $\sigma \in S_n$ es un **ciclo** si para cada par de elementos $x, y \in \{1, \ldots, n\}$, tales que $\sigma(x) \neq x$ y $\sigma(y) \neq y$, existe un entero positivo $h \in \mathbb{N}$ tal que $\sigma^h(x) = y$.

3301-02.tex

Si $\sigma \in S_n$ es un ciclo, llamamos **longitud** de σ al número de elementos que mueve.
Dos permutaciones $\sigma, \tau \in S_n$ se llaman **disjuntas** si los elementos que mueve una quedan fijos por la otra, esto es; si $\sigma(x) \neq x$ y $\tau(y) \neq y$, entonces $\tau(x) = x$ y $\sigma(y) = y$ para todos $x, y \in \{1, \ldots, n\}$.

Teorema. 2.2.
Toda permutación $\sigma \in S_n$, distinta de 1, es un producto de ciclos disjuntos de longitud mayor ó igual que 2. Esta descomposición es única salvo en el orden de los factores.

DEMOSTRACIÓN. Dada una permutación $\sigma \neq 1$, en el conjunto $\{1, \ldots, n\}$ definimos la relación:

$$x \mathscr{R} y \text{ si existe } h \in \mathbb{N} \text{ tal que } \sigma^h(x) = y.$$

$\mathscr{R}$ es una relación de equivalencia en $X = \{1, \ldots, n\}$. Dado $x \in X$, debe existir $k \in \mathbb{N}$ tal que $x = \sigma^k(x)$, supongamos que k es el mínimo, no nulo, verificando esta condición. Entonces la clase de equivalencia $[x]$ de x tiene exactamente k elementos y es igual a $[x] = \{x, \sigma(x), \ldots, \sigma^{k-1}(x)\}$. Asociado a $[x]$ definimos entonces el ciclo $\gamma_{[x]} = (x\sigma(x)\ldots\sigma^{k-1}(x))$. Se verifica

$$\gamma_{[x]}(y) = \begin{cases} y & \text{si } y \notin [x] \\ \sigma(y) & \text{si } y \in [x] \end{cases}$$

Repetimos el proceso para cada una de las clases de equivalencia en $X/\mathscr{R}$. Supongamos que tenemos r clases de equivalencia, $[x_1], \ldots, [x_r]$, los ciclos asociados son respectivamente $\gamma_1, \ldots, \gamma_r$. Vamos a probar que se tiene $\sigma = \gamma_1 \ldots \gamma_r$. Dado $y \in X$, existe un índice i tal que $y \in [x_i]$, luego $\gamma_i(y) = \sigma(y)$, y $\gamma_j(y) = y$ si $j \neq i$; tenemos pues:

$$\gamma_1 \cdots \gamma_i \cdots \gamma_r(y) = \gamma_1 \cdots \gamma_i(y) = \gamma_1 \cdots \gamma_{i-1}(\sigma(y)) = \sigma(y),$$

ya que $\sigma(y) \in [x_i]$. Si algún γ_i tiene longitud igual a uno, entonces $\gamma_i = 1$, y por tanto podemos eliminarlo de la descomposición de σ. Supongamos ahora que $\sigma = \lambda_1 \ldots \lambda_s$ es otra descomposición de σ en producto de ciclos disjuntos con $\lambda_j \neq 1$ para todo índice j. Por ser los ciclos λ_j disjuntos cada uno mueve elementos de una sola clase de equivalencia, supongamos que λ_j mueve elementos de la clase $[x_i]$, entonces necesariamente λ_j mueve todos los elementos de $[x_i]$, luego $\lambda_j = \gamma_i$. Como consecuencia, repitiendo el proceso, para cada uno de los λ_j existe un γ_i tal que $\lambda_j = \gamma_i$. Y las dos descomposiciones de σ coinciden salvo en el orden. □

Como consecuencia inmediata de esta descomposición de permutaciones en producto de ciclos disjuntos tenemos:

Corolario. 2.3.
(1) Dos permutaciones cíclicas disjuntas conmutan.
(2) Cada dos permutaciones disjuntas conmutan.

Teorema. 2.4.
Toda permutación $\sigma \in S_n$, $n \geq 2$, es un producto de ciclos de longitud 2.

DEMOSTRACIÓN. Si $\sigma = 1$, es claro que $\sigma = (1\,2)(2\,1)$. Si $\sigma \neq 1$, entonces σ es un producto de ciclos disjuntos, como consecuencia basta probar que todo ciclo de longitud mayor ó igual que 2 es un producto de ciclos de longitud 2. Tenemos:

$$(x_1 \dots x_r) = (x_1 x_r) \cdots (x_1 x_2).$$

□

Un ciclo de longitud dos se llama una **trasposición**.

3. Subgrupos

Sea G un grupo; un subconjunto no vacío H de G que es cerrado para la operación del grupo G (esto es; para cada $a, b \in H$ se tiene $ab \in H$) y tal que con ella sea un grupo se llama un **subgrupo** de G y se representa por $H \leq G$ ó $H \subseteq G$.

Ejemplos. 3.1.
(1) Para todo grupo G el subconjunto $\{e\}$ es un subgrupo, al que se llama **subgrupo trivial** de G.
(2) Para todo grupo G el subconjunto G es un subgrupo, al que se llama **subgrupo total**. Los subgrupos total y trivial se llaman también **subgrupos impropios**, el resto de los subgrupos de G se llaman **subgrupos propios**.
(3) Si consideramos el grupo aditivo de los números reales $\mathbb{R}$, entonces el grupo aditivo $\mathbb{Z}$ es un subgrupo propio.
(4) Si G_1 y G_2 son subgrupos, el grupo $G_1 \times \{e\}$ es un subgrupo de $G_1 \times G_2$.
(5) El subconjunto de las matrices de $\mathrm{GL}_2(\mathbb{R})$ con determinante igual a 1 es un subgrupo de $\mathrm{GL}_2(\mathbb{R})$.

A continuación vamos a dar algunas caracterizaciones de subgrupos.

Lema. 3.2.
Sea G un grupo, y H un subconjunto no vacío de G, son equivalentes:

(a) H es un subgrupo de G.
(b)
  (I) Si $e \in G$ es el elemento neutro de G, entonces $e \in H$.
  (II) Si $a \in H$, entonces $a^{-1} \in H$.
  (III) Si $a, b \in H$, entonces $ab \in H$.
(c)
  (I) Si $a \in H$, entonces $a^{-1} \in H$.
  (II) Si $a, b \in H$, entonces $ab \in H$.
(d) Si $a, b \in H$, entonces $ab^{-1} \in H$.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). (I). Llamamos e' al elemento neutro de H, entonces en G tenemos para todo elemento $h \in H$; $e'h = h = eh$. Por lo tanto $e' = e$.
(II). Llamamos h' al inverso en H del elemento $h \in H$, entonces se verifica $h'h = e = h^{-1}h$. Por lo tanto $h' = h^{-1}$.
(III). Es inmediato de la definición de subgrupo.
(b) $\Rightarrow$ (c). Es evidente.
(c) $\Rightarrow$ (d). Si tomamos $a, b \in H$, entonces $b^{-1} \in H$, y por tanto tenemos $ab^{-1} \in H$.

3301-03.tex

(d) $\Rightarrow$ (b). Ya que H es no vacío, existe $a \in H$, entonces $aa^{-1} \in H$, y por tanto $e \in H$. Para cada $a \in H$, ya que $e \in H$, tenemos $ea^{-1} \in H$, luego $a^{-1} \in H$. Dados ahora $a, b \in H$, tenemos que $b^{-1} \in H$, por tanto $ab = a(b^{-1})^{-1} \in H$.

(b) $\Rightarrow$ (a). Por (III) H es un subconjunto cerrado para la operación definida en G. Por lo tanto esta operación verifica en H la propiedad asociativa. Por (I) existe un elemento neutro en H, este es e. Y por (II) cada elemento $h \in H$ tiene un inverso en H, este es h^{-1}. Luego H es un grupo, y por tanto un subgrupo de G. □

Corolario. 3.3.
Sea G un grupo, un subconjunto H de G no vacío y finito es un subgrupo si, y sólo si, es cerrado para la operación de G.

DEMOSTRACIÓN. ($\Rightarrow$). Es inmediato de la definición de subgrupo.

($\Leftarrow$). Supongamos que H no es un subgrupo de G, entonces por el Lema (3.2.), apartado (c), existe $h \in H$ tal que $h^{-1} \notin H$. Es inmediato que $h \neq e$. Consideramos todas la potencias de h con exponente entero positivo, ya que el conjunto de los números naturales es infinito y todas estas potencias pertenecen a H, que deben existir dos potencias con distinto exponente que sean iguales. Supongamos que $h^n = h^m$, con $n < m$ y sea $k \in \mathbb{N}$ tal que $0 \neq k$ y $m = n + k$, entonces tenemos que $h^k = e$. Se tiene entonces que $h^{-1} = h^{k-1} \in H$. Lo que es una contradicción. Por tanto para cada elemento $h \in H$ se ha de tener $h^{-1} \in H$, y H es un subgrupo de G. □

Vamos a estudiar ahora los subgrupos de un grupo y cómo están relacionados entre sí. En el conjunto $S(G)$ de los subgrupos de un grupo G se puede considerar una relación de orden mediante

$$H \leq K \text{ si } H \subseteq K, \text{ esto es } H \text{ está contenido en } K.$$

Se trata ahora de estudiar los supremos e ínfimos de familias de subgrupos.

Lema. 3.4.
Sea G un grupo y $\{H_i \mid i \in I\}$ una familia de subgrupos de G, entonces $\cap\{H_i \mid i \in I\}$ es un subgrupo de G y es el ínfimo, en $S(G)$, de esta familia.

DEMOSTRACIÓN. Vamos a utilizar la caracterización dada por el apartado (d) del Lema (3.2.). Sean $a, b \in \cap\{H_i \mid i \in I\}$, entonces para cada $i \in I$ se tiene $a, b \in H_i$, y ya que H_i es un subgrupo se verifica $ab^{-1} \in H_i$, entonces $ab^{-1} \in \cap\{H_i \mid i \in I\}$. El subgrupo $\cap\{H_i \mid i \in I\}$ es el mayor subgrupo contenido en todos los subgrupos H_i, luego es el ínfimo de la familia. □

También es posible determinar el menor subgrupo de G que contiene a todos los subgrupos H_i, este subgrupo es el supremo de la familia y se nota $\vee\{H_i \mid i \in I\}$. Se puede caracterizar como:

$$\vee\{H_i \mid i \in I\} = \cap\{H \mid H \subseteq G \text{ y } H_i \subseteq H \text{ para todo } i \in I\}.$$

Proposición. 3.5.
El conjunto de todos los subgrupos de un grupo G tiene estructura de retículo (conjunto parcialmente ordenado en el que cada par de elementos tiene un supremo y un ínfimo).

Si S es un subconjunto de un grupo G, por un razonamiento similar al anterior, existe un menor subgrupo de G que contiene a S, se representa por $\langle S\rangle$, se llama el **subgrupo generado** por S y está determinado por:

$$\langle S\rangle = \cap\{H \mid H \leq G \text{ y } S \subseteq H\}.$$

El conjunto S se llama **conjunto de generadores** o **sistema de generadores** de $\langle S\rangle$, y $\langle S\rangle$ se dice que está generado por S. Si S es un conjunto finito, se dice que $\langle S\rangle$ es un **grupo finitamente generado**, y cuando S está formado por un único elemento, $\langle S\rangle$ se llama un **grupo cíclico**. Para cada elemento a de un grupo G, se define el **orden** de a, $\text{ord}(a)$, como el orden del subgrupo cíclico $\langle a\rangle$ de G.

Lema. 3.6.
Sea G un grupo y $a \in G$ un elemento de G de orden finito n. Entonces n es el menor entero positivo m que verifica $a^m = e$.

DEMOSTRACIÓN. Consideremos los $n+1$ elementos $a^0 = e$, $a^1 = a$, a^2, $\ldots$, $a^n \in \langle a\rangle$, entonces existen enteros no negativos r, s tales que $r < s \leq n$ y $a^r = a^s$. Se tiene $s = r + h$ para algún entero positivo h, y por tanto $a^h = e$ y $0 < h \leq n$. Dado un entero m hacemos la división con resto por h y obtenemos $m = hc + t$ para algún entero t verificando $0 \leq t < h$, entonces $a^m = a^t \in \{e, a, \ldots, a^{n-1}\}$. Como consecuencia $\langle a\rangle = \{e, a, \ldots, a^{n-1}\}$ y $h = n$, lo que implica $a^n = e$. □

El siguiente paso es estudiar grupos con un número finito de elementos (grupos de orden finito). Si G es un grupo de orden n y H es un subgrupo de G de orden m, entonces se tiene que $m \leq n$. Se trata ahora de probar que además se verifica $m|n$, esto es; el orden de cada subgrupo de un grupo finito es un divisor del orden del grupo.

En la situación anterior, dado el subgrupo H de G se define en G una relación $\sim_H$ mediante:

$$a \sim_H b \text{ si } a^{-1}b \in H.$$

Lema. 3.7.
La relación $\sim_H$ es una relación de equivalencia en G.

Para un elemento $a \in G$, su clase de equivalencia es:

$$\begin{aligned}\overline{a} &= \{g \in G \mid a^{-1}g \in H\} \\ &= \{g \in G \mid \text{existe } h \in H \text{ tal que } a^{-1}g = h\} \\ &= \{g \in G \mid \text{existe } h \in H \text{ tal que } g = ah\} = aH.\end{aligned}$$

El conjunto aH se llama una **clase a la izquierda** de H en G. Se pretende contar el número de elementos de un grupo finito G utilizando las clases a la izquierda de H en G.

Lema. 3.8.
Para cada grupo finito G y cada subgrupo H de G existe una biyección entre cada dos clases a la izquierda de H en G.

DEMOSTRACIÓN. Sean $a \in G$, definimos $f : H \longrightarrow aH$ mediante: $f(h) = ah$. Es claro que f es sobreyectiva. Además, si $h, k \in H$ verifican $f(h) = f(k)$, entonces $ah = ak$, luego $h = k$, y f es también inyectiva. □

Teorema. 3.9. (Teorema de Lagrange)
Sea G un grupo finito y H un subgrupo de G, el orden de H divide al orden de G.

DEMOSTRACIÓN. La relación $\sim_H$ en G es de equivalencia y las clases de equivalencia dan lugar a una partición de G; ya que las clases de equivalencia son las clases a la izquierda de H en G tenemos una descomposición de G, por ejemplo $G = a_1H \cup \ldots \cup a_rH$, entonces $|G|$, el número de elementos de G, es igual a r por el número de elementos de H, $|H|$. Luego $|G| = r|H|$, y tenemos el resultado. □

Dado un grupo finito G y un subgrupo H, se llama **índice** de H en G al número entero $\mid G \mid / \mid H \mid$, y se nota por $[G : H]$.
Cuando G es un grupo no necesariamente finito, también se puede definir la relación $\sim_H$, esta relación sigue siendo de equivalencia, y si el conjunto cociente $G/\sim_H$ es finito, se puede llamar índice de H en G el número de elementos de $G/\sim_H$.
De forma análoga es posible definir las clases a la derecha de H en G, obteniéndose análogos resultados.

4. Ejercicios propuestos

Definición de grupo

Relaciones aritméticas entre elementos de un grupo

Ejercicio. 4.1.
Sea G un grupo arbitrario. Razona si las siguientes afirmaciones son ciertas:

(1) Para todo elemento $a \in G$ existe $b \in G$ tal que $aba = e$.
(2) Existe a lo sumo un elemento $a \in G$ tal que $aa = a$.
(3) La aplicación $f : G \longrightarrow G$, definida $f(x) = x^{-1}$ para $x \in G$ es una biyección.
(4) Para cada elemento $b \in G$ la aplicación $g_b : G \longrightarrow G$ definida $g_b(x) = bx$ es biyectiva.
(5) La ecuación $X^n = 1$ tiene como máximo n soluciones.

Ref.: 3301e_015 SOLUCIÓN

Ejercicio. 4.2.
Sean G un grupo y $a, b \in G$, si $ab = ba$, demuestra que para cada número entero $n \in \mathbb{Z}$, se verifica $(ab)^n = a^n b^n$.
Ref.: 3301e_003 SOLUCIÓN

Ejercicio. 4.3.
Sea G es un grupo. Demuestra que son equivalentes:

(a) G es un grupo abeliano.
(b) Para todos $a, b \in G$ se tiene $(ab)^2 = a^2 b^2$.
(c) Para todos $a, b \in G$ se tiene $(ab)^{-1} = a^{-1} b^{-1}$.
(d) Para todos $a, b \in G$ y para todo número entero $n \in \mathbb{Z}$ se tiene $(ab)^n = a^n b^n$.

Ref.: 3301e_004 SOLUCIÓN

3301-09.tex

Ejercicio. 4.4.
Demuestra que en un grupo G de orden par siempre existe un elemento, distinto del elemento neutro, que es su propio inverso.
Ref.: 3301e_006 SOLUCIÓN

Ejercicio. 4.5.
Sea G un grupo y $\{a_0,\dots,a_n\}$ una familia finita de elementos de G. Definimos:

$$\prod_{i=0}^{0} a_i = a_0, \quad \prod_{i=0}^{r+1} a_i = \left(\prod_{i=0}^{r} a_i\right) a_{r+1},$$

para todo $0 \le r < n$. Demuestra que se verifica:

(1) $\prod_{i=0}^{r} a_i = a_0(\prod_{i=1}^{r} a_i)$, *para todo* $0 < r \le n$.

(2) $(\prod_{i=0}^{r} a_i)(\prod_{j=r+1}^{n} a_j) = \prod_{k=0}^{n} a_k$, *para todo* $0 \le r < n$.

Ref.: 3301e_007 SOLUCIÓN

Ejercicio. 4.6.
Si G es un grupo y $a, b \in G$ elementos que verifican $a^2 = 1$ y $ab^2a = b^3$, demuestra que $b^5 = 1$.
Ref.: 3301e_008 SOLUCIÓN

Ejercicio. 4.7.
Sea G un grupo y $a, b, c \in G$, resuelve en G la siguiente ecuación:

$$aXbcX = abX.$$

Ref.: 3301e_016 SOLUCIÓN

Ejemplos de grupos

Ejercicio. 4.8.
Consideramos en el conjunto $\mathbb{Z}$ la operación binaria $*$ definida por:

$$a * b = a + b + 1.$$

Demuestra que $(\mathbb{Z}, *)$ es un grupo abeliano.
Ref.: 3301e_001 SOLUCIÓN

Ejercicio. 4.9.
Prueba que si G es un grupo y para cada elemento $a \in G$ se verifica $a^2 = 1$, entonces G es un grupo abeliano.
Ref.: 3301e_002 SOLUCIÓN

Ejercicio. 4.10.
Se considera el intervalo abierto $I = (-1, 1) \subseteq \mathbb{R}$, y en él la operación:

$$x * y = \frac{x + y}{1 + xy}.$$

Prueba que $(I, *)$ es un grupo abeliano.
Ref.: 3301e_043 SOLUCIÓN

Ejercicio. 4.11.
Sea X un conjunto, demuestra que $\mathscr{P}(X)$ junto con la operación binaria definida por:

$$A \Delta B = (A \setminus B) \cup (B \setminus A),$$

para todo $A, B \in \mathscr{P}(X)$, es un grupo abeliano.
Ref.: 3301e_005 SOLUCIÓN

Ejercicio. 4.12.
Se considera $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, *y en él la operación* $x * y = \begin{cases} xy, & si\ x > 0, \\ x/y, & si\ x < 0. \end{cases}$ *Prueba que* $(\mathbb{R}^*, *)$ *es un grupo no necesariamente abeliano.*
Ref.: 3301e_048 SOLUCIÓN

Ejercicio. 4.13.
Sea $\mathbb{R}$ *el conjunto de los números reales. Consideramos el conjunto*

$$X = \{f : \mathbb{R} \longrightarrow \mathbb{R} \mid f(x) = ax + b,\ para\ a, b \in \mathbb{R},\ a \neq 0\}.$$

Demuestra que X *junto con la composición es un grupo.*
Ref.: 3301e_009 SOLUCIÓN

Ejercicio. 4.14.
Consideramos el cuerpo $\mathbb{R}$ *de los números reales. Para* $a, b, c, d \in \mathbb{R}$, *con* $ad - bc = 1$ *consideramos la aplicación*

$$f_{a,b,c,d} : \mathbb{R} \cup \{\infty\} \longrightarrow \mathbb{R} \cup \{\infty\},\ definida\ por\ f_{a,b,c,d}(x) = \frac{ax + b}{cx + d}, \quad f_{a,b,c,d}(\infty) = z\ y\ f_{a,b,c,d}(z) = \infty,$$

en donde $cz + d = 0$. *Demuestra que el conjunto* $\{f_{a,b,c,d} \mid ad - bc \neq 0\}$, *junto con la composición de aplicaciones, es un grupo.*
Compara con el Ejercicio (11.8.).
Ref.: 3301e_010 SOLUCIÓN

Ejercicio. 4.15.
Sean G_1 *y* G_2 *dos grupos, en el producto cartesiano* $G_1 \times G_2$ *se define una operación binaria mediante*

$$(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2),\ para\ cualesquiera\ a_1, b_1 \in G_1\ y\ a_2, b_2 \in G_2.$$

Demuestra que $G_1 \times G_2$ *es un grupo con esta operación, y que es abeliano si, y sólo si,* G_1 *y* G_2 *lo son.*

Ver el Lema (1.12.).
Ref.: 3301e_011 SOLUCIÓN

Ejercicio. 4.16.
Sea $\{G_i \mid i \in I\}$ *una familia de grupos. Demuestra que* $\prod\{G_i \mid i \in I\}$ *es un grupo con la operación*

$$(g_i)_i(f_i)_i = (g_i f_i)_i;$$

y que $\prod\{G_i \mid i \in I\}$ *es un grupo abeliano si, y sólo si, lo es cada uno de los grupos* G_i.
Ref.: 3301e_012 SOLUCIÓN

Ejercicio. 4.17.
Dado un grupo G *y un conjunto* H, *llamamos* G^H *al conjunto de todas las aplicaciones de* H *en* G. *En* G^H *definimos una operación binaria mediante:* $(f\ g)(h) = f(h)\,g(h)$ *para cada* $h \in H$. *Demuestra que* G^H *con esta operación es un grupo y que es abeliano si, y sólo si,* G *lo es.*
Ref.: 3301e_014 SOLUCIÓN

Ejercicio. 4.18.
Sea $G = \{(a,b) \in \mathbb{R} \times \mathbb{R} \mid a \neq 0\}$. *En* G *definimos la operaciónbinaria*

$$(a,b)\cdot(c,d) = (ac, ad+b).$$

Demuestra que con esta operación G *es un grupo no abeliano.*
Ref.: 3301e_013 SOLUCIÓN

Grupos simétricos I

Ejercicio. 4.19.
Reduce los siguientes productos a productos de ciclos disjuntos y hallar su paridad:

(1) (1 2 3 4 5)(1 5 6)(2 4 6)
(2) (1 2 3 4)(2 3 4 5)(3 4 5 1)
(3) (1 2)(2 3)(3 4)(4 5)(5 1)
(4) (2 4 6)(1 5 6)(1 2 3 4 5).

Ref.: 3301e_017 SOLUCIÓN

Ejercicio. 4.20.
Demuestra que todo ciclo de longitud ≥ 3 y par se puede escribir como un producto de ciclos de longitud 3.
Ref.: 3301e_018 SOLUCIÓN

Subgrupos

Ejemplos de subgrupos

Ejercicio. 4.21.
Determina todos los subgrupos del grupo aditivo de los números enteros.
Ref.: 3301e_019 SOLUCIÓN

Ejercicio. 4.22.
Determina todos los subgrupos de S_3. Representa el retículo $S(S_3)$.
Ref.: 3301e_027 SOLUCIÓN

Ejercicio. 4.23.
Determina todos los subgrupos de D_4. Representa el retículo $S(D_4)$.
Ref.: 3301e_028 *SOLUCIÓN*

Ejercicio. 4.24.
Determina todos los subgrupos de D_5. Representa el retículo $S(D_5)$.
Ref.: 3301e_029 *SOLUCIÓN*

Ejercicio. 4.25.
Calcula el orden de todos los elementos de S_4.
Ref.: 3301e_030 *SOLUCIÓN*

Ejercicio. 4.26.
Calcula el orden de todos los elementos de D_6.
Ref.: 3301e_031 *SOLUCIÓN*

Ejercicio. 4.27.
Demuestra que un grupo con un número finito de subgrupos es un grupo finito.
Ref.: 3301e_037 *SOLUCIÓN*

Órdenes de elementos

Ejercicio. 4.28.
Dado un grupo G y elementos $a, x \in G$. Demuestra que:

(1) a, a^{-1} y xax^{-1} tienen el mismo orden;
(2) ax y xa tienen el mismo orden;
(3) si existen números naturales n y m verificando $a^m x^n = xa$, entonces $a^{m-2}x^n$, $a^m x^{n-2}$ y ax^{-1} tienen el mismo orden.

Ref.: 3301e_047 SOLUCIÓN

Ejercicio. 4.29.
Sea G un grupo y $a \in G$ un elemento de orden n.

(1) Demostrar que si m y r son números naturales tales que $n \mid mr$ entonces $\frac{n}{d} \mid r$, siendo $d = \mathrm{mcd}(n, m)$.
(2) Demostrar que para cualquier número natural m,

$$\mathrm{ord}(a^m) = \frac{n}{\mathrm{mcd}(n, m)}.$$

Ref.: 3301e_041 SOLUCIÓN

Ejercicio. 4.30.
Sea G un grupo y $a, b \in G$ elementos que verifican $ab = ba$; si $\langle a \rangle \cap \langle b \rangle = \{1\}$, demuestra que $\mathrm{ord}(ab) = \mathrm{mcm}\{n, m\}$.
Ref.: 3301e_022 SOLUCIÓN

Ejercicio. 4.31.
Sean $a, b \in G$ dos elementos de un grupo, que conmutan entre sí, $ab = ba$, de órdenes primos relativos, $\mathrm{mcd}\{\mathrm{ord}(a), \mathrm{ord}(b)\} = 1$. *Demuestra que* $\mathrm{ord}(ab) = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$.
Ref.: 3301e_042 SOLUCIÓN

Ejercicio. 4.32.
*Dado un grupo G, llamamos el **exponente** de G al supremo de los órdenes de los elementos de G. Demuestra que:*

(1) Si G tiene exponente finito, entonces existe un elemento $a \in G$ tal que el orden de a es igual al exponente de G.
(2) Si el orden de G es finito, entonces el exponente de G es un divisor del orden de G.
(3) Si G es abeliano y el exponente de G es finito, entonces el orden de cada elemento divide al exponente de G.

Ref.: 3301e_024 SOLUCIÓN

Ejercicio. 4.33.
¿Si a y b son elementos de un grupo y tienen orden finito, es necesariamente ab de orden finito?
(Nota: Considera el grupo de matrices cuadradas con determinante no nulo y coeficientes en $\mathbb{Q}$, y los elementos

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ y } b = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}.$$

Ref.: 3301e_032 SOLUCIÓN

Ejercicio. 4.34.
Definimos Q_2 como el subgrupo del grupo $GL_2(\mathbb{C})$ generado por las matrices:

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ y } \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

(1) Demuestra que Q_2 es un grupo no abeliano de orden 8.
(2) Determina todos los subgrupos de Q_2.
(3) Representa el retículo $\mathscr{S}(Q_2)$.

*El grupo Q_2 se llama **grupo cuaternio** ó **grupo de los cuaternios**.*
Ref.: 3301e_033 SOLUCIÓN

Ejercicio. 4.35.
Sea G un grupo y sean $a, b \in G$ tales que $ba = ab^k$ y $a^n = 1$ con $n > 0$.

(1) Demuestra que para todo $i \in \mathbb{Z}$ se verifica $b^i a = ab^{ik}$.
(2) Demuestra que para todo $j \geq 0$ se verifica $ba^j = a^j b^{k^j}$.
(3) Demuestra que para todo $i \in \mathbb{Z}$ y todo $j \geq 0$ se verifica $b^i a^j = a^j b^{ik^j}$.
(4) Demuestra que todo elemento de $\langle a, b\rangle$ puede escribirse como $a^r b^s$ con $0 \leq r < n$.
(5) Demuestra que si $k \neq \pm 1$ existe un $m > 0$ tal que $b^m = 1$.

Ref.: 3301e_050 SOLUCIÓN

Ejercicio. 4.36.
Sea a un elemento de orden finito de un grupo G. Si $\text{ord}(a) = mn$, con $\text{mcd}\{n, m\} = 1$, prueba que existen dos elementos $x, y \in G$ tales que $a = xy = yx$, y $\text{ord}(x) = n$, $\text{ord}(y) = m$.
Ref.: 3301e_058 SOLUCIÓN

Ejercicio. 4.37.
Demuestra que un grupo finito de orden un número impar no tiene elementos de orden dos.
Ref.: 3303e_013 SOLUCIÓN

Subgrupos

Ejercicio. 4.38.
Demuestra que si A y B son subgrupos de un grupo G, entonces $A \cup B$ es un subgrupo de G si, y sólo si, $A \subseteq B$ ó $B \subseteq A$.
Ref.: 3301e_020 SOLUCIÓN

Ejercicio. 4.39.
Demuestra que si $\{H_i \mid i \in \mathbb{N}\}$ *es una familia de subgrupos de un grupo* G *tales que* $H_i \subseteq H_j$ *si* $i \leq j$, *entonces* $\vee\{H_i \mid i \in \mathbb{N}\} = \cup\{H_i \mid i \in \mathbb{N}\}$.
Ref.: 3301e_026 SOLUCIÓN

Ejercicio. 4.40.
Sea G *un grupo finito no trivial, prueba que son equivalentes:*
(a) La unión de cada dos subgrupos de G *es un subgrupo de* G.
(b) $G \cong \mathbb{Z}_{p^e}$ *para* p *primo.*

Ref.: 3301e_023 SOLUCIÓN

Ejercicio. 4.41.
Sea G *un grupo y* S *un subconjunto de* G, *da una descripción explícita de los elementos del subgrupo* $\langle S \rangle$.
(Nota. Comprueba que $\langle S \rangle = \{s_1 \cdots s_r \mid s_i \text{ ó } s_i^{-1} \in S\}$*).*
Ref.: 3301e_025 SOLUCIÓN

Ejercicio. 4.42.
Sea G *un grupo, definimos el* ***centro*** *de* G *como* $Z(G) = \{g \in G \mid xg = gx \text{ para todo } x \in G\}$.
(1) Demuestra que $Z(G)$ *es un subgrupo de* G.
(2) Demuestra que G *es un grupo abeliano si, y sólo si,* $G = Z(G)$.

Ref.: 3301e_034 SOLUCIÓN

Ejercicio. 4.43.
Sean H y K subgrupos de un grupo G tales que para algunos $a, b \in G$ se tiene $Ha = Kb$. Demuestra que $H = K$.
Ref.: 3301e_021 SOLUCIÓN

Ejercicio. 4.44.
Sean H, K y L subgrupos de un grupo G verificando las relaciones:
(1) $H \subseteq K$;
(2) $H \cap L = K \cap L$;
(3) $HL = KL$.

Demuestra que $H = K$.
Ref.: 3301e_038 SOLUCIÓN

Índices de subgrupos

Ejercicio. 4.45.
Demuestra que si se tienen subgrupos $H \leq T \leq G$ de un grupo finito G, entonces

$$[G : H] = [G : T][T : H].$$

Ref.: 3301e_045 SOLUCIÓN

Ejercicio. 4.46.
Sea G un grupo, H, K subgrupos de G de índices finitos y primos relativos. Demuestra que $G = H \vee K$.
Ref.: 3301e_035 SOLUCIÓN

Ejercicio. 4.47. (Teorema de Poincaré)
Sea G un grupo, H, K subgrupos de G de índices finitos. Demuestra que $H \cap K$ tiene índice finito y se verifica:

$$[G : H \cap K] \leq [G : H][G : K].$$

Ref.: 3301e_036 SOLUCIÓN

Ejercicio. 4.48.
Sean H y K subgrupos de un grupo G.

(1) Demuestra que HK es una unión de clases a la izquierda de K (resp. de clases a la derecha de H).
(2) Demuestra que el número de estas clases es $[H : H \cap K]$ (resp. $[K : H \cap K]$.)

Ref.: 3303e_027 SOLUCIÓN

Grupos de elementos invertibles

Ejercicio. 4.49.
El grupo de los elementos invertibles de un anillo conmutativo.

(1) Si A es un anillo, no necesariamente conmutativo, se define su grupo de unidades o grupo de elementos invertibles $U(A)$ como

$$U(A) = \{a \in A \mid \text{ existe } a^{-1} \in A \text{ tal que } aa^{-1} = 1 = a^{-1}a\}.$$

Demuestra que $U(A)$ es efectivamente un grupo con la operación de multiplicación en el anillo.
(2) Demuestra que si A y B son dos anillos, entonces

$$U(A \times B) = U(A) \times U(B).$$

(3) Prueba que si $f : A \longrightarrow B$ es un isomorfismo de anillos, este restringe a un isomorfismo entre sus correspondientes grupos de unidades $f : U(A) \longrightarrow U(B)$.

Ref.: 3301e_051 SOLUCIÓN

Ejercicio. 4.50.
Sea $n \geq 2$ un entero y $U(\mathbb{Z}_n)$ el grupo de los elementos invertibles del anillo de clases de restos módulo n. Demuestra que

$$U(\mathbb{Z}_n) = \{\bar{r} \mid 1 \leq r \leq n, \quad \text{mcd}(r,n) = 1\}$$

Ref.: 3301e_052 SOLUCIÓN

Ejercicio. 4.51.
Sea p un número primo. Demuestra que $U(\mathbb{Z}_p) = \mathbb{Z}_p \setminus \{0\}$, y por tanto tiene $p-1$ elementos.
*Deduce el **Pequeño Teorema de Fermat**: Para todo entero primo positivo p y para todo entero m, primo relativo con p, se verifica $m^{p-1} \equiv 1 \pmod{p}$.*
Ref.: 3301e_053 SOLUCIÓN

Ejercicio. 4.52.
Grupos de elementos invertibles de cocientes de $\mathbb{Z}$.
(1) Demuestra que si $\text{mcd}(m,n) = 1$, entonces existe un isomorfismo de anillos $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$.
(2) Da un ejemplo mostrando que el isomorfismo anterior no existe si m y n no son primos entre sí.
(3) Demuestra que si $\text{mcd}(m,n) = 1$, hay un isomorfismo de grupos

$$U(\mathbb{Z}_{nm}) \cong U(\mathbb{Z}_n) \times U(\mathbb{Z}_m).$$

Ref.: 3301e_054 SOLUCIÓN

Ejercicio. 4.53.
La función tociente de Euler $\varphi(n)$ se define para n entero positivo como el número de naturales menores que n y primos relativos con n. Esto es

$$\varphi(n) = |\{r \mid 1 \leq r \leq n, \text{mcd}(r,n) = 1\}|.$$

(1) *Demuestra que* $\varphi(n) = |U(\mathbb{Z}_n)|$.
(2) *Demuestra que si* $\mathrm{mcd}(m,n) = 1$, *entonces* $\varphi(nm) = \varphi(n)\varphi(m)$.
(3) *Demuestra que para cada primo* p *y cada* $e \geq 1$ *se verifica que* $\varphi(p^e) = (p-1)p^{e-1}$.
(4) *Calcula* $\varphi(8)$, $\varphi(72)$ *y* $\varphi(100)$.

Ref.: 3301e_055 SOLUCIÓN

Ejercicio. 4.54.
Deduce el ***Teorema de Euler****: Para todo entero positivo* n *y para todo entero* m *primo relativo con* n *se verifica* $m^{\varphi(n)} \equiv 1 \pmod{n}$.
Ref.: 3301e_056 SOLUCIÓN

Ejercicio. 4.55.
Determina los dos últimos dígitos de $3^{3^{100}}$.
(Pista: determina $3^{100} \pmod{\varphi(100)}$*).*
Ref.: 3301e_057 SOLUCIÓN

Ejercicio. 4.56.
Demuestra que el grupo de Klein abstracto $V = \mathbb{Z}_2 \times \mathbb{Z}_2$ *es, salvo isomorfismo, el único grupo de orden 4 que no es cíclico.*
Para la unicidad, demuestra primero que si G *un grupo de orden 4 que no es cíclico entonces todos sus elementos, a excepción del trivial, tienen orden 2. Construye la tabla de* G *y demuestra finalmente que* $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
Ref.: 3301e_046 SOLUCIÓN

Ejercicio. 4.57.
Determina el grupo de los elementos invertibles de $\mathbb{Z}_{12}$.
Ref.: 3301e_040 SOLUCIÓN

Desubicados

Capítulo II

Homomorfismos de grupos

5 Homomorfismos de grupos 37
6 Subgrupos normales y grupos cocientes 41
7 Grupos cíclicos 54
8 Grupos simétricos II 58
9 Ejercicio propuestos 62

Introducción.

5. Homomorfismos de grupos

Sean G y G' dos grupos y $f : G \longrightarrow G'$ una aplicación, f se llama un **homomorfismo de grupos** si para cualesquiera $a, b \in G$ se tiene

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

Ejemplos. 5.1.
(1) Si G es un grupo, la aplicación identidad de G en sí mismo es un homomorfismo de grupos.
(2) Si H es un subgrupo de un grupo G, la aplicación inclusión de H en G es un homomorfismo de grupos.
(3) Si G_1 y G_2 son grupos, las proyecciones del producto $p_i : G_1 \times G_2 \longrightarrow G_i$ para $i = 1, 2$ son homomorfismos de grupos.

Lema. 5.2.
Sea $f : G \longrightarrow G'$ un homomorfismo de grupos, entonces:
(1) $f(e) = e'$, donde e y e' son los elementos neutros de G y G' respectivamente.
(2) $f(a^{-1}) = f(a)^{-1}$, para todo $a \in G$.

3302-01.tex

DEMOSTRACIÓN. (1). Tenemos para $e \in G$ el elemento neutro

$$e'f(e) = f(e) = f(ee) = f(e)f(e),$$

luego $e' = f(e)$.
(2). Para cada $a \in G$ tenemos:

$$e' = f(e) = f(aa^{-1}) = f(a)f(a^{-1}),$$

luego $f(a^{-1}) = f(a)^{-1}$. □

En general representaremos e' también por e.
Si $f : G \longrightarrow G'$ es un homomorfismo de grupos y $A \subseteq G$ un subconjunto, llamamos $f_*(A)$ a la **imagen** de A por f, esto es;

$$f_*(A) = \{f(a) \mid a \in A\}$$

y si $B \subseteq G'$ es un subconjunto, llamamos $f^*(B)$ a la **imagen inversa** de B por f, esto es;

$$f^{-1}(B) = f^*(B) = \{g \in G \mid f(g) \in B\}.$$

Lema. 5.3.
Sea $f : G \longrightarrow G'$ un homomorfismo de grupos, se verifica:
(1) Si H es un subgrupo de G, entonces $f_*(H)$ es un subgrupo de G'.
(2) Si K es un subgrupo de G', entonces $f^*(K)$ es un subgrupo de G.

DEMOSTRACIÓN. (1). Si H es un subgrupo de G, entonces H es no vacío, luego $f_*(H)$ es no vacío. Sean ahora $a, b \in f_*(H)$, entonces existen $x, y \in H$ tales que $f(x) = a$ y $f(y) = b$. Por ser H un subgrupo tenemos que $xy^{-1} \in H$, y se verifica:

$$ab^{-1} = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in f_*(H).$$

Luego $f_*(H)$ es un subgrupo de G'.
(2). Si K es un subgrupo de G', entonces $e' \in K$, y por tanto $e \in f^*(K)$, luego $f^*(K)$ es no vacío. Sean ahora $a, b \in f^*(K)$, entonces $f(a), f(b) \in K$, y por ser K un subgrupo tenemos que $f(a)f(b)^{-1} \in K$. Se verifica por tanto que

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} \in K,$$

luego $ab^{-1} \in f^*(K)$, y por tanto $f^*(K)$ es un subgrupo de G. □

Dado un homomorfismo $f : G \longrightarrow G'$, el subgrupo $f_*(G)$ de G' se llama **imagen** de f, y se representa por Im(f). Y el subgrupo $f^*(\{e\})$ de G se llama **núcleo** de f, y se representa por Ker(f).

Un homomorfismo de grupos $f : G \longrightarrow G'$ tal que la aplicación f sea sobreyectiva se llama un **homomorfismo sobreyectivo** o un **epimorfismo**; si la aplicación f es inyectiva, entonces f se llama un **homomorfismo inyectivo** o un **monomorfismo**. Si un homomorfismo es a la vez inyectivo y sobreyectivo, entonces se llama **isomorfismo**.

Lema. 5.4.
Sea $f : G \longrightarrow G'$ un homomorfismo de grupos, entonces:
(1) f es un homomorfismo inyectivo si, y sólo si, $\mathrm{Ker}(f) = \{e\}$.
(2) f es un homomorfismo sobreyectivo si, y sólo si, $\mathrm{Im}(f) = G'$.
(3) f es un isomorfismo si, y sólo si, existe $g : G' \longrightarrow G$ homomorfismo de grupos tal que $fg = 1_{G'}$ y $gf = 1_G$.

DEMOSTRACIÓN. (1). ($\Rightarrow$). Si f es un homomorfismo inyectivo y $f(a) = e'$, entonces por ser $f(e) = e'$, se verifica $a = e$, luego $\mathrm{Ker}(f) = \{e\}$.
($\Leftarrow$). Si $f(a) = f(b)$, para $a, b \in G$, entonces $e' = f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$. Por tanto $ab^{-1} \in \mathrm{Ker}(f) = \{e\}$, y $ab^{-1} = e$, entonces $a = b$.
(2). Es evidente.
(3). ($\Rightarrow$). Si f es un isomorfismo, entonces f es una biyección, y por tanto existe una aplicación $g : G' \longrightarrow G$ tal que $fg = 1_{G'}$ y $gf = 1_G$. Vamos a comprobar que g es un homomorfismo de grupos. Sean $a, b \in G'$, entonces tenemos:

$$g(ab) = g(fg(a)fg(b)) = g(f(g(a)g(b))) = gf(g(a)g(b)) = g(a)g(b).$$

($\Leftarrow$). Si existe un homomorfismo $g : G' \longrightarrow G$ verificando las condiciones del enunciado, entonces f es una aplicación biyectiva, y por tanto f es un homomorfismo inyectivo y un homomorfismo sobreyectivo, luego es un isomorfismo. □

Al contrario que en el caso de conjuntos, un homomorfismo de grupos inyectivo no necesariamente ha de tener un homomorfismo inverso a la izquierda (dar un ejemplo). Lo mismo ocurre con los homomorfismos sobreyectivos (dar un ejemplo).
Si $f : G \longrightarrow G'$ es un homomorfismo de grupos, es posible relacionar los subgrupos de $\mathrm{Im}(f)$ con subgrupos de G de la siguiente forma:

Lema. 5.5.
Sea $f : G \longrightarrow G'$ un homomorfismo de grupos, existe una correspondencia biyectiva que mantiene el orden entre los subgrupos de $\mathrm{Im}(f)$ *y los subgrupos de G que contienen a* $\mathrm{Ker}(f)$. *Esta correspondencia asocia a un subgrupo K de* $\mathrm{Im}(f)$ *su imagen inversa $f^*(K)$, y a un subgrupo H de G, que contiene a* $\mathrm{Ker}(f)$, *su imagen $f_*(H)$.*

DEMOSTRACIÓN. Considerando $\Gamma = \{H \mid \operatorname{Ker}(f) \leq H \leq G\}$ y $\Theta = \{K \mid K \leq G'\}$, definimos las aplicaciones $f_* : \Gamma \longrightarrow \Theta$ y $f^* : \Theta \longrightarrow \Gamma$, es claro que están bien definidas; basta comprobar que $f_* f^* = 1_\Theta$ y $f^* f_* = 1_\Gamma$.
Para $H \in \Gamma$ tenemos

$$H \subseteq f^* f_*(H),$$

además, si $x \in f^* f_*(H)$, entonces $f(x) \in f_*(H)$, luego existe $h \in H$ tal que $f(h) = f(x)$, por tanto $xh^{-1} \in \operatorname{Ker}(f)$, pero por ser $\operatorname{Ker}(f) \leq H$, tenemos $x \in H$, entonces $f^* f_*(H) \subseteq H$.
Para $K \in \Theta$, ya que la aplicación $f : G \longrightarrow \operatorname{Im}(f)$ es sobreyectiva, tenemos

$$K = f_* f^*(K),$$

□

Lema. 5.6.
Sean $f : G \longrightarrow G'$ y $g : G' \longrightarrow G''$ dos homomorfismos de grupos, entonces:

(1) La composición $gf : G \longrightarrow G''$ es un homomorfismo de grupos.
(2) Si f y g son homomorfismos sobreyectivos (resp. homomorfismos inyectivos, isomorfismos), entonces gf es un homomorfismo sobreyectivo (resp. homomorfismo inyectivo, isomorfismo).
(3) Si gf es un homomorfismo sobreyectivo (resp. homomorfismo inyectivo), entonces g es un homomorfismo sobreyectivo (resp. f es un homomorfismo inyectivo).

DEMOSTRACIÓN. (1). Para $a, b \in G$ se verifica:

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

(2). Es inmediato, ya que la composición de aplicaciones sobreyectivas (resp. inyectivas, biyectivas) es también una aplicación sobreyectiva (resp. inyectiva, biyectiva).
(3). Es inmediato, ya que si la aplicación gf es sobreyectiva (resp. inyectiva), entonces g es una aplicación sobreyectiva (resp. f es una aplicación inyectiva). □

Si G es un grupo, un endomorfismo de G es un homomorfismo $f : G \longrightarrow G$, y un automorfismo es un endomorfismo que es además isomorfismo. El conjunto de todos los endomorfismos de G se representa por $\operatorname{End}(G)$, y el de todos los automorfismos de G se representa por $\operatorname{Aut}(G)$.

6. Subgrupos normales y grupos cocientes

Subgrupos normales

Lema. 6.1.
Sea G un grupo y N un subgrupo de G. Son equivalentes las siguientes afirmaciones:
(a) $aN = Na$ *para cada* $a \in G$.
(b) Para cada $a, b \in G$ *se tiene* $ab \in N$ *implica* $ba \in N$.
(c) $aNa^{-1} = \{ana^{-1} \mid n \in N\} \subseteq N$ *para cada* $a \in G$.
(d) $aNa^{-1} = N$ *para cada* $a \in G$.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Si $a, b \in G$ y $ab \in N$, entonces existe $n \in N$ tal que $ab = n$, y tenemos $b = a^{-1}n \in a^{-1}N = Na^{-1}$, luego existe $n' \in N$ tal que $b = n'a^{-1}$, y entonces $ba = n' \in N$.
(b) $\Rightarrow$ (c). Si $a \in G$ y $n \in N$, llamamos $b = ana^{-1}$, entonces $a^{-1}(ba) = n \in N$, luego $ana^{-1} = b = (ba)a^{-1} \in N$.
(c) $\Rightarrow$ (d). Consideramos $a^{-1} \in G$, entonces $a^{-1}Na \subseteq N$, luego tenemos las siguientes inclusiones: $N = a(a^{-1}Na)a^{-1} \subseteq aNa^{-1} \subseteq N$. Por lo tanto $N = aNa^{-1}$.
(d) $\Rightarrow$ (a). Si $a \in G$ tenemos por hipótesis que $N = aNa^{-1}$, luego se verifica $aN = aN(a^{-1}a) = (aNa^{-1})a = Na$. □

Un subgrupo N que verifica las condiciones del Lema (6.1.) se llama **subgrupo normal** de G.
Si N es un subgrupo de un grupo G, para cada $a \in G$ el subconjunto aNa^{-1} es también un subgrupo de G, se llama **subgrupo conjugado** de N en G. Por lo tanto un subgrupo N de G es normal si, y sólo si, coincide con todos sus conjugados.

Ejemplos. 6.2.
(a) Si $f : G \longrightarrow G'$ es un homomorfismo de grupos, entonces $\mathrm{Ker}(f)$ es un subgrupo normal de G.
(b) Si G es un grupo abeliano, entonces todo subgrupo de G es normal.
(c) Si G es un grupo, el subgrupo $Z(G)$ es un subgrupo normal.

Una relación de equivalencia $\sim$ en un grupo G se llama **compatible** si verifica:

$$a \sim b \text{ y } c \sim d \text{ implica } ac \sim bd$$

para todo $a, b, c, d \in G$.

3302-02.tex

Lema. 6.3.
Sea G un grupo y N un subgrupo de G, son equivalentes:
(a) $\sim_N$ es una relación compatible.
(b) El subgrupo N es un subgrupo normal de G.

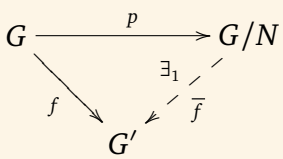
DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Supongamos que $a \in G$ y $n \in N$ son elementos arbitrarios. Se verifica $a \sim a$, $n \sim e$ y $a^{-1} \sim a^{-1}$, entonces por ser $\sim$ compatible, tenemos: $ana^{-1} \sim aea^{-1}$, luego $ana^{-1} \sim e$, y $ana^{-1} \in N$.
(b) $\Rightarrow$ (a). Supongamos que $a, b, c, d \in G$ y que $a \sim_N b$, $c \sim_N d$; entonces $a^{-1}b \in N$ y $c^{-1}d \in N$. Por el Lema (6.1.) tenemos $dc^{-1} \in N$, luego $a^{-1}bdc^{-1} \in N$, y aplicando nuevamente el Lema 6.1. tenemos $c^{-1}a^{-1}bd \in N$, luego $(ac)^{-1}(bd) \in N$, y entonces $ac \sim_N bd$. □

Teorema. 6.4.
Sea G un grupo, N un subgrupo normal de G, existe entonces una única operación binaria en $G/\sim_N$ de forma que la proyección canónica $p : G \longrightarrow G/\sim_N$ sea un homomorfismo de grupos.

DEMOSTRACIÓN. Si p fuese un homomorfismo de grupos, para cada $a, b \in G$ se debe verificar $p(a)p(b) = p(ab)$; entonces tenemos que definir $aNbN = abN$. Por ser $\sim_N$ una relación de equivalencia compatible, la operación está bien definida, esto es; no depende de los representantes de las clases elegidos. La operación binaria en $G/\sim_N$ verifica la propiedad asociativa, el elemento neutro es eN, y el elemento inverso de aN es $a^{-1}N$; luego $G/\sim_N$ es un grupo. Además es la única operación binaria que podemos definir en $G/\sim_N$ para que p sea un homomorfismo de grupos. □

El nuevo grupo así definido se llama **grupo cociente** de G por el subgrupo normal N, y se representa por G/N. Como consecuencia inmediata de la construcción del grupo cociente, se tiene que cada subgrupo normal N de G es el núcleo de algún homomorfismo de grupos con dominio G, por ejemplo de la proyección canónica de G en el grupo cociente G/N.

Teorema. 6.5. (Propiedad Universal del Grupo Cociente)
Sea G un grupo y N un subgrupo normal de G, llamamos $p : G \longrightarrow G/N$ a la proyección canónica. Para cada homomorfismo $f : G \longrightarrow G'$ tal que $N \subseteq \mathrm{Ker}(f)$ existe un único homomorfismo $\overline{f} : G/N \longrightarrow G'$ tal que $\overline{f}p = f$.



DEMOSTRACIÓN. Supongamos que existe $\overline{f}$ verificando la igualdad $\overline{f}p = f$, entonces se verifica: $\overline{f}(aN) = \overline{f}(p(a)) = \overline{f}p(a) = f(a)$. Vamos a probar ahora que, así definido $\overline{f}$, es un homomorfismo de grupos. Primero comprobamos que es una aplicación; sean $aN = bN$, entonces $a^{-1}b \in N$, y por tanto $f(a^{-1}b) = e$, luego $f(a) = f(b)$. Segundo comprobamos que es un homomorfismo de grupos; sean aN, $bN \in G/N$, entonces $\overline{f}(aNbN) = \overline{f}(abN) = f(ab) = f(a)f(b) = \overline{f}(aN)\overline{f}(bN)$. Es claro que con esta definición $\overline{f}$ es el único homomorfismo de grupos que verifica $\overline{f}p = f$. □

Corolario. 6.6.
En la misma situación que el Teorema 6.5. se verifica:

(1) Si f es un homomorfismo sobreyectivo, entonces $\overline{f}$ también lo es.
(2) Si $N = \mathrm{Ker}(f)$, entonces $\overline{f}$ es un homomorfismo inyectivo.

DEMOSTRACIÓN. (1). Es inmediato.
(2). Sea $N = \mathrm{Ker}(f)$, si para $a \in G$ se verifica $\overline{f}(aN) = e$, entonces $f(a) = e$, y por tanto $a \in \mathrm{Ker}(f) = N$, luego $aN = eN$, y $\mathrm{Ker}(\overline{f}) = \{eN\}$, y es un homomorfismo inyectivo. □

Teoremas de isomorfía

Teorema. 6.7. (Primer Teorema de Isomorfía)
Sea $f : G \longrightarrow G'$ un homomorfismo de grupos, entonces podemos construir un diagrama conmutativo

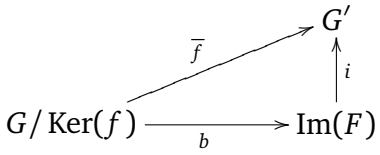
$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & G' \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ G/\mathrm{Ker}(f) & \xrightarrow[\ b\ ]{} & \mathrm{Im}(f) \end{array}$$

donde p es la proyección canónica, b es un isomorfismo e i es la inclusión.

DEMOSTRACIÓN. Por ser $\mathrm{Ker}(f)$ un subgrupo normal de G tenemos la factorización

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & G' \\ {\scriptstyle p}\downarrow & \nearrow_{\overline{f}} & \\ G/\mathrm{Ker}(f) & & \end{array}$$

y por tanto $\overline{f}$ es un homomorfismo inyectivo. Consideramos el subgrupo $\mathrm{Im}(f)$. Tenemos $\mathrm{Im}(f) = \mathrm{Im}(\overline{f})$, entonces existe una factorización de $\overline{f}$ a través de $\mathrm{Im}(f)$,



Por ser $\overline{f}$ inyectivo, también b lo es, y para comprobar que es sobreyectivo basta tener en cuenta que $\mathrm{Im}(f) = \mathrm{Im}(\overline{f})$. □

Teorema. 6.8.
Sea G un grupo y $f : G \longrightarrow G'$ un homomorfismo de grupos, entonces en la correspondencia biunívoca, que conserva el orden, entre los subgrupos de $\mathrm{Im}(f)$ *y los subgrupos de G que contienen a* $\mathrm{Ker}(f)$*, los subgrupos normales de G que contienen a* $\mathrm{Ker}(f)$ *se corresponden con los subgrupos normales de* $\mathrm{Im}(f)$.

DEMOSTRACIÓN. En la notación del Lema 5.5., si $N \in \Gamma$ es un subgrupo normal de G, entonces para cada $a \in \mathrm{Im}(f)$ existe $x \in G$ tal que $f(x) = a$, se verifica pues

$$af_*(N)a^{-1} = f(x)f_*(N)f(x)^{-1} = f_*(xNx^{-1}) \subseteq f_*(N),$$

y $f_*(N)$ es un subgrupo normal de $\mathrm{Im}(f)$. De forma análoga, si $K \in \Theta$ es un subgrupo normal de $\mathrm{Im}(f)$, existe $H \in \Gamma$ tal que $f_*(H) = K$, para cada $a \in G$ se tiene

$$f_*(af^*(K)a^{-1}) = f(a)f_*(f^*(H))f(a)^{-1} = f(a)f_*(H)f(a)^{-1} = f(a)Kf(a)^{-1} = K,$$

y por tanto $f^*(K) = af^*(K)a^{-1}$ y es un subgrupo normal de G □

Como consecuencia los subgrupos del grupo cociente G/N son de la forma H/N, donde H es un subgrupo de G que contiene a N, y H es un subgrupo normal de G si, y sólo si, H/N es un subgrupo normal de G/N.

Dado un grupo G y subgrupos H y K de G, se define la **composición** de H y K como:

$$HK = \{hk \in G \mid h \in H \text{ y } k \in K\}.$$

En general HK no es un subgrupo de G, pero si HK es un subgrupo de G, entonces se tiene $HK = H \vee K$, esto es; el menor subgrupo de G que contiene a H y a K.

Lema. 6.9.
Sea G un grupo y H, K subgrupos de G. Son equivalentes:
(a) HK es un subgrupo de G.
(b) $HK = KH$.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Si HK es un subgrupo de G, para $h \in H$ y $k \in K$ se verifica $kh = (h^{-1}k^{-1})^{-1} \in HK$, luego $KH \subseteq HK$. Si consideramos ahora hk tenemos $(hk)^{-1} \in HK$ por ser HK un subgrupo de G, por tanto existen $h_1 \in H$ y $k_1 \in K$ tales que $(hk)^{-1} = h_1k_1$, y entonces tenemos $hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$, luego $HK \subseteq KH$.
(b) $\Rightarrow$ (a). Supongamos que $HK = KH$, entonces para $h_1k_1, h_2k_2 \in HK$ tenemos:

$$(h_1k_1)(h_2k_2)^{-1} = (h_1k_1)(k_2^{-1}h_2^{-1}) = h_1(k_1(k_2^{-1}h_2^{-1})) =$$

$$= h_1((k_1k_2^{-1})h_2^{-1}) = h_1(hk) = (h_1h)k \in HK,$$

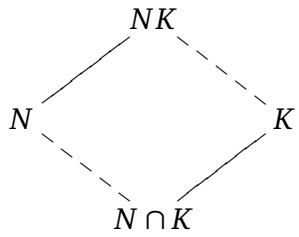
donde $hk = (k_1k_2^{-1})h_2^{-1}$. Entonces HK es un subgrupo de G. □

Corolario. 6.10.
Sea G un grupo, K un subgrupo de G y N un subgrupo normal de G, entonces NK es un subgrupo de G.

Teorema. 6.11. (Segundo Teorema de Isomorfía)
Sea G un grupo, K un subgrupo de G y N un subgrupo normal de G, entonces $N \cap K$ es un subgrupo normal de K y existe un isomorfismo entre los grupos $K/(N \cap K)$ y $(NK)/N$.

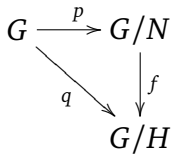
DEMOSTRACIÓN. Llamamos g al homomorfismo inclusión de K en G y p a la proyección canónica de G en G/N. Tenemos $\mathrm{Ker}(pg) = N \cap K$. Además $\mathrm{Im}(pg) = \{Nk \mid k \in K\}$, y por la correspondencia dada por el Teorema (6.8.), aplicada a p, tenemos $\mathrm{Im}(pg) = (NK)/N$. Por tanto $N \cap K$ es un subgrupo normal de K, y por el Primer Teorema de Isomorfía existe un isomorfismo de grupos entre $K/(N \cap K)$ y $(NK)/N$. □

El segundo teorema de isomorfía se llama también **Teorema del paralelogramo** ya que los lados paralelos en el siguiente diagrama producen grupos isomorfos.



Teorema. 6.12. (Tercer Teorema de Isomorfía)
Sea G un grupo y N un subgrupo normal de G. Si H es un subgrupo normal de G verificando $N \leq H \leq G$, entonces existe un isomorfismo entre los grupos $\dfrac{G/N}{H/N}$ y G/H.

DEMOSTRACIÓN. Consideramos la proyección canónica $p : G \longrightarrow G/N$, por el Teorema 6.8. $p_*(H) = H/N$ es un subgrupo normal de G/N. Llamamos $q : G \longrightarrow G/H$ a la proyección canónica, tenemos el diagrama



Por ser $\mathrm{Ker}(p) = N \leq H = \mathrm{Ker}(q)$, existe un único homomorfismo de grupos $f : G/N \longrightarrow G/H$ verificando $q = fp$. Por ser q un homomorfismo sobreyectivo, también f lo es; el núcleo de f es precisamente H/N, y por tanto aplicando el Primer Teorema de Isomorfía tenemos:

$$\frac{G/N}{H/N} \cong \frac{G/N}{\mathrm{Ker}(f)} \cong \mathrm{Im}(f) = G/H.$$

□

El tercer teorema de isomorfía se llama también **Teorema del doble cociente**.

Proposición. 6.13.
Sea G un grupo y N_1, N_2 subgrupos normales de G verificando $N_1N_2 = G$ y $N_1 \cap N_2 = \{e\}$, entonces existe un isomorfismo $f : N_1 \times N_2 \longrightarrow G$ dado por $f(n_1, n_2) = n_1n_2$.

DEMOSTRACIÓN. Así definida f es una aplicación, para comprobar que es un homomorfismo de grupos, sean (n_1,n_2), $(h_1,h_2)\in N_1\times N_2$, entonces

$$f(n_1,n_2)f(h_1,h_2)=(n_1n_2)(h_1h_2)=n_1(n_2h_1)h_2=(*),$$

consideramos el elemento $n_2h_1n_2^{-1}h_1^{-1}$, se verifica:

$$n_2(h_1n_2^{-1}h_1^{-1})\in N_2 \text{ y}$$

$$(n_2h_1n_2^{-1})h_1^{-1}\in N_1,$$

por lo tanto es igual a e, y se tiene $n_2h_1=h_1n_2$, y entonces

$$(*)=n_1(h_1n_2)h_2=(n_1h_1)(n_2h_2)=f(n_1h_1,n_2h_2).$$

Falta probar que f es una aplicación biyectiva. Su núcleo es:

$$\begin{aligned}\mathrm{Ker}(f)&=\{(n_1,n_2)\in N_1\times N_2 \mid n_1n_2=e\}\\&=\{(n_1,n_2)\in N_1\times N_2 \mid n_2=n_1^{-1}\}\\&=\{(n_1,n_1^{-1})\in N_1\times N_2 \mid n_1\in N_1\}=\{(e,e)\},\end{aligned}$$

por lo tanto es inyectivo. Y evidentemente es sobreyectiva. □

Si un grupo G contiene dos subgrupos normales N_1 y N_2 verificando las condiciones de la Proposición, se dice que G es el **producto directo interno** de los subgrupos N_1 y N_2. Esta situación puede generalizarse a una familia finita de subgrupos normales.

Corolario. 6.14.
Sea G un grupo y $\{N_1,\dots,N_r\}$ subgrupos normales de G verificando $N_1\dots N_r = G$ y $N_i\cap N_1\dots N_{i-1}N_{i+1}\dots N_r=\{e\}$, entonces existe un isomorfismo $f : N_1\times\dots\times N_r\longrightarrow G$ dado por $f(n_1,\dots,n_r)=n_1\dots n_r$.

Lema de la mariposa

Lema. 6.15. (Regla de Dedekind)
Sea G un grupo y A,B y C subgrupos de G tales que $C\subseteq B$, entonces

$$(A\cap B)C=AC\cap B.$$

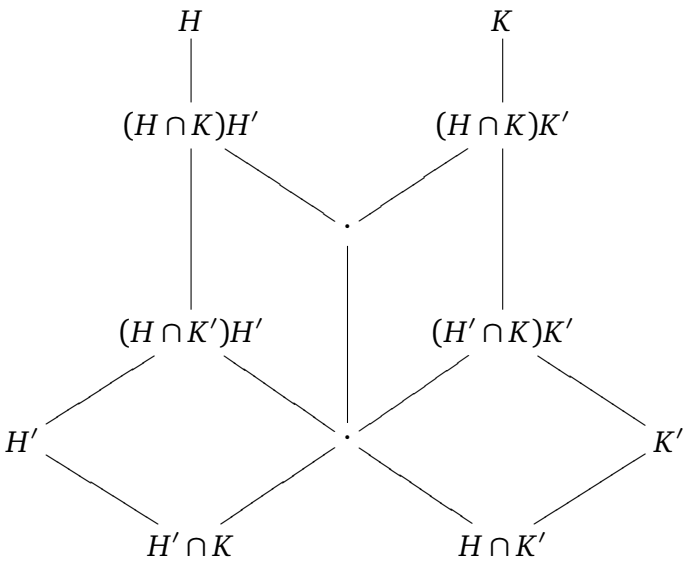
DEMOSTRACIÓN. Supongamos que $x \in (A\cap B)C$, entonces $x = ac$, con $a \in A\cap B$ y $c \in C$, entonces $ac \in AC$, y ya que $C \subseteq B$, tenemos $ac \in B$, luego $ac \in AC \cap B$. Supongamos ahora que $x \in AC \cap B$, entonces $x \in B$ y $x = ac$, con $a \in A$ y $c \in C$, ya que $C \subseteq B$, se tiene $c \in B$, y por tanto $a = xc^{-1} \in B$, tenemos entonces que $x = ac \in (A\cap B)C$. □

La regla de Dedekind se conoce también como **Ley modular**.

Observación. 6.16.
Recordar que AB no es en general un subgrupo de G aunque A y B lo sean.

Proposición. 6.17. (Lema de Zassenhaus o de la mariposa)
Sea G un grupo y H, H', K, K' subgrupos de G tales que H' es normal en H y K' es normal en K, entonces se verifica:

(1) $(H' \cap K)K' \lhd (H \cap K)K'$ *es un subgrupo normal;*
(2) $(H \cap K')H' \lhd (H \cap K)H'$ *es un subgrupo normal;*
(3) $\dfrac{(H \cap K)K'}{(H' \cap K)K'} \cong \dfrac{(H \cap K)H'}{(H \cap K')H'}$.



DEMOSTRACIÓN. (1) Tenemos que $H \cap K$ y K' son subgrupos de K y K' es normal, entonces por el segundo teorema de isomorfía tenemos que $(H \cap K) \cap K' = H \cap K'$ es un subgrupo normal de $H \cap K$, y existe un isomorfismo

$$\frac{H \cap K}{H \cap K'} \cong \frac{(H \cap K)K'}{K'}. \tag{II.1}$$

De forma análoga tenemos que $H' \cap K$ es normal en $H \cap K$, y por tanto $(H' \cap K)(H \cap K')$ es un subgrupo normal de $H\cap$K. A través del isomorfismo (II.1) el subgrupo $(H' \cap K)(H \cap K')$ corresponde a $(H' \cap K)(H \cap K')K' = (H' \cap K)K'$, y por lo tanto es un subgrupo normal de $(H \cap K)K'$.

(2) El resultado es simétrico al anterior.
(3) Por el tercer teorema de isomorfía y la regla de Dedekind tenemos:

$$\begin{aligned}
\frac{(H\cap K)K'}{(H'\cap K)K'} &\cong \frac{(H\cap K)K'/K'}{(H'\cap K)K'/K'} && \text{tercer teorema de isomorfía}\\
&\cong \frac{(H\cap K)K'/K'}{(H'\cap K)(H\cap K')K'/K'} && \text{identificación anterior}\\
&\cong \frac{(H\cap K)/(H\cap K')}{(H'\cap K)(H\cap K')/[(H'\cap K)(H\cap K')]\cap K'} && \text{segundo teorema de isomorfía}\\
&\cong \frac{(H\cap K)/(H\cap K')}{(H'\cap K)(H\cap K')/(H\cap K')} && \text{regla de Dedekind}\\
&\cong \frac{(H\cap K)}{(H'\cap K)(H\cap K')}
\end{aligned}$$

El resultado se completa también por simetría. □

Subgrupos especiales

Un subgrupo N de un grupo G es normal si para cada automorfismo interno φ de G resulta que $\varphi(N)\subseteq N$. Vamos a definir nuevos tipos de subgrupos normales.
Un subgrupo H de G se llama **característico** si $\phi(H)\subseteq H$ para cada automorfismo ϕ de G. Es claro que cada subgrupo característico es un subgrupo normal.
Un subgrupo H de G se llama **totalmente invariante** si $f(H)\subseteq H$ para cada endomorfismo f de G.

El centro

El primer ejemplo de subgrupo especial que vamos a estudiar es el centro. Si G es un grupo, se define $Z(G)$, el **centro** de G, como

$$Z(G)=\{a\in G \mid ax=xa \text{ para todo } x\in G\}.$$

Evidentemente G es abeliano si y sólo si $G=Z(G)$. En general $Z(G)$ puede ser trivial (por ejemplo para $G=S_n$, $n\geq 3$). Pero algunos tipos especiales de grupos (grupos abelianos, p-grupos, grupos nilpotentes) tienen siempre un centro no trivial. Para grupos abelianos es evidente; en los otros casos lo demostraremos mas adelante.

Lema. 6.18.
El centro es un subgrupo característico de G.

El i–ésimo centro

Otro ejemplo de subgrupo especial es el i–ésimo centro. Si G es un grupo, se define $Z_i(G)$, el **i-ésimo centro** de G, por recurrencia como:

$$Z_0=1 \text{ y}$$
$$\frac{Z_{i+1}(G)}{Z_i(G)}=Z\left(\frac{G}{Z_i(G)}\right) \text{ para cada } i\in\mathbb{N}.$$

Lema. 6.19.
El grupo $Z_i = Z_i(G)$ es un subgrupo característico de G.

DEMOSTRACIÓN. Hacer inducción sobre i. □

El hipercentro

Si G es un grupo, se define $H(G)$, el **hipercentro** de G, mediante:

$$H(G) = \cup_0^\infty Z_i.$$

Lema. 6.20.
$H(G)$ es un subgrupo característico de G.

El concepto de centro de un grupo admite dos generalizaciones interesantes:

Centralizador y normalizador

Sea S un subconjunto de un grupo G. Llamamos **centralizador** de S en G al conjunto

$$C_G(S) = \{x \in G \mid \ xa = ax \text{ para cada } a \in S\}$$

Llamamos **normalizador** de S en G al conjunto

$$N_G(S) = \{x \in G \mid \ xS = Sx\}$$

Lema. 6.21.
(1) El normalizador $N_G(S)$ es un subgrupo de G.
(2) El centralizador $C_G(S)$ es un subgrupo normal de $N_G(S)$.
(3) Si S es un subgrupo de G, entonces S es un subgrupo normal de $N_G(S)$.

Teorema. 6.22.
Sea G un grupo $H \subseteq K$ subgrupos suyos. Entonces H es normal en K si y sólo si $K \subseteq N_G(H)$.

Este teorema caracteriza al normalizador $N_G(H)$ como el mayor subgrupo de G en el que H es normal.

Teorema. 6.23.
Sea G un grupo y H un subgrupo suyo. Existe un monomorfismo:

$$f : \frac{N_G(H)}{C_G(H)} \longrightarrow \mathrm{Aut}(H)$$

definido por $f(\overline{a}) = \varphi_a$ (el automorfismo interno definido por a).

Corolario. 6.24.
Llamamos $\mathrm{Int}(G)$ *al grupo de los automorfismo internos de G. Entonces existe un isomorfismo* $\mathrm{Int}(G) \cong G/Z(G)$.

Lema. 6.25.
Sea $f : G \to H$ un epimorfismo de grupos. Entonces $f(Z(G)) \subset Z(H)$.

Lema. 6.26.
Sea G un grupo y H un subgrupo de G. Entonces $Z(H) = C_G(H) \cap H$.

Teorema. 6.27.
Sea $H \subseteq G$ con H abeliano. Entonces $HZ(G)$ es un grupo abeliano

Corolario. 6.28.
Sea G un grupo con centro $Z(G)$ y $x \in G$ tal que $x \notin Z(G)$. El grupo $\langle Z(G), x\rangle$ es abeliano.

Corolario. 6.29.
Si G no es abeliano, el cociente $G/Z(G)$ no es cíclico.

Subgrupo conmutador

Sea G un grupo arbitrario. Para dos elementos $x, y \in G$ definimos su **conmutador** como el elemento $[x, y] = xyx^{-1}y^{-1}$. El conmutador recibe tal nombre porque verifica

$$[x, y]yx = xy.$$

Lema. 6.30.
Para cualquier homomorfismo $f : G \longrightarrow H$ se verifica $f([x, y]) = [f(x), f(y)]$.

Como $[x, y]^{-1} = [y, x]$, el inverso de un conmutador es un conmutador. Sin embargo el producto de dos conmutadores no tiene porqué ser un conmutador. Llamamos **(primer) subgrupo conmutador** o **(primer) subgrupo derivado** de G al subgrupo generado por todos los conmutadores de G; se representa por $[G, G]$, $\Gamma(G)$ ó G'.

Lema. 6.31.
Para cada grupo G se tiene que $[G, G]$ es un subgrupo totalmente invariante de g.

Es inmediato comprobar que G es un grupo abeliano si y sólo si $[G, G] = 1$.
El grupo cociente $G/[G, G]$ se representa por G^{ab} y se llama **grupo abelianizado** de G.

Teorema. 6.32. (Propiedad universal del grupo abelianizado)
Sea G un grupo y $p : G \to G^{ab}$ el epimorfismo canónico. Para todo grupo abeliano A y par todo homomorfismo $f : G \to A$ existe un único homomorfismo $\overline{f} : G^{ab} \to A$ tal que $f = \overline{f}\,p$.
Además $\mathrm{Im}(f) = \mathrm{Im}(\overline{f})$ *y* $\mathrm{Ker}(\overline{f}) = \mathrm{Ker}(f)/[G,G]$.

Corolario. 6.33.
Sea N un subgrupo normal de un grupo G. El grupo cociente G/N es abeliano si y sólo si $[G,G] \subseteq N$.

El teorema anterior y su corolario pueden parafrasearse de dos formas:
(1) El grupo $[G,G]$ es el mínimo subgrupo normal de G tal que el cociente es abeliano;
(2) G^{ab} es el mayor grupo cociente abeliano de G.
También suele decirse que G^{ab} es la "*imagen abeliana*" de G (el grupo abeliano que más se parece a G), de ahí le viene el nombre.
Todo homomorfismo de grupos $f : G \to H$ induce un homomorfismo de grupos $f^{ab} : G^{ab} \to H^{ab}$.
Sean H, K subgrupos de G. Definimos el **conmutador** de H y K como el subgrupo $[H,K]$ de G generado por los conmutadores $[x,y]$ con $x \in H$, $y \in K$.

Lema. 6.34.
Si H y K son subgrupos característicos de un grupo G, entonces $[H,K]$ es un subgrupo característico de G.

Definimos el **i-ésimo subgrupo derivado de** G por recurrencia mediante:

$$G^0 = G; \qquad \text{y} \qquad G^{(i+1} = [G^{(i}, G^{(i}] \text{ para cada } i \in \mathbb{N}$$

Definimos el **i-ésimo subgrupo conmutador de** G por recurrencia mediante:

$$\Gamma^0(G) = G; \qquad \text{y} \qquad \Gamma^{i+1}(G) = [\Gamma^i(G), G] \text{ para cada } i \in \mathbb{N}$$

Llamamos **hiperconmutador** de G al grupo $\Gamma(g) = \cap_0^\infty \Gamma^i(G)$

Lema. 6.35.
Para cada grupo G se verifica que $G^{(i}$, $\Gamma^i(G)$ y $\Gamma(G)$ son subgrupos totalmente invariantes en G.

7. Grupos cíclicos

El grupo $\mathbb{Z}$ tiene una propiedad de interés que esta recogida en el siguiente Lema.

Lema. 7.1.
Sea G un grupo, para cada elemento $a \in G$ existe un homomorfismo de grupos $f_a : \mathbb{Z} \longrightarrow G$ definido por $f_a(n) = a^n$ para cada $n \in \mathbb{Z}$.

DEMOSTRACIÓN. Si existe f_a y verifica $f_a(n) = a^n$, entonces se verifica:

$$f_a(n+m) = a^{n+m} = a^n a^m = f_a(n) f_a(m),$$

luego f_a es un homomorfismo de grupos. □

En la situación anterior la imagen de f_a es un subgrupo de G,

$$\mathrm{Im}(f_a) = \{a^n \in G \mid \ n \in \mathbb{Z}\} = \langle a \rangle,$$

y es el subgrupo cíclico de G generado por a. Como consecuencia, si G es un grupo cíclico, entonces existe un elemento $a \in G$ tal que $G = \langle a \rangle$, y por tanto todo grupo cíclico es un cociente del grupo $\mathbb{Z}$ de los números enteros. Se deduce fácilmente que todo grupo cíclico es abeliano.
Por lo tanto para estudiar los grupos cíclicos se han de estudiar los cocientes de $\mathbb{Z}$, y para ello es necesario estudiar los subgrupos de $\mathbb{Z}$. Este estudio ya fue realizado en el Ejercicio (4.21.), sin embargo es conveniente desarrollarlo aquí en detalle.

Lema. 7.2.
Todo subgrupo del grupo aditivo $\mathbb{Z}$ de los números enteros es de la forma $n\mathbb{Z} = \{nr \in \mathbb{Z} \mid \ r \in \mathbb{Z}\}$ para algún $n \in \mathbb{N}$.

DEMOSTRACIÓN. Sea H un subgrupo de $\mathbb{Z}$, si $H \neq 0$, entonces $L = (H \cap \mathbb{N}) \setminus \{0\} \neq \emptyset$. Por lo tanto existe un mínimo de L. Sea $n = \mathrm{mín}(L)$. Es claro que $\langle n \rangle = n\mathbb{Z} \leq H$. Dado $m \in H$, aplicando el algoritmo de la división, existen $q, r \in \mathbb{Z}$ tales que $m = nq + r$ con $0 \leq r < n$. Si $r \neq 0$, entonces $r = m - nq \in (H \cap \mathbb{N}) \setminus \{0\}$, lo que es una contradicción; por lo tanto $r = 0$. Tenemos entonces $m = nq \in \langle n \rangle = n\mathbb{Z}$, y $H = n\mathbb{Z}$. □

Dado un grupo cíclico $G = \langle a \rangle$, el homomorfismo $f_a : \mathbb{Z} \longrightarrow G$ es sobreyectivo y tiene por núcleo un subgrupo de $\mathbb{Z}$, el cual será de la forma $n\mathbb{Z}$, para algún $n \in \mathbb{N}$. Si $n = 0$, entonces $G \cong \mathbb{Z}$, y si $n \neq 0$, entonces $G \cong \mathbb{Z}/n\mathbb{Z}$.

3302-03.tex

Lema. 7.3.
Sea G un grupo y $a \in G$ distinto de e. Son equivalentes:
(a) a tiene orden finito n.
(b) $\mathrm{Ker}(f_a) = n\mathbb{Z}$, con $n \neq 0$.
(c) $n \neq 0$ es el menor entero positivo tal que $a^n = e$.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b) Si a tiene orden finito n, entonces el grupo $\langle a \rangle$ tiene n elementos. Ya que existe $m \in \mathbb{N}$ tal que $\langle a \rangle \cong \mathbb{Z}/m\mathbb{Z}$, donde $m\mathbb{Z} = \mathrm{Ker}(f_a)$, vamos a comprobar que $\mathbb{Z}/m\mathbb{Z}$ tiene m elementos cuando $m \neq 0$, y por lo tanto se tendrá que $n = m$ y $\mathrm{Ker}(f_a) = n\mathbb{Z}$. Es claro que $m \neq 0$, ya que en caso contrario $\langle a \rangle$ tendría infinitos elementos. Dado un elemento $x \in \mathbb{Z}/m\mathbb{Z}$, vamos a comprobar que existe un representante $r \in \mathbb{Z}$ de x tal que $0 \leq r < m$; dado un representante s de x, por el algoritmo de la división, existen $q, r \in \mathbb{Z}$ tales que $s = mq + r$ y $0 \leq r < m$, entonces $r - s = mq \in m\mathbb{Z}$, y se tiene $x = r + m\mathbb{Z}$. Para comprobar que $\mathbb{Z}/m\mathbb{Z}$ tiene m elementos basta entonces comprobar que si $0 \leq r_1, r_2 < m$ y $r_1 \neq r_2$, entonces $r_1 + m\mathbb{Z} \neq r_2 + m\mathbb{Z}$; supongamos que $r_1 + m\mathbb{Z} \neq r_2 + m\mathbb{Z}$ y $0 \leq r_1, r_2 \leq m$, entonces $r_1 - r_2 \in m\mathbb{Z}$, pero $|r_1 - r_2| < m$, lo que implica que $r_1 - r_2 = 0$, tenemos pues $r_1 = r_2$.
(b) $\Rightarrow$ (c). Es consecuencia de la demostración del Lema 7.2..
(c) $\Rightarrow$ (a) Consideremos el subgrupo $\langle a \rangle$ de G generado por a, se tiene que $\langle a \rangle = \{a^r \in G \mid r \in \mathbb{Z}\}$. Si n es el menor entero positivo que verifica $a^n = e$, entonces $\mathrm{Ker}(f) = n\mathbb{Z}$, y por tanto $\langle a \rangle \cong \mathbb{Z}/n\mathbb{Z}$ tiene n elementos, luego el orden de a es igual a n. □

Corolario. 7.4.
Sea G un grupo finito de orden m, y sea $a \in G$ un elemento de G de orden n, entonces n divide a m y se verifica $a^m = e$.

DEMOSTRACIÓN. Por el Teorema de Lagrange el orden de cada subgrupo de G divide al orden de G. Si $n = \mathrm{ord}(a) = |\langle a \rangle|$, tenemos que $n \mid m$, luego existe $k \in \mathbb{Z}$ tal que $m = nk$ con $k > 0$, entonces

$$a^m = a^{nk} = (a^n)^k = e^k = e.$$

□

Lema. 7.5.
(1) Todo cociente de un grupo cíclico es un grupo cíclico.
(2) Todo subgrupo de un grupo cíclico es un grupo cíclico.

DEMOSTRACIÓN. (1) Supongamos que G es un grupo cíclico y que $f : G \longrightarrow G'$ es un homomorfismo sobreyectivo de grupos, sea $a \in G$ un generador de G, entonces $f(a)$ es un generador de G', y por lo tanto G' es un grupo cíclico.

(2) Supongamos que G es un grupo cíclico, entonces existe un homomorfismo de grupos sobreyectivo $f : \mathbb{Z} \longrightarrow G$. Por el Lema 5.5., los subgrupos de G están en correspondencia biunívoca con los subgrupos de $\mathbb{Z}$ que contienen a $\mathrm{Ker}(f)$; por esta correspondencia la imagen de un subgrupo $n\mathbb{Z}$ de $\mathbb{Z}$ que contiene a $\mathrm{Ker}(f)$ es $n\mathbb{Z}/Ker(f)$, por tanto es un cociente de $n\mathbb{Z}$, y es un grupo cíclico. □

Lema. 7.6.
Sea G un grupo cíclico de orden finito m. Para cada divisor n de m existe un único subgrupo N de G de orden n. Si $a \in G$ es un generador de G, entonces $a^{\frac{m}{n}}$ es un generador de N. Además, todos los subgrupos de G son de esta forma.

DEMOSTRACIÓN. Si n es un divisor de m, y $a \in G$ es un generador de G, llamamos $b = a^{\frac{m}{n}}$, entonces $\langle b \rangle$ es un subgrupo de G, y su orden es menor ó igual que n. Si r es un entero positivo menor que n verificando $b^r = e$, entonces $e = b^r = (a^{\frac{m}{n}})^r = a^{mr/n}$, luego $\frac{mr}{n}$ es un múltiplo de m, y como consecuencia $\frac{r}{n}$ es un número entero positivo, lo que implica que $n = r$; como consecuencia el orden de $b = a^{\frac{m}{n}}$ es igual a n, y G contiene un subgrupo de orden n. Supongamos ahora que H es un subgrupo de G de orden s, entonces s es un divisor de m, llamamos $b = a^{\frac{m}{s}}$, vamos a comprobar que H es el subgrupo de G generado por b. Sea t el menor entero positivo tal que $a^t \in H$; si u es otro entero positivo verificando $a^u \in H$, entonces por el algoritmo de la división t divide a u, y para cada elemento $a^u \in H$ se verifica que existe v tal que $u = tv$, y por tanto $a^u = a^{tv} = (a^t)^v$, luego a^t es un generador de H y t es un divisor de m. Además si s es el orden de a^t, entonces s es el menor entero positivo tal que $ts = m$, y por tanto $t = m/s$; como consecuencia $b = a^{m/s} = a^t$ es un generador de H. □

Corolario. 7.7.
Sea G un grupo cíclico de orden p^m generado por $a \in G$, con p un número entero primo positivo y m un entero positivo, entonces los únicos subgrupos de G son los generados por los elementos a^{p^r}, para todo $0 \leq r \leq m$, y tienen de orden p^{m-r}. Además los subgrupos de G forman una cadena.

Vamos a estudiar el número de generadores de un grupo cíclico. Sea G un grupo cíclico infinito, entonces G es isomorfo a $\mathbb{Z}$ el grupo de los números enteros no nulos, y por tanto G tiene dos generadores, la imagen de 1 y la imagen de -1. Si G es un grupo cíclico finito el problema es más complicado, vamos a resolverlo. Definimos una aplicación

$$\varphi : \mathbb{N}^+ \longrightarrow \mathbb{N}$$

mediante:

$$\begin{aligned}\varphi(1) &= 1\\ \varphi(n) &= \text{número de enteros positivos primos relativos con } n\\ &\qquad \text{y menores que } n, \text{ si } n \geq 2.\end{aligned}$$

φ se llama la **función tociente de Euler**.

Lema. 7.8.
Sea G un grupo no nulo cíclico de orden finito m. El número de elementos de G que generan G es exactamente $\varphi(m)$. Además, si $a \in G$ es un generador, entonces todos los generadores de G son de la forma a^r, con $1 \leq r < m$ primo relativo con m.

DEMOSTRACIÓN. Sea $a \in G$ un generador de G y G un grupo cíclico no nulo de orden m, y supongamos que $b = a^r$, con $1 \leq r < m$, es otro generador de G, entonces el orden de b es m. Si $d > 0$ es un máximo común divisor de r y m, entonces existen números enteros positivos r' y m' tales que $r = dr'$ y $m = dm'$. Se verifica

$$b^{m'} = (a^r)^{m'} = a^{rm'} = a^{dr'm'} = a^{mr'} = (a^m)^{r'} = e^{r'} = e,$$

luego $m \mid m'$, tenemos por tanto $m = m'$, y $d = 1$, entonces m y r son primos relativos. Supongamos ahora que r y m son números enteros positivos primos relativos y que $a \in G$ es un generador de G, para probar que a^r es un generador de G, supongamos que $(a^r)^s = e$, entonces $a^{rs} = e$, y por tanto $m \mid rs$, por ser m y r primos relativos tenemos que $m \mid s$, y por tanto el orden de a^r es m, luego es un generador de G. □

8. Grupos simétricos II

Lema. 8.1.
Sea $\sigma \in S_n$ un ciclo, σ es de longitud r si, y sólo si, σ es de orden r.

DEMOSTRACIÓN. ($\Rightarrow$). Si $r = 1$, entonces el resultado es cierto. Supongamos ahora que $r > 1$, entonces $\sigma = (x_1 \dots x_r)$, hacemos el siguiente convenio, $x_j = x_h$, cuando $1 \leq h \leq r$ y $j - h \in r\mathbb{Z}$. Para $h \leq r$ se tiene: si $h = 1$, $\sigma^1(x_i) = \sigma(x_i) = x_{i+1}$, para todo índice i. Suponemos que este resultado es cierto para algún $h \leq r$, entonces

$$\sigma^{h+1}(x_i) = \sigma\sigma^h(x_i) = \sigma(x_{i+h}) = x_{i+(h+1)}.$$

Luego tenemos $\sigma^h(x_i) = x_{i+h}$ para cada h y cada i. En particular $\sigma^h(x_1) = x_{h+1}$, luego si $h < r$ se tiene $\sigma^h \neq 1$, y $\sigma^r = 1$, luego el orden de σ es r.

($\Leftarrow$). Si σ es un ciclo de orden r, entonces $\sigma = (x_1 \dots x_t)$ para algún entero positivo t. Si $r = 1$, entonces $x_1 = \dots = x_t$ y $\sigma = 1$. Si $1 \leq s < r$, entonces $\sigma^s \neq 1$ y $\sigma^s(x_i) = x_{i+s} \neq x_i$, luego t es el menor entero positivo tal que $\sigma^t = 1$, entonces $r = t$. □

Corolario. 8.2.
El orden de una permutación σ es el mínimo común múltiplo de las longitudes de sus ciclos disjuntos.

DEMOSTRACIÓN. Si tenemos $\sigma = \gamma_1 \cdots \gamma_s$, con γ_i ciclos disjuntos de longitudes r_i respectivamente. Llamamos $r = \text{mcm}\{r_1, \dots, r_s\}$, $0 < r$. Es claro que $\sigma^r = 1$. Si $\sigma^t = 1$, entonces $1 = (\gamma_1 \cdots \gamma_s)^t = \gamma_1^t \cdots \gamma_s^t$, y por ser los γ_i ciclos disjuntos dos a dos se tiene $\gamma_i^t = 1$, para cada índice i, luego t es un múltiplo de r_i para cada índice i, entonces $r|t$, y por tanto r es el orden de σ. □

Dada una permutación $\sigma \in S_n$, si $\sigma \neq 1$, entonces $\sigma = \gamma_1 \cdots \gamma_s$, con γ_i ciclos disjuntos dos a dos. Definimos:

$$N(\sigma) = 1, \qquad \text{si } \sigma = 1.$$
$$N(\sigma) = (\text{long}(\gamma_1) - 1) + \cdots + (\text{long}(\gamma_s) - 1), \quad \text{si } \sigma \neq 1.$$

3302-04.tex

Lema. 8.3.
Para cada permutación $\sigma \in S_n$ y cada $x, y \in X$, $x \neq y$, se tiene que $N(\sigma)$ y $N((xy)\sigma)$ tienen distinta paridad.

DEMOSTRACIÓN. Dados $x, y \in X$, $x \neq y$, se verifica

$$(xy)(xc_1 \dots c_h y d_1 \dots d_k) = (y d_1 \dots d_k)(xc_1 \dots c_h),$$

para $c_1, \dots, c_h, d_1, \dots, d_k \in X$, todos distintos, si h ó k son nulos, entonces no existen los "ces" ó los "des" correspondientes. Entonces si $\sigma \neq 1$, se verifica:
Caso 1. Si x, e y forman parte de un mismo ciclo de σ, podemos suponer que este ciclo es γ_1, entonces:

$$\begin{aligned} N((xy)\sigma) &= N((xy)(xc_1 \dots c_h y d_1 \dots d_k)\gamma_2 \dots \gamma_s) \\ &= N((y d_1 \dots d_k)(xc_1 \dots c_h)\gamma_2 \dots \gamma_s) \\ &= k + h + (\text{long}(\gamma_2) - 1) + \cdots + (\text{long}(\gamma_s) - 1). \end{aligned}$$

$$N(\sigma) = (h + k + 1) + (\text{long}(\gamma_2) - 1) + \cdots + (\text{long}(\gamma_s) - 1),$$

y se tiene $N(\sigma) - N((xy)\sigma) = 1$.
Caso 2. Si sólo x forma parte de un ciclo de σ e y no forma parte de ninguno, entonces:

$$\begin{aligned} N((xy)\sigma) &= N((xy)(xc_1 \dots c_h)\gamma_2 \cdots \gamma_s) \\ &= N((xc_1 \dots c_h y)\gamma_2 \cdots \gamma_s) \\ &= h + 1 + (\text{long}(\gamma_2) - 1) + \cdots + (\text{long}(\gamma_s) - 1). \end{aligned}$$

$$N(\sigma) = h + (\text{long}(\gamma_2) - 1) + \cdots + (\text{long}(\gamma_s) - 1),$$

y se tiene $N(\sigma) - N((xy)\sigma) = -1$.
Caso 3. Si x forma parte de un ciclo e y forma parte de otro, podemos suponer que estos son respectivamente γ_2 y γ_1, entonces:

$$\begin{aligned} N((xy)\sigma) &= N((xy)(y d_1 \dots d_k)(xc_1 \dots c_h)\gamma_3 \cdots \gamma_s) \\ &= N((xc_1 \dots c_h y d_1 \dots d_k)\gamma_3 \cdots \gamma_s) \\ &= (k + h + 1) + (\text{long}(\gamma_3) - 1) + \cdots + (\text{long}(\gamma_s) - 1). \end{aligned}$$

$$N(\sigma) = k + h + (\text{long}(\gamma_3) - 1) + \cdots + (\text{long}(\gamma_s) - 1),$$

y se tiene $N(\sigma) - N((xy)\sigma) = -1$.
Caso 4. Si ni x ni y forman parte de los ciclos de σ, entonces $N((xy)\sigma) = N(\sigma) + 1$.
En los cuatro casos tenemos que la paridad de $N(\sigma)$ y de $N((xy)\sigma)$ es distinta. Igual resultado tenemos si $\sigma = 1$. □

Corolario. 8.4.
Dada una permutación $\sigma \in S_n$, el número de trasposiciones que aparecen en una factorización de σ en producto de trasposiciones tiene siempre la misma paridad que $N(\sigma)$.

DEMOSTRACIÓN. Supongamos que $\sigma = \tau_1 \cdots \tau_s$ es una factorización de σ en producto de trasposiciones, entonces $N(\sigma)$, $N(\tau_2\tau_1\sigma), \ldots, N(\tau_{2h}\cdots\tau_2\tau_1\sigma)$, tienen la misma paridad, y ésta es distinta de la de $N(\tau_1\sigma), \ldots, N(\tau_{2h+1}\cdots\tau_2\tau_1\sigma)$. Luego si s es un número par, entonces $N(1) = N(\tau_s \ldots \tau_1\sigma)$ tiene la misma paridad que $N(\sigma)$, y por tanto éste es un número par. Si s es un número impar, entonces $N(\tau_s) = (\tau_{s-1} \ldots \tau_2\tau_1\sigma)$ tiene la misma paridad que $N(\sigma)$, luego éste es un número impar. □

Una permutación $\sigma \in S_n$ se llama **par** si $N(\sigma)$ es un número par, y se llama impar si $N(\sigma)$ es un número impar.

Teorema. 8.5.
La aplicación sign : $S_n \longrightarrow \{1,-1\}$ *definida* $\text{sign}(\sigma) = (-1)^{N(\sigma)}$ *es un morfismo de grupos si consideramos en* $\{1,-1\}$ *la multiplicación.*

DEMOSTRACIÓN. Dadas dos permutaciones $\sigma,\ \nu \in S_n$, consideramos factorizaciones en producto de trasposiciones:

$$\sigma = \tau_1 \cdots \tau_s,\ \nu = \vartheta_1 \cdots \vartheta_t,$$

entonces $N(\sigma\nu)$ tiene la misma paridad que $s+t$, luego $\text{sign}(\sigma\nu) = (-1)^{s+t}$. Por otro lado $\text{sign}(\sigma) = (-1)^s$ y $\text{sign}(\nu) = (-1)^t$, y se tiene $\text{sign}(\sigma)\,\text{sign}(\nu) = (-1)^s(-1)^t = (-1)^{s+t}$. □

Corolario. 8.6.
Para $n > 1$ el conjunto $A_n \subseteq S_n$ de las permutaciones pares de S_n es un subgrupo normal y su orden es $(n!)/2$.

El grupo A_n se llama **subgrupo alternado** de S_n.

Una prueba alternativa

Proposición. 8.7.
Se considera la aplicación $\pi : S_n \longrightarrow \{1,-1\}$ definida por $\pi(\sigma) = (-1)^s$, siendo $\sigma = \tau_1 \cdots \tau_s$ una descomposición de σ como producto de trasposiciones. Entonces π es un homomorfismo de grupos.

DEMOSTRACIÓN. Supongamos que $\sigma = \tau_1 \cdots \tau_s = \omega_1 \cdots \omega_t$ son dos descomposiciones de σ como producto de trasposiciones. Entonces $1 = \tau_1 \cdots \tau_s \omega_t \cdots \omega_1$, y para comprobar que π está bien definida, basta basta ver que $s+t$ es un número par.

Para simplificar supongamos que $1 = \tau_1 \cdots \tau_h$ es un producto de trasposiciones; vamos a ver que h es un número par. Supongamos que $\tau_1 = (a\ x) \neq 1$, entonces a se mueve por alguna de las trasposiciones $\tau_2, \ldots, \tau_h$ ya que el producto $\tau_1 \cdots \tau_h$ es la identidad. Sea i el mínimo en $\{2, \ldots, h\}$ de forma que τ_i mueve a a; supongamos que $\tau_i = (a\ y)$.

Si τ_{i-1} y τ_i son disjuntos, entonces $1 = \tau_1 \cdots \tau_i \tau_{i-1} \cdots \tau_h$, y repitiendo este proceso las veces que sean necesarias podemos suponer, si $i \neq 2$, que τ_{i-1} y τ_i son siempre disjuntos.

Si τ_{i-1} y τ_i no son disjuntos, $i \neq 2$, supongamos que $\tau_{i-1} = (b\ x)$, entonces

$$\tau_{i-1}\tau_i = (b\ x)(a\ x) = (x\ a\ b) = (a\ b)(b\ x),$$

y conseguimos una expresión de 1 con el elemento a es el lugar $i-1$.

Después de un número finito de pasos llegamos a una expresión del tipo

$$1 = (a; x)(x\ z)\tau'_3 \cdots \tau'_h.$$

Si $x = z$, entonces $1 = \tau'_3 \cdots \tau'_h$. Si $x \neq z$, entonces $1 = (a\ z)(z\ y)\tau'_3 \cdots \tau'_h$, y hemos reducido el número de $a$es que aparecen en la expresión en uno. Repitiendo el proceso, el número de veces que sea necesario, podemos eliminar todas las ocurrencias de a; en este caso obtendremos una expresión del tipo $1 = \tau'_3 \cdots \tau'_h$.

Ahora aplicando inducción sobre h, se obtiene que siempre h tiene que ser un número par. □

9. Ejercicio propuestos

Homomorfismos de grupos

Ejercicio. 9.1.
Si G es un grupo, $a \in G$ y $f : G \longrightarrow G$ un homomorfismo de grupos, demostrar que para todo $n \in \mathbb{Z}$ se verifica $f(a^n) = f(a)^n$.
Ref.: 3302e_002 *SOLUCIÓN*

Ejercicio. 9.2.
Sea G un grupo. Demuestra que son equivalentes los siguientes enunciados:
(a) G es abeliano;
(b) La aplicación $f : G \longrightarrow G$ definida $f(x) = x^{-1}$ es un homomorfismo de grupos;
(c) La aplicación $f : G \longrightarrow G$ definida $f(x) = x^2$ es un homomorfismo de grupos.

Ref.: 3302e_003 *SOLUCIÓN*

Ejercicio. 9.3.
Se considera el grupo $\mathbb{Z}$ con la operación $*$ definida en el Ejercicio (4.8.), demuestra que es isomorfo a $\mathbb{Z}$ con la operación suma.
Ref.: 3302e_001 *SOLUCIÓN*

Ejercicio. 9.4.
Demostrar que los siguientes grupos son isomorfos:
(1) El subgrupo multiplicativo de $\mathbb{C}$ generado por i;

3302-09.tex

(2) El grupo $\mathbb{Z}_4$;
(3) El subgrupo de S_4 generado por

$$\sigma = \begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,4\,1 \end{pmatrix}.$$

Ref.: 3302e_004 SOLUCIÓN

Ejercicio. 9.5.
Si K es un cuerpo, definimos en K una operación binaria mediante:

$$a * b = a + b - ab,$$

para $a, b \in K$. Demuestra que el conjunto $F = K \setminus \{1\}$, junto con la operación $*$, es un grupo que es isomorfo al grupo multiplicativo $K^* = K - \{0\}$.
Ref.: 3302e_008 SOLUCIÓN

Ejercicio. 9.6.
Demuestra que los grupos $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$ no son isomorfos.
Ref.: 3302e_005 SOLUCIÓN

Ejercicio. 9.7.
Demuestra que únicamente existen dos automorfismos de $\mathbb{Z}$, uno el homomorfismo identidad, y otro el que aplica x en $-x$.
Ref.: 3302e_006 SOLUCIÓN

Ejercicio. 9.8.
Consideramos las aplicaciones de $F = \mathbb{R} \setminus \{0,1\}$ en F que llevan x en x, $\frac{1}{1-x}$, $\frac{x-1}{x}$, $\frac{1}{x}$, $1-x$, $\frac{x}{x-1}$ respectivamente.

(1) Demuestra que el conjunto formado por estas seis aplicaciones, junto con la composición de aplicaciones, es un grupo.
(2) Demuestra que este grupo es isomorfo al grupo S_3.

Ref.: 3302e_007 SOLUCIÓN

Ejercicio. 9.9.
Sea $\{G_i \mid i \in I\}$ una familia de grupos. En el conjunto producto cartesiano $\prod\{G_i \mid i \in I\}$ consideramos la operación definida en el Ejercicio (4.16.). Demuestra que las proyecciones canónicas $p_i : \prod_i G_i \longrightarrow G_i$ son homomorfismos de grupos.
Ref.: 3302e_009 SOLUCIÓN

Ejercicio. 9.10.
Sea G un grupo y $f \in \mathrm{Aut}(G)$, definimos $H = \{x \in G \mid f(x) = x\}$.
(1) Demuestra que H es un subgrupo de G.

*El subgrupo H se llama **subgrupo de los puntos fijos** por f.*
Sea $\mathbb{R}$ cuerpo de los números reales y $\mathrm{GL}_n(\mathbb{R})$ el grupo de las matrices cuadradas de n filas con determinante no nulo. Para $A \in \mathrm{GL}_n(\mathbb{R})$ llamamos A^t a la matriz traspuesta de A.
(2) Demuestra que la aplicación $f : \mathrm{GL}_n(\mathbb{R}) \longrightarrow \mathrm{GL}_n(\mathbb{R})$, definida por $f(A) = (A^{-1})^t$, es un automorfismo.
(3) Demuestra que el subgrupo de los puntos fijos es el conjunto de las matrices ortogonales.

*(Nota. Una matriz $A \in \mathrm{GL}_n(\mathbb{R})$ es **ortogonal** si $AA^t = 1$).*
Ref.: 3302e_010 SOLUCIÓN

Ejercicio. 9.11.
Sea G un grupo y $a \in G$.
(1) Demuestra que la aplicación $f : G \longrightarrow G$, definida $f(x) = axa^{-1}$ para todo $x \in G$, es un automorfismo de G.

Un automorfismo del tipo anterior se llama ***automorfismo interno****.*

(2) Demuestra que el conjunto $\mathrm{Int}(G)$ *de los automorfismos internos de* G *es un subgrupo de* $\mathrm{Aut}(G)$*.*
(3) Demuestra que $\mathrm{Int}(G)$ *es un grupo trivial si, y sólo si,* G *es un grupo abeliano.*

Ref.: 3302e_011 *SOLUCIÓN*

Ejercicio. 9.12.
Sea $f : G \longrightarrow H$ *un homomorfismo de grupos. Demuestra que* $\mathrm{ord}(a)$ *divide a* $\mathrm{ord}(f(a))$*, para cada* $a \in G$*, y que se da la igualdad si* f *es inyectiva.*
Ref.: 3303e_017 *SOLUCIÓN*

Ejercicio. 9.13.
Sea F *un cuerpo. Llamamos* $F^\times$ *al grupo multiplicativo de* F*, esto es,* $F^\times = F\backslash\{0\}$ *con la multiplicación como operación. Llamamos* F^+ *al grupo aditivo de* F*. Demuestra que no existe ningún isomorfismo* $F^\times \cong F^+$*.*
(NOTA. Considera la imagen de -1 *cuando la característica de* F *es distinta de 2.)*
Ref.: 3303e_018 *SOLUCIÓN*

Subgrupos normales y grupos cocientes

Ejercicio. 9.14.
Demuestra que si G *es un grupo, entonces todo subgrupo* $N \subseteq G$ *de índice 2 es un subgrupo normal.*
Ref.: 3302e_012 *SOLUCIÓN*

Ejercicio. 9.15.
Demuestra que si H *y* K *son subgrupo normales de un grupo* G*, entonces* $H \vee K$ *es un subgrupo normal de* G*.*
Ref.: 3303e_024 *SOLUCIÓN*

Ejercicio. 9.16.
Demuestra que si H, K y N son subgrupos de un grupo G tales que H es normal en K y N es normal en G, entonces $H \vee N$ es normal en $K \vee N$.
Ref.: 3303e_025 SOLUCIÓN

Ejercicio. 9.17.
Sea G un grupo y N, L subgrupos normales de G, demuestra que NL es un subgrupo normal de G.
Ref.: 3302e_013 SOLUCIÓN

Ejercicio. 9.18.
Sea G un grupo y N, L, H subgrupos de G de forma que L es un subgrupo normal de H y N es un subgrupo normal de G. Demuestra que NL es un subgrupo normal de NH.
Ref.: 3302e_014 SOLUCIÓN

Ejercicio. 9.19.
Demuestra que el grupo cociente $\mathbb{R}/\mathbb{Z}$ es isomorfo al grupo multiplicativo de los números complejos de módulo 1.
Ref.: 3302e_015 SOLUCIÓN

Ejercicio. 9.20.
Sea G un grupo y H, K subgrupos de G, demostrar que HK es una unión disjunta de clases a la derecha de H (y una unión disjunta de clases a la izquierda de K). Demuestra que si G es finito, entonces el número de estas clases es igual a $[K : H \cap K]$.
Ref.: 3302e_016 SOLUCIÓN

Ejercicio. 9.21.
Si cada subgrupo de un grupo G es normal, demuestra que cada dos elementos de órdenes primos relativos conmutan.
Ref.: 3302e_017 SOLUCIÓN

Ejercicio. 9.22.
Da un ejemplo de tres grupos $L \leq N \leq G$, de forma que L es normal en N, N normal en G y L no sea normal en G.
Ref.: 3302e_018 SOLUCIÓN

Ejercicio. 9.23.
Sea G un grupo finito y N un subgrupo normal de G de forma que $|N|$ y $[G:N]$ son primos relativos, demuestra que cada elemento de orden un divisor de $|N|$ está contenido en N.
Ref.: 3302e_019 SOLUCIÓN

Ejercicio. 9.24.
Sean G y G' dos grupos, N y N' subgrupos normales de G y G' respectivamente, y $f : G \to G'$ un homomorfismo de grupos verificando $f_*(N) \leq N'$. Demuestra que existe un único homomorfismo de grupos $f' : G/N \to G'/N'$ verificando $p'f = f'p$, donde p y p' son las respectivas proyecciones canónicas.
Ref.: 3302e_020 SOLUCIÓN

Ejercicio. 9.25.
Sea $f : G \longrightarrow G'$ un homomorfismo de grupos, demuestra que f es un homomorfismo inyectivo si, y sólo si, es un homomorfismo simplificable a la izquierda (esto es; para dos homomorfismos de grupos cualesquiera $h, k : G'' \longrightarrow G$ se tiene que $f\ h = f\ k$ implica $h = k$.
Ref.: 3302e_044 SOLUCIÓN

Ejercicio. 9.26.
Sean G un grupo, $N \subseteq G$ un subgrupo normal de G y $K \subseteq N$ un subgrupo característico de N, demuestra que K es un subgrupo normal de G. Compara con el Ejercicio (9.22.).
Ref.: 3302e_040 SOLUCIÓN

Ejercicio. 9.27.
Sean G un grupo, $N \subseteq G$ un subgrupo característico de G y $K \subseteq N$ un subgrupo característico de N, demuestra que K es un subgrupo característico de G.
Ref.: 3302e_041 SOLUCIÓN

Ejercicio. 9.28.
Se considera el conjunto de matrices

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R}) \mid \ a \neq 0 \right\}.$$

Demuestra que G, junto con el producto de matrices, es un grupo. Halla su centro.
Ref.: 3302e_043 SOLUCIÓN

Ejercicio. 9.29.
Demuestra que $D_4/Z(D_4)$ es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$, y que $D_6/Z(D_6)$ es isomorfo a S_3.
Ref.: 3302e_045 SOLUCIÓN

Ejercicio. 9.30.
Sea G un grupo finito y H un subgrupo propio de G. Demuestra que $G \neq \cup\{xHx^{-1} : \ x \in G\}$.
Ref.: 3302e_046 SOLUCIÓN

Ejercicio. 9.31.
Definimos $f : \mathbb{R}^+ \longrightarrow \mathbb{C}^*$ *mediante* $f(x) = \exp(2\pi x i)$.

(1) Demuestra que es un homomorfismo de grupos.
(2) Calcula la imagen y el núcleo de f.
(3) Haz lo mismo para $f_{|\mathbb{Q}^+}$.

Ref.: 3302e_047 SOLUCIÓN

Ejercicio. 9.32.
Sea G *un grupo en el que todos los elementos tienen orden* 2. *Demuestra:*

(1) Si $a \in G$ *entonces existe un subgrupo* $H \leq G$ *tal que* $G \cong \langle a \rangle \times H$.
(2) Si $a_1, \ldots, a_r \in G$ *verifican* $a_1 \neq 0$ *y* $a_{i+1} \notin \langle a_1, \ldots, a_i \rangle$, $1 \leq i < r$, *entonces existe un subgrupo* $H \subseteq G$ *tal que* $\langle a_1, \ldots, a_r \rangle \times H \cong G$. *Además se tiene unisomorfismo de grupos* $\langle a_1, \ldots, a_r \rangle \cong (\mathbb{Z}_2)^r$.

Ref.: 3302e_048 SOLUCIÓN

Ejercicio. 9.33.
Sea G *un grupo, llamamos* G^2 *al subgrupo de* G *generado por todos los elementos de la forma* x^2, *para todo* $x \in G$, *esto es,* $G^2 = \langle x^2 \mid x \in G \rangle$.

(1) Describe los elementos de G^2.
(2) Demuestra que G^2 *es un subgrupo totalmente invariante de* G, *por tanto normal.*
(3) Demuestra que G/G^2 *es un grupo abeliano.*

Ref.: 3302e_042 SOLUCIÓN

Ejercicio. 9.34.
Sea $n > 1$ *un número natural y sea* G *un grupo con la propiedad de que para todo par* $x, y \in G$ *se verifica* $(xy)^n = x^n y^n$. *Definimos*

$$H = \{x \in G \mid x^n = 1\} \text{ y}$$
$$K = \{x^n \mid x \in G\}.$$

Demuestra que H y K son subgrupos normales de G y que $|K| = [G : H]$.
Ref.: 3302e_081 SOLUCIÓN

Ejercicio. 9.35.
Sea G un grupo. Para cada $n \in \mathbb{N}$ definimos $H_n = \{x \in G \mid x^n = 1\}$.
(1) Demuestra que si G es abeliano, H_n es un subgrupo de G.
(2) Demuestra que si G no es abeliano, H_n no es necesariamente un subgrupo de G.

Ref.: 3303e_011 SOLUCIÓN

Grupos cíclicos

Ejercicio. 9.36.
Demuestra que todo grupo finito de orden un número primo es cíclico.
Ref.: 3302e_049 SOLUCIÓN

Ejercicio. 9.37.
Sea G un grupo, H un subgrupo de G y $c \in G$ un elemento de orden n. Si r es el menor entero positivo tal que $c^r \in H$, demuestra que $r|n$.
Ref.: 3302e_050 SOLUCIÓN

Ejercicio. 9.38.
Sea G un grupo cíclico generado por un elemento a, y sea G' un grupo cualquiera. Demuestra que cada homomorfismo $f : G \longrightarrow G'$ está determinado por la imagen del elemento a.
Ref.: 3302e_051 SOLUCIÓN

Ejercicio. 9.39.
Demuestra que si dos grupos cíclicos tienen el mismo orden, entonces son isomorfos.
Ref.: 3302e_052 SOLUCIÓN

Ejercicio. 9.40.
Comprueba los siguientes isomorfismos:
(1) $\mathrm{Aut}(\mathbb{Z}_6) \cong \mathbb{Z}_2$;
(2) $\mathrm{Aut}(\mathbb{Z}_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$;
(3) $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$, *si* p *es un entero primo positivo.*

Ref.: 3302e_053 SOLUCIÓN

Ejercicio. 9.41.
Demuestra las siguientes propiedades de la función totiente φ *de Euler.*

1. *Prueba que si* p *es un entero primo positivo, entonces* $\varphi(p^n) = p^n(1-1/p)$.
2. *Prueba que si* n *y* m *son números enteros positivos primos relativos, entonces* $\varphi(nm) = \varphi(n)\varphi(m)$.
3. *Prueba que para todo número entero positivo* n *se tiene* $\varphi(n) = n(1-1/p_1)\cdots(1-1/p_r)$, *donde* $p_1, \ldots, p_r$ *son todos los primos positivos que aparecen en la descomposición en factores primos de* n *con exponentes no nulos.*

Ref.: 3302e_054 SOLUCIÓN

Ejercicio. 9.42.
Encuentra todos los grupos cíclicos que tienen exactamente dos generadores.
Ref.: 3302e_055 SOLUCIÓN

Ejercicio. 9.43.
Sea $C_n = \langle a \mid a^n = 1\rangle = \{1, a, a^2, \cdots, a^{n-1}\}$ el grupo cíclico de orden n generado por a.

(1) Demuestra que para cualquier m, verificando $1 \leq m \leq n$, el elemento a^m es un generador de C_n si, y sólo si, $\text{mcd}\{m, n\} = 1$.
(2) Demuestra que el número de diferentes generadores de C_n es precisamente $\varphi(n)$.

Ref.: 3302e_021 SOLUCIÓN

Ejercicio. 9.44.
Sea $C_n = \langle a \mid a^n = 1\rangle$, un grupo cíclico de orden n.

(1) Demuestra que para todo divisor positivo m de n, el subgrupo cíclico $C_m = \langle a^{\frac{n}{m}}\rangle$ es de ese orden m.
(2) Demuestra que si $H \subseteq C_n$ es un subgrupo de orden m, y consideramos el número $s = \text{mín}\{x \mid 1 \leq x \leq n, a^x \in H\}$, entonces s es un divisor de n, que $H = \langle a^s\rangle$ y finalmente que $s = \frac{n}{m}$, de manera que $H = C_m$.
(3) Concluye con que la correspondencia $m \mapsto C_m$ establece un isomorfismo entre el retículo de los divisores positivos de n (donde la relación de orden es la de divisibilidad) y el de subgrupos de C_n.

Ref.: 3302e_022 SOLUCIÓN

Ejercicio. 9.45.
Sea G un grupo cíclico, si N es un subgrupo de G y se verifica $G/N \cong G$, prueba que $N = \{e\}$.
Ref.: 3302e_056 SOLUCIÓN

Ejercicio. 9.46.
Sea $f : G \longrightarrow G$ un homomorfismo de grupos. Si C es un subgrupo cíclico de G y se verifica $f_*(C) \subseteq C$, demuestra que para cualquier subgrupo H de C se verifica $f_*(H) \subseteq H$.
Como consecuencia cada subgrupo de un grupo cíclico es característico.
Ref.: 3302e_057 SOLUCIÓN

Ejercicio. 9.47.
Sea G un grupo y N un subgrupo normal de G que es cíclico, demuestra que todo subgrupo de N es un subgrupo normal de G.
Ref.: 3302e_058 SOLUCIÓN

Ejercicio. 9.48.
Si $\mathbb{Q}$ es el grupo aditivo de los números racionales, demuestra que cada subgrupo de $\mathbb{Q}$ con un sistema de generadores finito es cíclico. Demuestra que $\mathbb{Q}$ no es un grupo cíclico.
Ref.: 3302e_059 SOLUCIÓN

Ejercicio. 9.49.
Sea G un grupo de orden pq, siendo p y q números enteros positivos primos relativos, demuestra que si existen $a, b \in G$ tales que $\text{ord}(a) = p$, $\text{ord}(b) = q$ y $ab = ba$, entonces G es un grupo cíclico de orden pq.
Ver Ejercicio (4.36.).
Ref.: 3302e_060 SOLUCIÓN

Ejercicio. 9.50.
Sea G un grupo, n y m números enteros primos relativos:

(1) Si $c \in G$, tiene orden nm, demuestra que existen elementos $a, b \in G$, potencias de c, tales que $c = ab$.
(2) Si dos elementos $a, b \in G$ conmutan y tienen por ordenes n y m respectivamente, demuestra que a y b son potencias de un mismo elemento.

Ver Ejercicio (4.36.).
Ref.: 3302e_068 SOLUCIÓN

Ejercicio. 9.51.
Sea G un grupo, demuestra que si $G/Z(G)$ es un grupo cíclico, entonces G es un grupo abeliano.
Ref.: 3302e_061 SOLUCIÓN

Ejercicio. 9.52.
Sea G un grupo cíclico finito. Son equivalentes:
(a) El orden de G es una potencia de un número primo.
(b) Para cada dos subgrupos H y K de G se tiene $H \subseteq K$ ó $K \subseteq H$.

Ver el Ejercicio (4.40.).
Ref.: 3302e_062 SOLUCIÓN

Ejercicio. 9.53.
Demostrar que si G es un grupo finito, entonces todo subgrupo propio de G está contenido en un subgrupo de G maximal
Ref.: 3302e_063 SOLUCIÓN

Ejercicio. 9.54.
Demostrar que si un grupo finito tiene exactamente un subgrupo maximal propio, entonces es cíclico de orden una potencia de un número primo.
Ref.: 3302e_064 SOLUCIÓN

Ejercicio. 9.55.
Demostrar que no existe un grupo G de forma que $\mathrm{Aut}(G)$ *sea no trivial, cíclico y de ordenimpar. (Nota. Utilizar el ejercicio* (9.32.)*).*
Ref.: 3302e_065 SOLUCIÓN

Ejercicio. 9.56.
Determinar grupos G verificando una de las siguientes condiciones:

(1) $\mathrm{Aut}(G)$ *es abeliano.*
(2) $\mathrm{Aut}(G)$ *no es abeliano.*
(3) $\mathrm{Aut}(G)$ *es cíclico y finito.*
(4) $\mathrm{Aut}(G) \cong G$.
(5) $\mathrm{Aut}(G) = \mathrm{Int}(G)$.
(6) $\mathrm{Aut}(G) = 1$.
(7) $\mathrm{Aut}(G)/\mathrm{Int}(G)$ *es isomorfo a* $\mathbb{Z}_2$.

Ref.: 3302e_066 SOLUCIÓN

Ejercicio. 9.57.
Sea $f : G \to G$ un automorfismo de G que fija únicamente al elemento neutro. Definimosg $: G \to G$ mediante $g(x) = f(x)x^{-1}$ para todo $x \in G$. Si G es un grupo finito,probar que g es una biyección. Si G es un grupo finito y $f^2 = 1_G$, probar que G es ungrupo abeliano de orden impar.
Ref.: 3302e_067 SOLUCIÓN

Ejercicio. 9.58.
Consideramos los grupos aditivos $\mathbb{Q}$ y $\mathbb{Z}$, demostrar que $\mathbb{Q}/\mathbb{Z}$ es un grupo infinito que contiene un subgrupo cíclico de orden n para cadaentero positivo n, y que sin embargo no contiene ningún subgrupo cíclico infinito.
Ref.: 3302e_069 SOLUCIÓN

Ejercicio. 9.59.
Sea p un número entero primo positivo, en el grupo cociente $\mathbb{Q}/\mathbb{Z}$ se considera el conjunto

$$\mathbb{Z}(p^\infty) = \left\{ \left[\frac{a}{b} \right] \in \mathbb{Q}/\mathbb{Z} \mid \ a, b \in \mathbb{Z},\ b = p^i,\ i \in \mathbb{N} \right\}.$$

(1) Demostrar que $\mathbb{Z}(p^\infty)$ es un subgrupo de $\mathbb{Q}/\mathbb{Z}$.

(2) *Demostrar que cada elemento de* $\mathbb{Z}(p^\infty)$ *tiene de orden una potencia de* p.
(3) *Si* N *es un subgrupo de* $\mathbb{Z}(p^\infty)$ *de exponente* p^k, $k \in \mathbb{N}$,*entonces* N *es el grupo cíclico de orden* p^k *generado por la clase de* $\frac{1}{p^k}$.
(4) *Si* H *es un subgrupo de* $\mathbb{Z}(p^\infty)$ *de exponente infinito, entonces* $H = \mathbb{Z}(p^\infty)$.
(5) *Determinar el retículo de los subgrupos de* $\mathbb{Z}(p^\infty)$.

Ref.: 3302e_070 SOLUCIÓN

Ejercicio. 9.60.
Sea p *un entero primo positivo, consideramos*

$$P = \left\{ \frac{a}{b} \in \mathbb{Q} \mid \frac{a}{b} \text{ es irreducible y } b \text{ es una potencia de } p \right\}$$

(1) *Demuestra que* P *es un subgrupo de* $(\mathbb{Q}, +)$.

Definimos $\overline{P} = P/\mathbb{Z}$.
(2) *Demuestra que para cada* $n \in \mathbb{N}^*$ *se tiene que* $\overline{P}$ *contiene un subgrupo isomorfo a* $\mathbb{Z}_{p^n}$.

Ref.: 3303e_029 SOLUCIÓN

Ejercicio. 9.61.
Sean $x_1, x_2, \ldots$ *elementos de un grupo abeliano* G *tales que* $\operatorname{ord}(x_1) = p$, $px_2 = x_1, \ldots, px_n = x_{n-1}, \ldots$ *Demostrar que le grupo generado por* $\{x_n : n \in \mathbb{N}^*\}$ *es isomorfo a* $\overline{P}$. *(Nota. Comprobar que la aplicación inducida por* $x_i \mapsto [\frac{1}{p^i}]$ *es un isomorfismo.)*

Ref.: 3303e_030 SOLUCIÓN

Ejercicio. 9.62.
Describir el retículo de subgrupos del grupo cíclico

$$C_8 = \langle x \mid x^8 = 1 \rangle.$$

Ref.: 3302e_023 SOLUCIÓN

Ejercicio. 9.63.
Describe el retículo de subgrupos del grupo cíclico

$$C_{p^n} = \langle x \mid x^{p^n} = 1 \rangle,$$

p primo.
Ref.: 3302e_024 SOLUCIÓN

Ejercicio. 9.64.
Describir el retículo de subgrupos del grupo cíclico

$$C_6 = \langle x \mid x^6 = 1 \rangle.$$

Ref.: 3302e_025 SOLUCIÓN

Ejercicio. 9.65.
Describir el retículo de subgrupos del grupo cíclico

$$C_{12} = \langle x \mid x^{12} = 1 \rangle.$$

Ref.: 3302e_026 SOLUCIÓN

Ejercicio. 9.66.
Describir el retículo de subgrupos del grupo de Klein abstracto $C_2 \times C_2$, donde $C_2 = \langle a \mid a^2 = 1 \rangle$, es un grupo cíclico de orden dos.
Ref.: 3302e_027 SOLUCIÓN

Grupos simétricos II

Ejercicio. 9.67.
Probar que si α es una permutación en S_n, entonces para cada $r \leq n$, tenemos

$$\alpha(i_1 i_2 \dots i_r)\alpha^{-1} = (\alpha(i_1)\alpha(i_2)\dots\alpha(1_r)).$$

Calcular todos los conjugados de $(12)(34)$ *en* S_5.
Ref.: 3302e_071 SOLUCIÓN

Ejercicio. 9.68.
Demostrar que S_n está generado por las transposiciones $(1\ 2), (2\ 3), \dots, (n-1\ n)$.
Ref.: 3302e_072 SOLUCIÓN

Ejercicio. 9.69.
Determinar los subgrupos de orden dos de S_4. Probar que existen nueve, y que de ellos tresestán contenidos en A_4. Probar que todos los subgrupos de orden tres de S_4 estáncontenidos en A_4.
Ref.: 3302e_073 SOLUCIÓN

Ejercicio. 9.70.
Hallar todos los subgrupos de A_4.
Ref.: 3302e_074 SOLUCIÓN

Ejercicio. 9.71.
Demostrar que A_n está generado por los ciclos $(12x)$, *donde x varía en* $\{3, \dots, n\}$.
Ref.: 3302e_075 SOLUCIÓN

Ejercicio. 9.72.
Demostrar que S_n está generado por los ciclos $(123\ldots n-1)$ y $(n-1\ n)$.
Ref.: 3302e_076 SOLUCIÓN

Ejercicio. 9.73.
Determinar los subgrupos de S_4 definidos por:

1. *Las permutaciones que conservan el conjunto $\{1,2\}$.*
2. *Las permutaciones que conservan el conjunto $\{1,2\}$ ó lo transforman en el conjunto $\{3,4\}$.*

Ref.: 3302e_077 SOLUCIÓN

Ejercicio. 9.74.
Demostrar que toda permutación de orden 14 sobre 10 letras es impar.
Ref.: 3302e_078 SOLUCIÓN

Ejercicio. 9.75.
Demostrar que el grupo diédrico D_n es isomorfo a subgrupo de S_n generado por

$$(123\ldots n)\ y\ (2\ n-1)(3\ n-2)\ldots([n/2]\ n-[n/2]+1),$$

donde $[n/2]$ denota parte entera de $n/2$.
Ref.: 3302e_079 SOLUCIÓN

Ejercicio. 9.76.
El n-ésimo GRUPO SIMÉTRICO, *S_n es el grupo formado por todas las permutaciones delconjunto $\{1,2,\ldots,n\}$ con la composición de aplicaciones.*

(1) *Expresar los 6 elementos de S_3 como productos de ciclos disjuntos. Escribir la tabla demultiplicar de S_3 usando esas expresiones para sus elementos.*
(2) *Sea $\sigma = (1,2,3)$ y $\tau = (1,2)$. Mirando la tabla de multiplicar, demostrar que*

$$S_3 = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}.$$

(3) *Reescribir la tabla de multiplicar de S_3 usando la anterior expresión de los elementos deS_3.*
(4) *De (2) se sigue que $S_3 = \langle \sigma, \tau \rangle$. Encontrar otro sistema de generadores deS_3 formado por dos elementos de orden 2.*

Ref.: 3302e_028 SOLUCIÓN

Ejercicio. 9.77.
Describir el retículo de subgrupos de S_3.
Ref.: 3302e_029 SOLUCIÓN

Ejercicio. 9.78.
El n-ésimo GRUPO ALTERNADO, *$n \geq 3$, es el subgrupo de S_n formado por las permutaciones pares. Lo representamos por A_n.*

(1) *Demostrar que A_n es un subgrupo normal de S_n y que $[S_n : A_n] = 2$. Concluir que $|A_n| = n!/2$.*
(2) *Demostrar que si $G \leq S_n$, entonces $G \subseteq A_n$ o $[G : G \cap A_n] = 2$. Concluir que un subgrupo de S_n o bien contiene sólo permutaciones pares o bien la mitad de sus permutaciones son pares y la otra mitad impares.*

Ref.: 3302e_030 SOLUCIÓN

Ejercicio. 9.79.
Describir el retículo de subgrupos de A_4.
Ref.: 3302e_031 SOLUCIÓN

Ejercicio. 9.80.
El n-ésimo GRUPO DIÉDRICO *es el grupo de isometrías del polígono regular de n lados, $n \geq 3$. Lo representamos por D_n. Es un grupo de orden $2n$, que contiene dos elementos significativos que lo generan: El giro de $2\pi/n$ radianes respecto al centro del polígono regular, que es un elemento de orden n y lo representamos por r, y la simetría respecto al eje que une el centro con uno de sus vértices, que es de orden 2 y la representamos por s. En términos de estos generadores, los $2n$ elementos de D_n se expresan de manera única en la forma:*

$$D_n = \{1, r, \cdots, r^{n-1}, s, rs, \cdots, r^{n-1}s\}.$$

Manejando esta representación de sus elementos, la multiplicación del grupo se deduce de las siguientes relaciones "fundamentales",

$$r^n = 1, s^2 = 1, sr = r^{-1}s.$$

(1) A partir de las relaciones fundamentales del grupo diédrico, demuestra que se verifican las siguientes,
$$sr^i = r^{-i}s,\ (r^i s)^2 = 1, \qquad i \in \mathbb{Z}.$$
(2) Demuestra que el subgrupo cíclico de orden n, $\langle r \rangle$ es normal, pero que el de orden 2, $\langle s \rangle$, no lo es.
(3) Escribe la tabla de multiplicar del grupo D_3.
(4) Compara la tabla obtenida en el apartado anterior con la obtenida para el grupo S_3 en el Ejercicio (9.43.), apartado (3). Concluye que existe un isomorfismo $D_3 \cong S_3$.
(5) ¿Es D_4 isomorfo a S_4?

Ref.: 3302e_032 SOLUCIÓN

Ejercicio. 9.81.
Describir el retículo de subgrupos de D_4.
Ref.: 3302e_033 SOLUCIÓN

Ejercicio. 9.82.
Determinar los subgrupos de S_4 definidos por:
(1) las permutaciones que conserven el conjunto $\{1, 2\}$;

(2) las permutaciones que conservan el conjunto $\{1,2\}$ *o lo transforman en el conjunto* $\{3,4\}$.

Ref.: 3303e_055 SOLUCIÓN

Ejercicio. 9.83.
Sea x *un elemento de un grupo finito* G *y* σ_x *la permutación de* G *definida por* $\sigma_x(y) = xy$. *Demostrar que si* G *es de orden impar, entonces* σ_x *es par.*
Ref.: 3303e_056 SOLUCIÓN

Ejercicio. 9.84.
Demostrar que A_4 *no contiene subgrupos de orden 6.*
Ref.: 3303e_057 SOLUCIÓN

Ejercicio. 9.85.
Sea $V = \{1,(12)(34),(13)(24),(14)(23)\}$. *Demostrar que* V *es un subgrupo normal de* S_4 *contenido en* A_4 *y que se tienen los siguientes isomorfismos:* $S_4/V \cong S_3$ *y* $A_4/V \cong C_3$.
Ref.: 3303e_058 SOLUCIÓN

Ejercicio. 9.86.
Demostrar que A_n *es un subgrupo característico de* S_n.
Ref.: 3303e_059 SOLUCIÓN

Ejercicio. 9.87.
Demostrar que toda permutación de S_n que mueve más de dos elementos se puede escribir como un producto de ciclos de longitud tres.
Ref.: 3303e_060 SOLUCIÓN

Ejercicio. 9.88.
Se considera el PUZZLE 15 *y los movimientos usuales. El conjunto de estos movimientos tiene estructura de grupo. Demuestra que este grupo es isomorfo a A_{15}.*
Ref.: 3303e_067 SOLUCIÓN

Otros ejemplos de grupos

Ejercicio. 9.89.
El GRUPO CUATERNIO*, que representamos por Q_2, es el grupo formado por los ocho elementos*

$$\{\pm 1,\ \pm i,\ \pm j,\ \pm k\}$$

con la ley de composición que determinan las igualdades

$$i^2 = j^2 = k^2 = ijk = -1,$$
$$(-1)^2 = 1,\ (-1)i = -i = i(-1),\ (-1)j = -j = j(-1),\ (-1)k = -k = k(-1)$$

(1) Escribir la tabla de grupo para Q_2.
(2) ¿Es Q_2 isomorfo a D_4?

Ref.: 3302e_034 SOLUCIÓN

Ejercicio. 9.90.
Escribir el retículo de subgrupos de Q_2.
Ref.: 3302e_035 SOLUCIÓN

Ejercicio. 9.91.
El n-ésimo GRUPO LINEAL GENERAL *de un cuerpo F, representado por $GL_n(F)$, es el grupo formado por todas las matrices $n \times n$, invertibles y con coeficientes en F, con la multiplicación de matrices como ley de composición.*

(1) Demostrar que $|GL_2(\mathbb{F}_2)| = 6$, escribiendo explícitamente todos los elementos que forman este grupo.
(2) Sea $\alpha = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ y $\beta = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Demostrar que

$$GL_2(\mathbb{F}_2) = \{1,\ \alpha,\ \alpha^2,\ \beta,\ \alpha\beta,\ \alpha^2\beta\}\ .$$

(3) Escribir, utilizando la representación anterior, la tabla de multiplicar de $GL_2(\mathbb{F}_2)$.
(4) Comparando las tablas de multiplicar, concluir que $GL_2(\mathbb{F}_2)$ es isomorfo al grupo diédrico diédrico D_3 (y entonces también al simétrico S_3, ver Ejercicio (9.64.)).

Ref.: 3302e_036 *SOLUCIÓN*

Ejercicio. 9.92.
Si F es un cuerpo finito con q elementos. Determinar el orden de $GL_n(F)$.
Ref.: 3302e_037 *SOLUCIÓN*

Ejercicio. 9.93.
El n-ésimo GRUPO LINEAL UNIMODULAR *ó* GRUPO LINEAL ESPECIAL *de un cuerpo F, que representamos por $SL_n(F)$, es el subgrupo de $GL_n(F)$ formado por las matrices de determinante 1.*

(1) Sea $\det : GL_n(F) \to F^\times$ la aplicación que lleva cada matriz en su determinante. Demostrar que es un epimorfismo de grupos ¿Cual es su núcleo?
(2) Si F un cuerpo finito con q elementos, determinar el orden de $SL_n(F)$.

Ref.: 3302e_038 *SOLUCIÓN*

Ejercicio. 9.94.
El grupo lineal espacial.

(1) *Demostrar que el subgrupo de* $SL_2(\mathbb{F}_3)$

$$Q = \langle a, b \rangle \ ,$$

generado por $a = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ *y* $b = \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ *es isomorfo al grupo cuaternio* Q_2.

(2) *Demostrar que* $SL_2(\mathbb{F}_3)$ *y* S_4 *son dos grupos no isomorfos de orden 24 (Indicación:demostrar que* S_4 *no contiene ningún subgrupo isomorfo a* Q_2*).*

Ref.: 3302e_039 *SOLUCIÓN*

Capítulo III

Presentación de un grupo

10 Presentaciones de un grupo. 87
11 Ejercicios propuestos 110

Introducción.

10. Presentaciones de un grupo.

Grupos de isometrías

Grupos diédricos

Una familia importante de ejemplos es la formada por los grupos cuyos elementos son simetrías de objetos geométricos. La subclase más sencilla es la que corresponde a las figuras planas regulares.

Para cada $n \in \mathbb{Z}$, $n \geq 3$ sea D_n el conjunto de simetrías de un n-gono regular, donde una simetría es cualquier movimiento rígido del plano (o **isometría**) que lleva el n-gono en sí mismo. Es fácil ver que la composición de dos de tales movimientos también dejan fijo al n-gono, que la identidad es uno de estos movimientos y que para cualquiera de los elementos de D_n la transformación inversa también pertenece a D_n, así que D_n es un grupo (más precisamente, un subgrupo del grupo de las isometrías del plano).

Numeramos los vértices del n-gono de manera que los vértices **1** y **2** sean adyacentes. Cualquier isometría del plano queda determinada por la imagen de tres puntos no alineados. En nuestro caso, cualquier elemento de D_n está determinado por la imagen del centro del n-gono (que siempre es él mismo) y por las imágenes de los vértices **1** y **2**. Bajo cualquier elemento de D_n la imagen del vértice

1 es necesariamente uno de los otros n vértices, y la imagen del vértice 2 tiene que ser uno de los dos vértices adyacentes a la imagen del vértice 1. Obtenemos así una cota para el orden de D_n: $|D_n| \leq 2n$.

Por otra parte, las n rotaciones r_k, $0 \leq k < n$ alrededor del centro del n-gono y con ángulos $2k\pi/n$ radianes son todas distintas y llevan el n-gono en sí mismo, así que todas ellas pertenecen a D_n. También pertenecen a D_n las n reflexiones en las rectas que pasan por el centro del n-gono y por cada uno de los vértices y de los puntos medios de las aristas. En total hemos obtenido $2n$ elementos distintos de D_n, así que $|D_n| \geq 2n$. Combinando con la desigualdad anterior vemos que $|D_n| = 2n$.

Ya que a lo largo del curso usaremos mucho los grupos diédricos como fuente de ejemplos, ahora fijaremos alguna notación y haremos algunos cálculos que simplificarán otros cálculos futuros y nos ayudarán a determinar D_n como un grupo abstracto (en lugar de volver al contexto geométrico cada vez que aparezca). Fijamos un n-gono regular centrado en el origen en un XY-plano y numeramos los vértices consecutivamente desde 1 hasta n en sentido contrario a las agujas del reloj. Sea r la rotación con centro en el origen y ángulo $2\pi/n$ radianes (en sentido contrario a las agujas del reloj). Sea s la reflexión en el eje que pasa por el vértice **1** y el origen.

Lema. 10.1.
(1) $1, r, \ldots, r^{n-1}$ *son todas distintas y* $r^n = 1$, *así que* $\mathrm{ord}(r) = n$.
(2) $\mathrm{ord}(s) = 2$.
(3) $s \neq r^i$ *para todo* i.
(4) $sr^i \neq sr^j$ *para todo* $0 \leq i, j \leq n-1$ *con* $i \neq j$, *así que*

$$D_n = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$$

es decir, cada elemento se puede escribir de forma única como $s^k r^j$ *para algún* $k = 0, 1$ *y* $0 \leq j \leq n-1$.
(5) $rs = sr^{-1}$. *En particular* r *y* s *no conmutan, así que* D_n *no es abeliano.*
(6) $r^i s = sr^{-i}$ *para todo* $0 \leq i \leq n$. *Esto indica como conmuta* s *con las potencias de* r.

Observamos ahora que la tabla completa de multiplicación de D_n puede escribirse en términos sólo de r y s, es decir, todos los elementos de D_n tienen una representación única de la forma $s^k r^i$, $k = 0, 1$ y $0 \leq i \leq n-1$, y cualquier producto de dos elementos en esta forma puede reducirse a la misma forma usando sólo las "relaciones" (1), (2) y (6) (reduciendo todos los cálculos módulo n). Por ejemplo, si $n = 12$, se tiene:

$$(sr^9)(sr^6) = s(r^9 s)r^6 = s(sr^{-9})r^6 = s^2 r^{-9+6} = r^{-3} = r^9$$

Generadores y relaciones

El uso de los generadores r y s para el grupo diédrico muestra un modo simple y corto de hacer cálculos en D_n. Análogamente introducimos las nociones de generadores y relaciones para grupos

arbitrarios. Es útil exponer estos conceptos ahora (antes de su justificación formal) ya que proporcionan formas simples de describir y hacer cálculos en muchos grupos. Generadores y relaciones se tratarán rigurosamente cuando hablemos de grupos libres.

Dado un grupo G, llamamos **conjunto de generadores de** G a cualquier subconjunto $S \subseteq G$ con la propiedad de que todo elemento de G puede escribirse como un producto finito de elementos de S y de sus inversos. Notaremos $G = \langle S \rangle$ y decimos que G **está generado por** S y también que S **genera** G. Por ejemplo, el entero 1 es un generador del grupo $\mathbb{Z} = (\mathbb{Z}, +)$ ya que todo entero es una suma de un número finito de copias de 1 y -1, así que $\mathbb{Z} = \langle 1 \rangle$. Otro ejemplo: Por la propiedad (4), $D_n = \langle r, s \rangle$.

Si el grupo G es finito, el conjunto S genera G si todo elemento de G es un producto finito de elementos de S (es decir, no es necesario incluir los inversos de elementos de S).

En un grupo arbitrario G, cualesquiera ecuaciones que satisfacen los generadores se llaman **relaciones de** G. Por ejemplo, en D_n tenemos las relaciones $r^n = 1$, $s^2 = 1$ y $rs = sr^{-1}$. Además estas tres relaciones tienen la propiedad de que *cualquier* otra relación entre los elementos del grupo puede deducirse de ellas (esto no es trivial; se sigue del hecho de que podemos decidir exactamente cuando dos elementos del grupo son iguales utilizando sólo esas tres relaciones).

En general, si algún grupo G está generado por un subconjunto S y existe una familia de relaciones, sean estas $R_1, R_2, \ldots, R_m$ (aquí cada R_i es una ecuación en los elementos de $S \cup \{1\}$), tales que cualquier relación entre los elementos de S puede deducirse de ellas, llamaremos a estos generadores y relaciones una **presentación de** G y denotamos

$$G = \langle S \mid R_1, R_2, \ldots, R_n \rangle.$$

Por ejemplo, una presentación para el grupo diédrico D_n es

$$D_n = \langle r, s \mid r^n = 1,\ s^2 = 1,\ rs = sr^{-1} \rangle.$$

Veremos que utilizar esta presentación para describir D_n (en lugar de volver siempre a la descripción geométrica original) simplifica mucho el trabajo con estos grupos.

Otros presentaciones para grupos conocidos son las siguientes: Todo grupo cíclico finito de orden n tiene la presentación

$$C_n = \langle x \mid x^n = 1 \rangle.$$

y el grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$ tiene la presentación

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V = \langle x, y \mid x^2 = 1,\ y^2 = 1,\ (xy)^2 = 1 \rangle.$$

A este último grupo se le llama **grupo de Klein abstracto**.

Enunciamos ahora un teorema muy útil, para cuya demostración necesitamos de la teoría de grupos libres y por eso la haremos más adelante.

Teorema. 10.2. (Teorema de Dyck)
Sea $G = \langle r_1, \ldots, r_n \rangle$ un grupo finitamente generado y sean $a_1, \ldots, a_n$ elementos de otro grupo H tales que cualquier relación en G satisfecha por los r_i también se satisface en H cuando sustituimos r_i por a_i para todo i. Entonces existe un único homomorfismo $f : G \longrightarrow H$ tal que $f(r_i) = a_i$ para todo i.

Si tenemos una presentación para $G = \langle r_1, \ldots, r_n \mid w_1, \ldots, w_m \rangle$, sólo tenemos que comprobar las relaciones $w_1, \ldots, w_m$ para los a_i, ya que toda otra relación en G se deduce de estas.
Si $H = \langle a_1, \ldots, a_n \rangle$, entonces f es suprayectiva. En este caso, si además $|H| = |G|$ son finitos, entonces f es un isomorfismo.
El resultado inverso también es cierto y más fácil de demostrar:

Teorema. 10.3.
Sea $G = \langle r_1, \ldots, r_n \rangle$ y sea $f : G \longrightarrow H$ un homomorfismo de grupos. Llamamos $a_i = f(r_i)$, $i = 1, \ldots, n$. Entonces cualquier relación en G que satisfagan los r_i también se satisface en H tras la sustitución de r_i por a_i para cada $i = 1, \ldots, n$.

Grupos poliédricos

En el espacio euclídeo de dimensión tres son interesantes los grupos finitos asociados con los poliedros regulares. Vamos a determinar los grupos de rotaciones de cada uno de ellos (es decir, el grupo de todas las rotaciones del espacio que dejan fijo a un poliedro regular). Obsérvese que cada rotación está totalmente determinada por la imagen de dos vertices adyacentes (es decir, unidos por una arista).

El grupo del tetraedro

Llamamos G_4 al grupo del tetraedro. Nuestro objetivo es determinar el orden y una presentación para G_4.
Un tetraedro regular tiene cuatro vértices, seis aristas y cuatro caras. Una rotación suya debe enviar un vértice en otro vértice, así que las posibilidades como imagen de un vértice fijo son cuatro. Una vez conocida la imagen de un vértice, otro adyacente a él sólo tiene tres posibilidades para la imagen, así que en total el número máximo de rotaciones del tetraedro es $4 \times 3 = 12$.
Vamos a describir ahora 12 rotaciones distintas del tetraedro:

- En primer lugar tenemos la identidad, única rotación de orden 1.

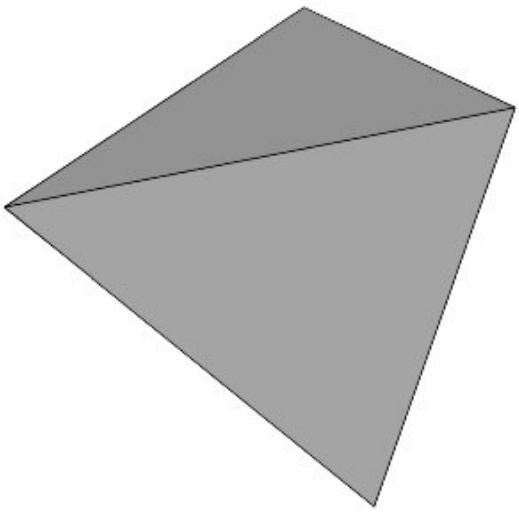


Figura III.1: El tetraedro

- Cada recta que une un vértice con el centro de la cara opuesta es un eje de simetría de orden tres, es decir, que alrededor de cada una de ellas hay dos rotaciones de orden tres del tetraedro. Ya que existen cuatro de tales rectas, tenemos en total $2 \cdot 4 = 8$ rotaciones de orden tres.
- Alrededor de cada recta que une los centros de dos aristas opuestas existe una rotación con ángulo π radianes que lleva el tetraedro en sí mismo. Como existen seis aristas (que forman tres pares de aristas opuestas), obtenemos tres rotaciones de orden dos.

Sumando vemos que hemos obtenido $1 + 8 + 3 = 12$ rotaciones distintas, así que $|G_4| = 12$. Posteriormente veremos que $G_4 \cong A_4$, el grupo alternado sobre cuatro elementos.

Para determinar una presentación numeramos los vértices del tetraedro: Llamamos **1** a uno de ellos y a los otros **2**,**3**,**4** en sentido antihorario vistos desde **1**.

- Sea x la rotación de orden tres que fija **4** y lleva **1** en **2**, y
- sea y la rotación de orden tres que fija **1** y lleva**2** en **3**.

Un poco de cálculo muestra que xy es la rotación de orden 2 que intercambia **1** y **2** y un poco mas de cálculo muestra que todas las rotaciones pertenecen al grupo $\langle x, y\rangle$, así que un candidato para la presentación es

$$G_4 = \langle x, y \mid x^3 = 1,\ y^3 = 1,\ (xy)^2 = 1\rangle \tag{III.1}$$

Más adelante veremos que el grupo dado por la presentación anterior tiene como máximo doce elementos, así que efectivamente, esta es una presentación para el grupo del tetraedro.

El grupo del cubo

Llamamos G_6 al grupo de todas las rotaciones que dejan fijo a un cubo ó hexaedro regular, de ahí el subíndice.

El hexaedro tiene ocho vértices, doce aristas y seis caras. Las posibles imágenes de un vértice determinado son ocho, y una vez fijada esta imagen, las posibilidades de la imagen de un vértice adyacente son sólo tres, así que $|G_6| \leq 8 \cdot 3 = 24$.

Vamos a describir diversas rotaciones:

- En primer lugar tenemos la identidad, única rotación de orden uno.
- Cada recta que une los centros de dos caras opuestas es un eje de rotación cuaternario, al que pertenecen la identidad, dos rotaciones de orden cuatro (las de ángulo $\pi/2$ y $-\pi/2$) y una rotación de orden dos (la de ángulo π). Como existen tres des estas rectas (porque hay tres pares de caras opuestas), en total hemos descrito seis rotaciones de orden cuatro y tres de orden dos.
- Cada recta que une pares de vértices opuestos es un eje de rotación ternario. Además de la identidad, tal eje determina dos rotaciones de orden tres, así que en total tenemos $4 \cdot 2 = 8$ rotaciones de orden tres.
- Cada recta que une los puntos medios de aristas opuestas es un eje de rotación binario, que determina una rotación de ángulo π. Como hay $12/2 = 6$ pares de aristas opuestas, hemos encontrado otras seis rotaciones de orden dos.

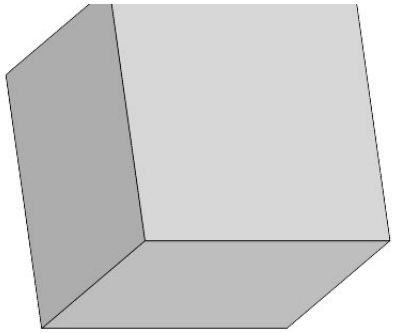


Figura III.2: El hexaedro o cubo

En total tenemos $1+(6+3)+8+6=24$ rotaciones distintas, así que $|G_6|=24$. Luego veremos que $G_6 \cong S_4$, el grupo simétrico sobre cuatro elementos.
Numeramos los vértices de una cara en sentido antihorario como **1**, **2**, **3**, **4**.

- Sea x la rotación de orden 4 que lleva **1** en **2**, y
- sea y la rotación de orden 3 que fija **1** y lleva **2** en **4**.

Es rutina comprobar que xy es la rotación de orden dos que intercambia **1** con **2**. También es rutina (y largo) comprobar que $G_6 = \langle x, y\rangle$. Esto nos lleva a suponer que

$$G_6 = \langle x, y \mid\ x^4 = 1,\ y^3 = 1,\ (xy)^2 = 1\rangle$$

es una presentación de G_6. Un poco de cálculo muestra que el grupo definido por dicha presentación tiene como máximo 24 elementos, con lo que vemos que efectivamente es un presentación de G_6.

El grupo del icosaedro

Llamamos G_{20} al grupo del icosaedro. Un icosaedro tiene en total 12 vértices, 30 aristas y 20 caras. Cada vértice tiene cinco adyacentes, así que tenemos 12 posibilidades como imagen de un vértice arbitrario y cinco como imagen de un vértice adyacente. En total $|G_{20}| \leq 12 \times 5 = 60$. Vamos a describir rotaciones:

- Sólo hay una rotación de orden uno, la identidad.
- Cada recta que una un par de vértices opuestos es un eje de simetría quinario, al que pertenecen cuatro rotaciones de orden 5 (además de la identidad). Existen seis de tales rectas, así que hemos encontrado $6 \cdot 4 = 24$ rotaciones distintas de orden cinco.
- Las rectas que unen los puntos medios de caras opuestas son ejes ternarios de simetría. Cada una de ellas determina dos rotaciones de orden tres, en total $10 \times 2 = 20$ rotaciones distintas de orden tres.

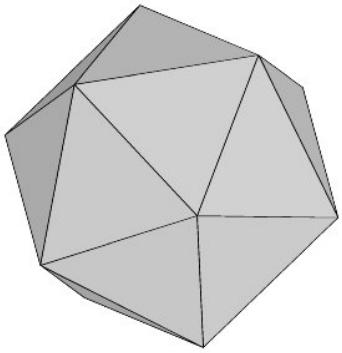


Figura III.3: El icosaedro

- Finalmente, las rectas que unen puntos medios de aristas opuestas son ejes binarios. Cada una determina una rotación de orden dos, en total 15 rotaciones de orden dos.

Sumando todo hemos obtenido $1+24+20+15=60$ rotaciones distintas y por tanto $|G_{20}|=60$. Ya veremos que $G_{20}\cong A_5$, el grupo alternado sobre cinco elementos.
Una presentación para este grupo viene dada por

$$G_{20}=\langle x,y\mid; x^5=1,\ y^3=1,\ (xy)^2=1\rangle$$

como puede comprobarse en dos pasos: Llamamos **1** a uno de los vértices y sucesivamente **2**, **3**, **4**, **5**, **6** a los cinco adyacentes a **1**, en sentido antihorario vistos desde **1**. Sea x la rotación de orden cinco que fija **1** y lleva **2** en **3**, y sea y la rotación de orden tres que lleva **1** en **6** y **6** en **2**. Entonces se comprueba que xy es la rotación de orden dos que intercambia **1** con **2**, así que $(xy)^2=1$. Además se comprueba que $G_{20}=\langle x,y\rangle$.
El último paso consiste en ver que el grupo definido por la presentación anterior tiene como máximo 60 elementos. Más adelante lo veremos.

Importancia de estos grupos

Además de los descritos, existen otros dos poliedros regulares: El octaedro (que tiene seis vértices, doce aristas y ocho caras triangulares) y el dodecaedro (que tiene veinte vértices, treinta aristas y doce caras pentagonales). Los cinco poliedros regulares se conocen también como **sólidos platónicos**. (En el diálogo de Platón titulado *Teeteto* se cuenta que ésta es la lista completa de todos los poliedros convexos regulares posibles. Teeteto es el hombre que descubrió y demostró este resultado.

Su demostración se recoge en el libro XIII de los *Elementos* de Euclides y mas o menos es la que se expone en la enseñanza elemental).

Pero estos poliedros se agrupan como pares de poliedros recíprocos que tienen el mismo grupo: Si unimos los puntos medios de un cubo obtenemos un octaedro regular (que está fijo para el mismo grupo que el cubo) y viceversa, así que el grupo del octaedro es el mismo del cubo. Igualmente, si unimos los puntos medios de las caras de un icosaedro regular obtenemos un dodecaedro regular, que tiene el mismo grupo que el icosaedro (Si unimos los puntos medios de las caras de un tetraedro regular obtenemos otro tetraedro regular). Así que los grupos G_4, G_6 y G_{20} son los únicos que aparecen como grupos de rotaciones de sólidos regulares.

Podemos considerar también los **diedros regulares**. Son poliedros que tienen dos caras (que son polígonos regulares). Son poliedros degenerados porque no encierran ningún espacio y ambas caras coinciden, pero su definición combinatoria tiene sentido. Sus grupos de rotaciones son los grupos diédricos D_n (de aquí les viene el nombre a estos grupos).

El interés de listar estos grupos estriba en que la lista es completa. En [5, sección 3.6], se demuestra:

Proposición. 10.4.
Todo subgrupo finito del grupo de rotaciones del espacio euclídeo de dimensión tres es isomorfo a un grupo cíclico C_n, un grupo diédrico D_n o uno de los grupos poliédricos G_4, G_6, G_{20}.

Una cuestión pertinente ahora sería describir los grupos de simetrías (rotaciones y reflexiones) de un poliedro regular. La respuesta es muy fácil basándonos en el siguiente lema que se puede demostrar cuando estudiemos los grupos de matrices.

Lema. 10.5.
Sea t la reflexión central en un punto O del espacio euclídeo. Entonces t conmuta con toda rotación cuyo eje pase por O.

Sea G cualquier subgrupo finito del grupo euclídeo y sea H el subgrupo de todos los movimientos directos (rotaciones). Si $G \gneqq H$ existe un movimiento inverso en G, y es fácil demostrar que $[G : H] = 2$ y por tanto $G \rhd H$.

Sea G el grupo de todas las simetrías (directas e inversas) del cubo o del icosaedro. La reflexión central t en el centro del poliedro pertenece a G (y está en su centro). Sea $K = \langle t \rangle$. Entonces $G \rhd G_n$ ($n = 6$ ó 20) y $G \rhd K$, $G_n \cap K = 1$ y $G = G_n K$. Luego $G \cong G_n \times K$ es el producto directo interno.

Para el tetraedro, la reflexión en el centro no lo deja fijo, y por tanto el proceso anterior es falso. Más adelante veremos que el grupo de todas las simetrías del tetraedro tiene orden 24 y es isomorfo al grupo simétrico S_4.

Grupos de matrices.

Sea F un cuerpo arbitrario. Llamamos $M_n(F)$ al conjunto de todas las matrices cuadradas $n \times n$ con coeficientes en F. En este conjunto se definen una suma y un producto, respecto a los cuales $M_n(F)$ es un anillo con elemento uno igual a la matriz I.

Nos interesa el grupo multiplicativo de este anillo. Lo representamos por $\mathrm{GL}_n(F)$ y lo llamamos **grupo lineal general** de orden n de F. Sus elementos son las matrices cuadradas que tengan inverso. Es conocido el siguiente resultado:

Lema. 10.6.
Para toda matriz $A \in M_n(F)$ son equivalentes:

(a) Existe $B \in M_n(F)$ tal que $AB = I = BA$.
(b) $\det(A) \neq 0$.
(c) Las filas de A son linealmente independientes sobre F.
(d) Las columnas de A son linealmente independientes sobre F.

Sea $V = F^n$ un espacio vectorial de dimensión n sobre F. Para cada elección de una base $v_1, \ldots, v_n$ existe un isomorfismo $\mathrm{Aut}(V) \cong \mathrm{GL}_n(F)$, por lo que tendemos a identificar estos dos grupos, pero ¡cuidado! el isomorfismo no es canónico, sino que depende de la base.

Los grupos de matrices están íntimamente ligados a la Geometría, Así por ejemplo, los grupos poliédricos que hemos visto pueden representarse por grupos de matrices. Por ejemplo, escojamos como base en $\mathbb{R}^3$ un sistema donde el origen esté en el centro de un cubo regular y los tres ejes sean perpendiculares a las caras del cubo, correspondiendo el vértice **1** al punto $(1,1,1)$ y él vértice **2** al punto $(-1,1,1)$. Es fácil ver que la matriz que corresponde a la rotación x de orden 4 citada en la presentación (III.1) es

$$A = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

y la que corresponde a la rotación y de orden tres citada también en la presentación (III.1) es

$$B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Ahora es muy fácil ver que

$$AB = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

es de orden 2 y que el grupo $\langle A, B \rangle$ tiene orden 24. En general es mas mecánico (y menos intuitivo) hacer cálculos en $\mathrm{GL}_3(\mathbb{R})$ que directamente en los grupos de transformaciones geométricas.

Se ha considerado a los grupos de matrices y a los grupos simétricos como el espejo al que referir los grupos abstractos. Por ello son muy importantes los homomorfismos de un grupo abstracto G a un grupo de matrices $\mathrm{GL}_n(F)$. Tales homomorfismos se llaman **representaciones lineales** del grupo G y son objeto de estudio en un curso de Álgebra más avanzado. Existen teoremas sobre grupos abstractos que actualmente sólo se saben demostrar a través de la teoría de representaciones.

Otra utilidad importante de los grupos de matrices es proveer ejemplos de grupos finitos. Sea $\mathbb{F}$ un cuerpo finito con q elementos. Veamos cual es el orden de $\mathrm{GL}_n(\mathbb{F})$: Sea $A \in \mathrm{GL}_n(\mathbb{F})$ arbitraria. Por el Lema (10.6.), la primera fila puede ser cualquier vector no nulo de $\mathbb{F}^n$, es decir que hay q^n-1 posibilidades. Una vez fijadas las primeras i filas, la $(i+1)$-ésima puede ser cualquier vector de $\mathbb{F}^n$ que no pertenezca al subespacio generado por las i primeras (que es de orden $\mathbb{F}^i$). Así que para esta fila tenemos q^n-q^i posibilidades. En total el número de matrices distintas de $\mathrm{GL}_n(\mathbb{F})$ es $|\mathrm{GL}_n(\mathbb{F})| = (q^n-1)(q^n-q)\dots(q^n-q^{n-1})$.

Por ejemplo, $|\mathrm{GL}_2(\mathbb{Z}_2)| = (2^2-1)(2^2-2) = 6$ y $|\mathrm{GL}_3(\mathbb{Z}_2)| = (2^3-1)(2^3-2)(2^3-2^2) = 168$.

Para cualquier cuerpo F y cualquier $n>0$ la aplicación $\det : \mathrm{GL}_n(F) \longrightarrow F^\times$ que asigna a cada matriz A su determinante $\det(A)$ es un homomorfismo de grupos (ya que el determinante de un producto de matrices es el producto de los determinantes de los factores). Su núcleo es un subgrupo interesante que recibe un nombre especial:

$$\mathrm{SL}_n(F) = \{A \in \mathrm{GL}_n(F) \mid \det(A) = 1\}.$$

Se llama **grupo unimodular** o **grupo lineal especial** del cuerpo F en dimensión n. Como es el núcleo de un homomorfismo, es un subgrupo normal de $\mathrm{GL}_n(F)$. El primer teorema de isomorfismo nos dice que $\mathrm{GL}_n(F)/\mathrm{SL}_n(F) \cong F^\times$. Si $|\mathbb{F}| = q$ es finito tenemos para el orden que

$$|\mathrm{SL}_n(\mathbb{F})| = \frac{1}{q-1}(q^n-1)(q^n-q)\dots(q^n-q^{n-1})$$

Existen otros subgrupos (¡y grupos cocientes!) interesantes de $\mathrm{GL}_n(F)$ como los grupos ortogonal y simpléctico (y los grupos proyectivos general y especial) y cada uno de ellos merece un estudio propio. Se conocen como *los grupos clásicos* y se les han dedicado varios libros. Para una primera aproximación, véase [2]

El grupo cuaternio

El **grupo cuaternio** se puede definir como un grupo de matrices. En el grupo $\mathrm{GL}_n(\mathbb{C})$ consideramos las siguientes matrices:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ i = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix},\ j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ k = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$$

Es fácil comprobar que el conjunto $Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$ es cerrado para el producto, así que forma un subgrupo de orden ocho de $\mathrm{GL}_n(\mathbb{C})$. Se llama **grupo de los cuaternios**. La tabla de multiplicación

puede escribirse a partir de los productos $i \cdot i = -1$, $j \cdot j = -1$, $i \cdot j = k$, $j \cdot i = -k$, los cuales nos dicen que $-1, k \in \langle i, j \rangle$. Como $i^{-1} = -i$ y $j^{-1} = -j$, podemos escribir la presentación:

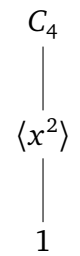
$$Q_2 = \langle i, j \mid \ i^4 = 1,\ j^2 = i^2,\ jij^{-1} = i^{-1} \rangle$$

Nótese que Q_2 *no es abeliano*

Grupos cíclicos.

El grupo $C_4 = \langle x \mid \ x^4 = 1 \rangle$

Sólo tiene un subgrupo propio de orden dos que es $\langle x^2 \rangle$



El grupo $C_8 = \langle x \mid \ x^8 = 1 \rangle$

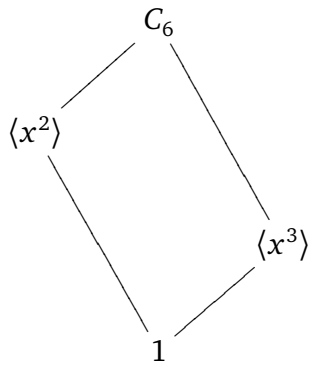
Tiene un único subgrupo cíclico de orden cuatro, a saber $\langle x^2 \rangle$ que contiene al único subgrupo de orden dos que es $\langle x^4 \rangle$.

El grupo $C_{p^n} = \langle x \mid x^{p^n} = 1 \rangle$, p **primo**

Tiene un único subgrupo cíclico $\langle x^{p^{n-k}} \rangle$ de orden p^k para cada k desde 0 hasta n. El retículo es lineal:

El grupo $C_6 = \langle x \mid x^6 = 1 \rangle$

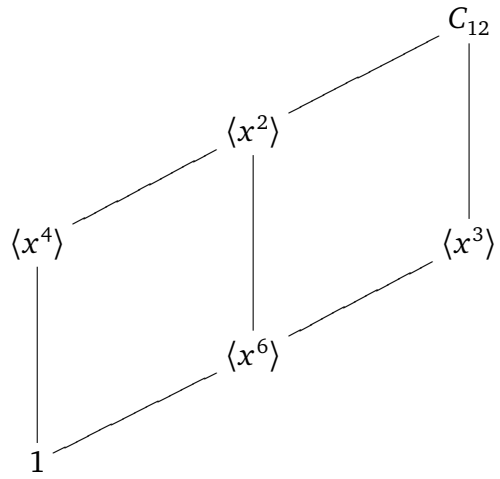
Tiene un subgrupo cíclico de orden tres, $\langle x^2 \rangle$, y otro subgrupo cíclico de orden dos, $\langle x^3 \rangle$.



El grupo $C_{12} = \langle x \mid x^{12} = 1 \rangle$

Tiene un subgrupo propio de cada uno de los órdenes seis, cuatro, tres y dos que son respectivamente $\langle x^2 \rangle$, $\langle x^3 \rangle$, $\langle x^4 \rangle$ y $\langle x^6 \rangle$. El grupo $\langle x^i \rangle$ contiene al $\langle x^j \rangle$ si, y sólo si, i divide a j. Por tanto el retículo

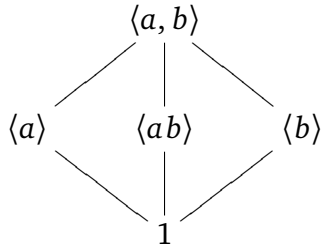
de subgrupos es el siguiente:



Otros grupos abelianos

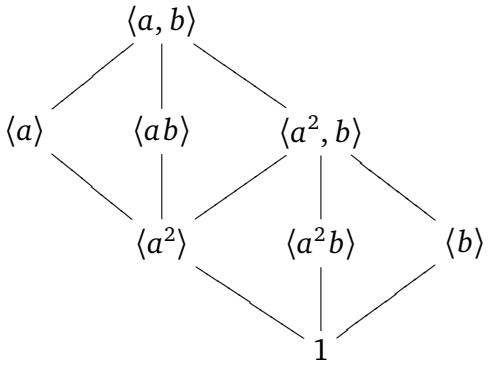
El grupo de Klein $C_2 \times C_2 = \langle a, b \mid\ a^2 = b^2 = 1,\, ab = ba \rangle$

Tiene tres subgrupos de orden dos: $\langle a \rangle$, $\langle b \rangle$ y $\langle ab \rangle$.



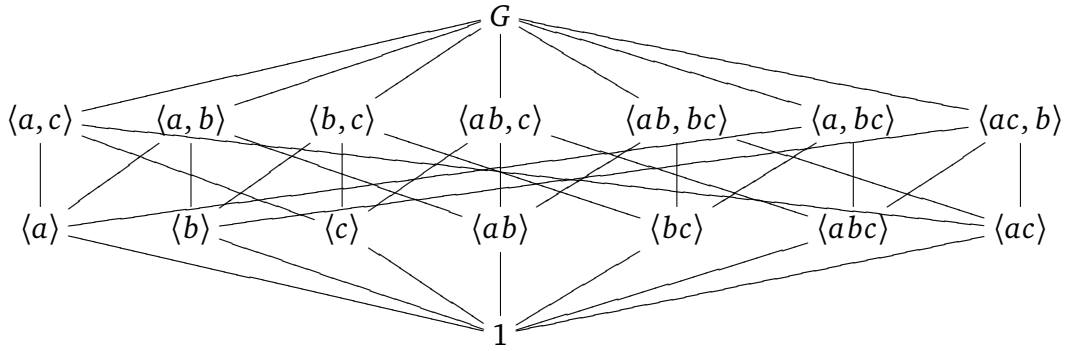
El grupo $C_4 \times C_2 = \langle a, b \mid\ a^4 = b^2 = 1,\, ab = ba \rangle$

Este grupo tiene orden ocho y tres subgrupos de orden cuatro: $\langle a^2, b \rangle \cong V$, $\langle a \rangle \cong C_4$ y $\langle ab \rangle \cong C_4$ y todo subgrupo propio está contenido en uno de estos.



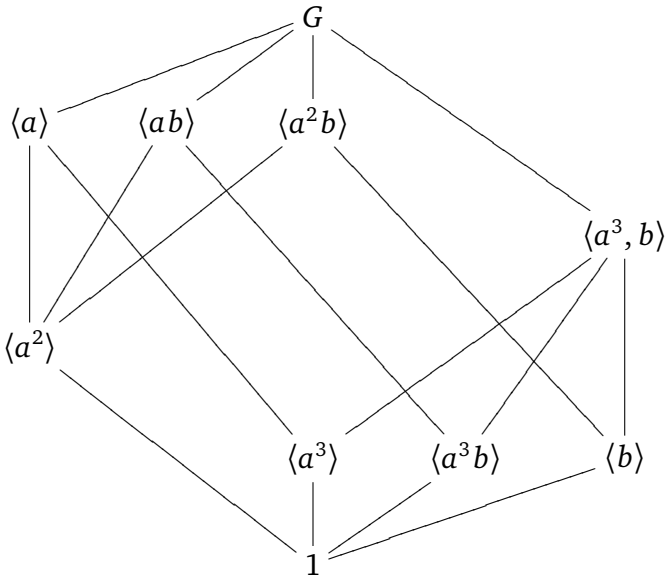
El grupo $C_2 \times C_2 \times C_2 = \langle a, b, c \mid\ a^2 = b^2 = c^2 = 1,\ ab = ba,\ ac = ca,\ bc = cb \rangle$

Es un grupo de orden ocho que contiene siete subgrupos de orden cuatro y siete subgrupos de orden dos. Cada subgrupo de orden cuatro contiene tres subgrupos de orden dos y cada subgrupo de orden dos está contenido en tres subgrupos de orden cuatro.



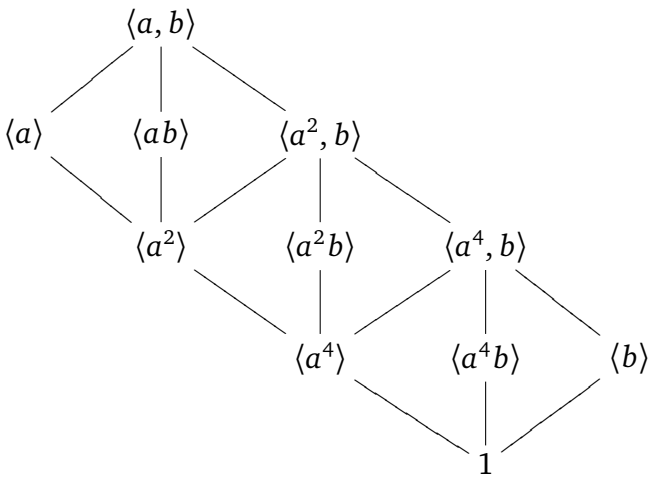
El grupo $C_6 \times C_2 = \langle a, b \mid\ a^6 = b^2 = 1,\ ab = ba \rangle$

El orden es 12. Tiene tres subgrupos de orden seis, todos ellos cíclicos, a saber: $\langle a \rangle$, $\langle ab \rangle$ y $\langle a^2 b \rangle$, y un único subgrupo de orden cuatro: $\langle a^3, b \rangle \cong V$. Todo subgrupo propio está contenido en uno de los citados.



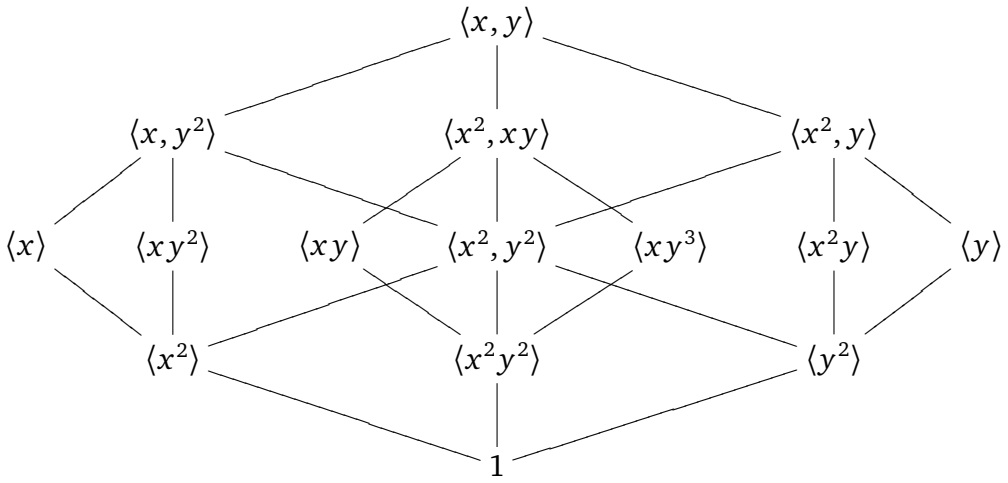
El grupo $C_8 \times C_2 = \langle a, b \mid \ a^8 = b^2 = 1,\, ab = ba \rangle$

Este grupo tiene orden dieciséis y tres subgrupos de orden ocho: $\langle a^2, b\rangle \cong C_4 \times C_2$, $\langle a\rangle \cong C_8$ y $\langle ab\rangle \cong C_8$ y todo subgrupo propio está contenido en uno de estos.



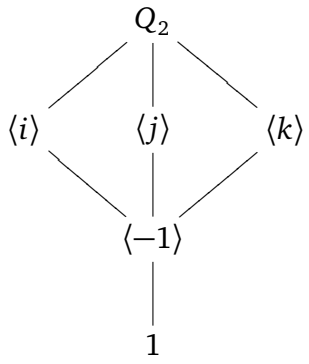
El grupo $C_4 \times C_4 = \langle x, y \mid x^4 = y^4 = 1,\ yx = yx \rangle$

Tiene tres subgrupos de orden ocho: $\langle x, y^2\rangle$, $\langle x^2, xy\rangle$ y $\langle x^2, y\rangle$. Cualquier otro subgrupo está contenido en uno de éstos.



El grupo cuaternio

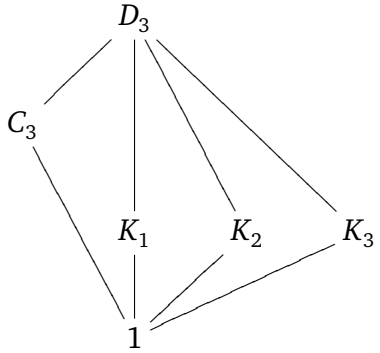
Tiene tres subgrupos de orden cuatro: $\langle i\rangle$, $\langle j\rangle$ y $\langle k\rangle$, todos ellos cíclicos, que tienen en común al único subgrupo de orden dos que es $\langle -1\rangle$.



Grupos diédricos

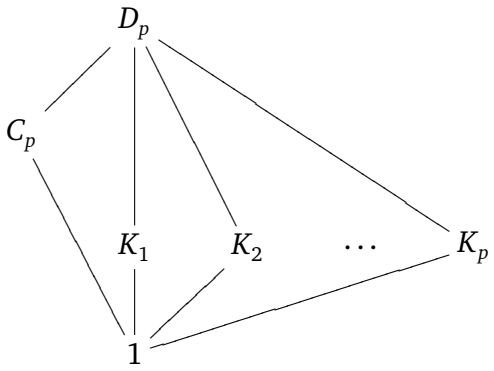
El grupo $D_3 = \langle \rho, \tau \mid \rho^3 = \tau^2 = 1, \rho\tau = \tau\rho^{-1}\rangle$

- Subgrupos de orden tres: $C_3 = \langle \rho\rangle$.
- Subgrupos de orden dos: $K_1 = \langle \tau\rangle$, $K_2 = \langle \tau\rho\rangle$, $K_3 = \langle \tau\rho^2\rangle$.



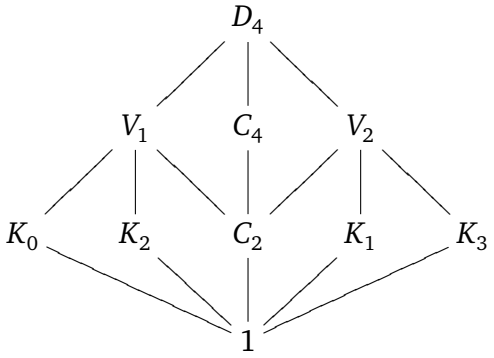
El grupo $D_p = \langle \rho, \tau \mid \rho^p = \tau^2 = 1, \rho\tau = \tau\rho^{-1}\rangle$**,** p **primo**

- Subgrupos de orden p: $C_p = \langle \rho\rangle$
- Subgrupos de orden dos: $K_1 = \langle \tau\rangle$, $K_2 = \langle \tau\rho\rangle$, $\ldots$, $K_p = \langle \tau\rho^{p-1}\rangle$



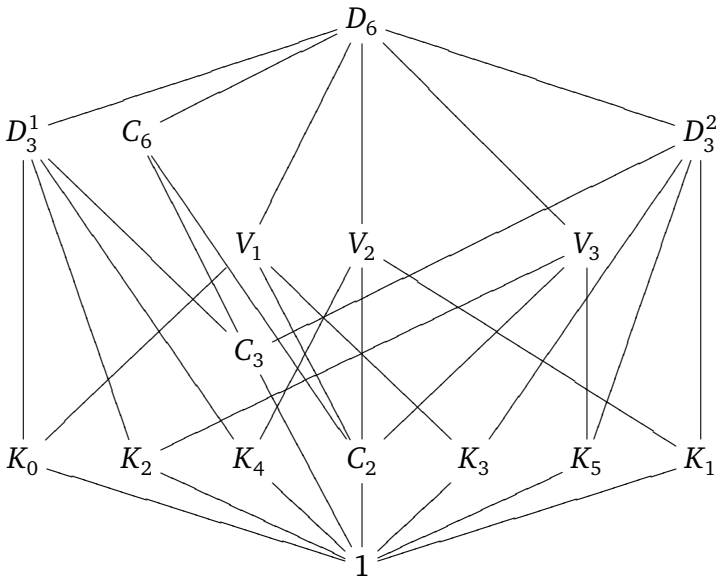
El grupo $D_4 = \langle \rho, \tau \mid \rho^4 = \tau^2 = 1, \rho\tau = \tau\rho^{-1} \rangle$

- Subgrupos de orden cuatro: $C_4 = \langle \rho \rangle$ (cíclico), $V_1 = \langle \rho^2, \tau \rangle$ (Klein), $V_2 = \langle \rho^2, \tau\rho \rangle$ (Klein).
- Subgrupos de orden dos: $C_2 = \langle \rho^2 \rangle$, $K_0 = \langle \tau \rangle$, $K_1 = \langle \tau\rho \rangle$, $K_2 = \langle \tau\rho^2 \rangle$, $K_3 = \langle \tau\rho^3 \rangle$.

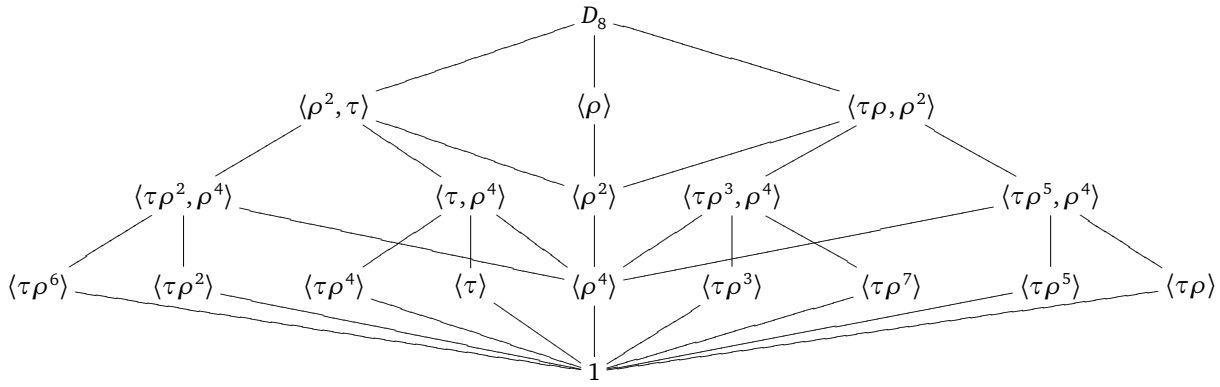


El grupo $D_6 = \langle \rho, \tau \mid \rho^6 = \tau^2 = 1, \rho\tau = \tau\rho^{-1} \rangle$

- Subgrupos de orden seis: $C_6 = \langle \rho \rangle$, $D_3^1 = \langle \rho^2, \tau \rangle$, $D_3^2 = \langle \rho^2, \tau\rho \rangle$.
- Subgrupos de orden cuatro: $V_1 = \langle \rho^3, \tau \rangle$, $V_2 = \langle \rho^3, \tau\rho \rangle$, $V_3 = \langle \rho^3, \tau\rho^2 \rangle$.
- Grupos de orden tres: $C_3 = \langle \rho^2 \rangle$.
- Grupos de orden dos: $K_0 = \langle \tau \rangle$, $K_1 = \langle \tau\rho \rangle$, $K_2 = \langle \tau\rho^2 \rangle$, $K_3 = \langle \tau\rho^3 \rangle$, $K_4 = \langle \tau\rho^4 \rangle$, $K_5 = \langle \tau\rho^5 \rangle$, $C_2 = \langle \rho^3 \rangle$.



El grupo $D_8 = \langle \rho, \tau \mid \rho^8 = \tau^2 = 1, \rho\tau = \tau\rho^{-1} \rangle$



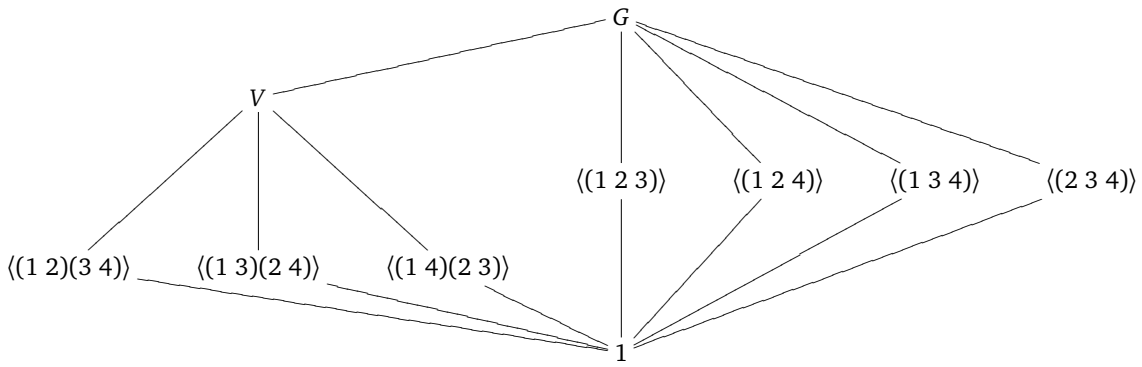
Obsérvese que es un grafo no planar (es decir, no puede dibujarse en un plano sin que se crucen algunas líneas).

Otros grupos de orden 12

En total existen cinco grupos no isomorfos de orden 12. Dos son abelianos: C_{12}, $C_6 \times C_2$ y tres no abelianos. De estos últimos ya hemos visto D_6. Veamos los otros dos:

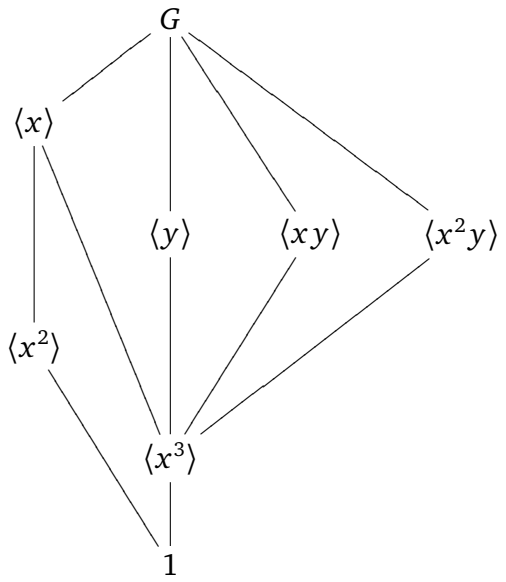
El grupo alternado A_4

Tiene un único subgrupo de orden cuatro que es el grupo de Klein original $V = \langle (1\,2)(3\,4), (1\,3)(2\,4)\rangle$, isomorfo a $C_2 \times C_2$ y cuatro subgrupos de orden tres. El diagrama de subgrupos es:



El grupo $Q_3 = \langle x, y \mid x^6 = 1,\, y^2 = x^3,\, yx = x^{-1}y\rangle$

Este es el segundo de los grupos **dicíclicos** (el primero es el cuaternio, Q_2). Tiene un único subgrupo de orden seis, $\langle x\rangle \cong C_6$, y tres subgrupos de orden cuatro: $\langle y\rangle$, $\langle xy\rangle$, $\langle x^2y\rangle$, todos ellos isomorfos a C_4. Cualquier grupo propio está contenido en una de los citados. El diagrama de subgrupos es:

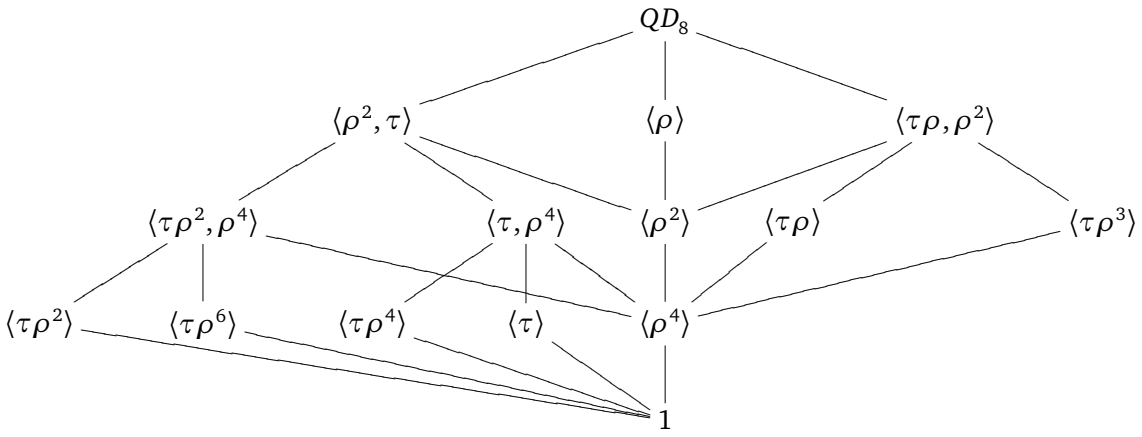


Otros grupos de orden 16

Existen cinco grupos abelianos de orden 16 y nueve no abelianos. En las secciones anteriores hemos visto los retículos de C_{16}, $C_8 \times C_2$ y D_8. Veamos algún otro

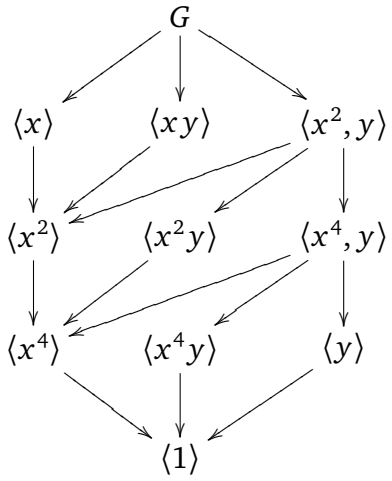
El grupo $QD_8 = \langle \rho, \tau \mid \rho^8 = \tau^2 = 1, \rho\tau = \tau\rho^3 \rangle$

Este grupo se llama **grupo semidiédrico** o **grupo cuasidiédrico** de orden 16. Tiene tres subgrupos de orden ocho: $\langle \rho^2, \tau \rangle \cong D_4$, $\langle \rho \rangle \cong C_8$ y $\langle \rho^2, \rho\tau \rangle \cong Q_2$, y todo subgrupo propio está contenido en uno de estos tres. El grafo tampoco es planar.

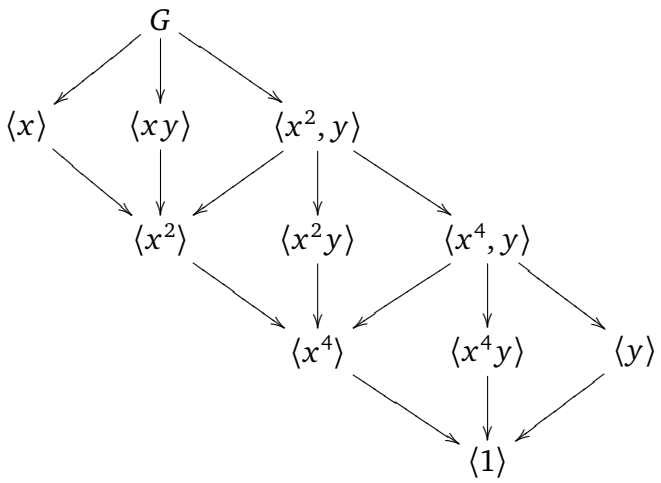


El grupo $G = C_8 \times C_2 = \langle x, y \mid x^8 = y^2 = 1, xy = yx \rangle$

Este grupo tiene tres subgrupos de orden ocho: $\langle x^2, y \rangle \cong C_4 \times C_2$, $\langle x \rangle \cong C_8$ y $\langle xy \rangle \cong C_8$ y todo subgrupo propio está contenido en uno de estos tres.

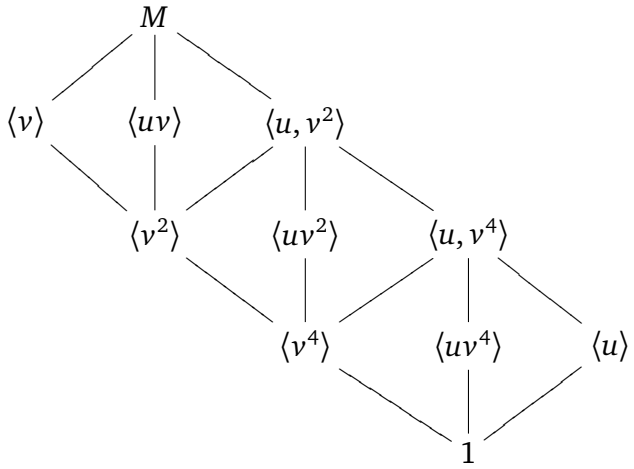


Que también puede dibujarse como



El grupo $M = \langle u, v \mid u^2 = v^8 = 1,\ vu = uv^5 \rangle$

Este grupo se llama **grupo modular** de orden 16. Tiene tres subgrupos de orden ocho: $\langle u, v^2 \rangle \cong C_2 \times C_4$, $\langle v \rangle \cong C_8$ y $\langle uv \rangle \cong C_8$ y todo subgrupo propio está contenido en uno de estos tres.



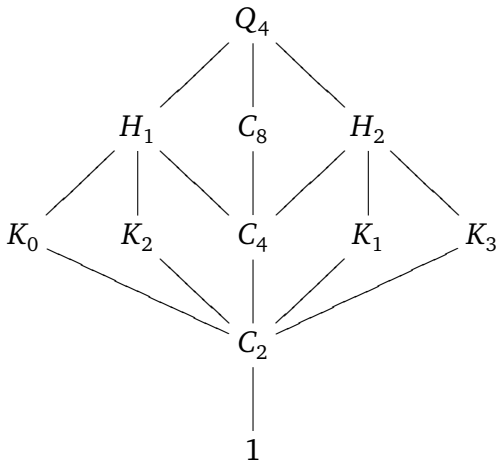
Obsérvese que los grupos M y $C_8 \times C_2$ tienen retículos de subgrupos isomorfos, aunque ellos no son grupos isomorfos.

El grupo $Q_4 = \langle x, y \mid x^8 = 1,\ x^4 = y^2,\ yxy^{-1} = x^{-1} \rangle$

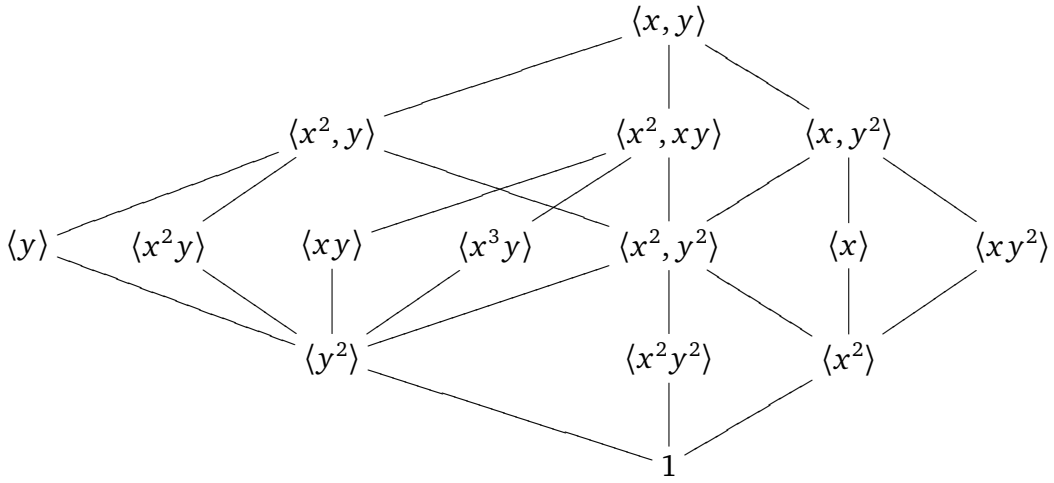
Este es el cuarto **grupo dicíclico**

- Subgrupos de orden ocho: $C_8 = \langle x \rangle$, $H_1 = \langle x^2, y \rangle$, $H_2 = \langle x^2, xy \rangle$.
- Subgrupos de orden cuatro: $C_4 = \langle x^2 \rangle$, $K_0 = \langle y \rangle$, $K_1 = \langle xy \rangle$, $K_2 = \langle x^2 y \rangle$, $K_3 = \langle x^3 y \rangle$.

- Un único subgrupo de orden dos: $C_2 = \langle x^4 \rangle$.



El grupo $C_4 \rtimes_{-1} C_4 = \langle x, y \mid x^4 = y^4 = 1,\ yxy^{-1} = x^{-1} \rangle$



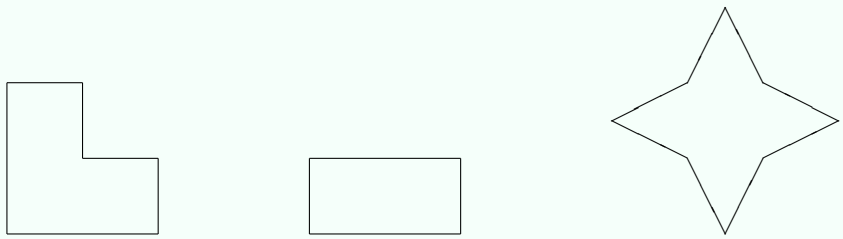
11. Ejercicios propuestos

Movimientos

Ejercicio. 11.1.
Dado un cuadrado (resp. un triángulo ó un polígono regular de n lados, $n \geq 3$), determina el conjunto de los movimientos del plano que lo aplican en sí mismo.Demostrar que junto con la composición el conjunto de estos movimientos forma un grupo.Los grupos resultantes se llaman grupos diédricos ó grupos de isometrías, y se representan por D_4, D_3 y D_n, respectivamente.
Ref.: 3303e_001 SOLUCIÓN

Ejercicio. 11.2.
Calcula la tablas de los grupos de isometrías D_3, D_4, D_5 y D_6.
Ref.: 3303e_002 SOLUCIÓN

Ejercicio. 11.3.
Determina los grupos de isometrías de las siguientes figuras:



Ref.: 3303e_003 SOLUCIÓN

3303-09.tex

Ejercicio. 11.4.
Demuestra que el conjunto de rotaciones respecto al origen del plano afín euclídeo, junto con el conjunto de simetrías respecto a las rectas que pasan por el origen es un grupo. Demuestra que el conjunto de las rotaciones es un subgrupo suyo y que no lo es el conjunto de las simetrías.
Ref.: 3303e_014 *SOLUCIÓN*

Matrices

Ejercicio. 11.5.
Demuestra que el siguiente conjunto de matrices

$$\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}-1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\0&-1\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\right\},$$

junto con la operación producto de matrices, es un grupo abeliano, y prueba que es isomorfo al grupo de Klein.
Ref.: 3303e_004 *SOLUCIÓN*

Ejercicio. 11.6.
Sea G el conjunto de todas las matrices de la forma $\begin{pmatrix}a&b\\0&c\end{pmatrix}$, donde $a,b,c\in\mathbb{R}$ y $ac\neq 0$.

(1) Demuestra que G es un subgrupo de $\mathrm{GL}(2,F)$, y que el conjunto H de todos los elementos de G con $a=c=1$ es un subgrupo de G isomorfo a $\mathbb{R}^+$.
(2) Determina los elementos de orden dos de G.

Ref.: 3303e_021 *SOLUCIÓN*

Números complejos

Ejercicio. 11.7.
Llamamos U_n al conjunto de los números complejos que son raíces n–ésimas de la unidad, esto es, $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$. Demuestra que U_n, junto con la multiplicación, es un grupo.
Ref.: 3303e_005 SOLUCIÓN

Ejercicio. 11.8.
Consideramos el cuerpo $\mathbb{C}$ de los números complejos. Para $a, b, c, d \in \mathbb{C}$, con $ad - bc \neq 0$ consideramos la aplicación

$$f_{a,b,c,d} : \mathbb{C} \cup \{\infty\} \longrightarrow \mathbb{C} \cup \{\infty\}, \text{ definida por } f_{a,b,c,d}(x) = \frac{ax+b}{cx+d}, \quad f_{a,b,c,d}(\infty) = z \text{ y } f_{a,b,c,d}(z) = \infty,$$

en donde $cz + d = 0$. Demuestra que el conjunto $\{f_{a,b,c,d} \mid ad - bc \neq 0\}$, junto con la composición de aplicaciones, es un grupo.
Compara con el Ejercicio (4.14.).
Ref.: 3303e_006 SOLUCIÓN

Ejercicio. 11.9.
Demostrar que la aplicación $f : \mathbb{R}^+ \longrightarrow \mathbb{C}^\times$ definida por $f(x) = e^{ix}$ es un homomorfismo de grupos. Determinar la imagen y el núcleo. Hacer lo mismo para la restricción a $\mathbb{Q}^+$.
Ref.: 3303e_023 SOLUCIÓN

Ejercicio. 11.10.
Se considera $\mathbb{C}_1 = \{z \in \mathbb{C} \mid \|z\| = 1\}$.
(1) Demostrar que $\mathbb{C}_1$, con la multiplicación, es un grupo.
(2) Demostrar que si C_n es un grupo cíclico finito de orden n, entonces existe un monomorfismo $C_n \longrightarrow \mathbb{C}_1$.
(3) Demostrar que $\mathbb{C}_1$ no es un grupo cíclico.
(4) ¿Contiene $\mathbb{C}_1$ algún subgrupo cíclico infinito?
(5) Si $a, b \in \mathbb{C}_1$ son de orden finito, demostrar que $\langle a, b \rangle$ es un grupo cíclico. ¿Cuál es el generador?
(6) Demostrar que existe un monomorfismo $P \longrightarrow \mathbb{C}_1$.
Ref.: 3303e_031 SOLUCIÓN

Números racionales y reales

Ejercicio. 11.11.
Demuestra que el subconjunto

$$X = \left\{ \frac{1+2n}{1+2m} \in \mathbb{Q} \mid \ n, m \in \mathbb{Z} \right\}$$

es un subgrupo del grupo multiplicativo $\mathbb{Q}^{\times}$.
Ref.: 3303e_009 SOLUCIÓN

Subgrupos

Ejercicio. 11.12.
Sea G un grupo finitamente generado y $H \subseteq G$ un subgrupo de índice finito. Demuestra que$H$ es también un grupo finitamente generado.
Ref.: 3303e_007 SOLUCIÓN

Ejercicio. 11.13.
Sea G un grupo abeliano. Demuestra que el conjunto de los elementos de G de orden finito es un subgrupo de G al que llamaremos ***subgrupo de torsión*** *de G.*
Ref.: 3303e_012 SOLUCIÓN

Ejercicio. 11.14.
Siguiendo con la notación del ejercicio **??**, *determinar los elementos $f \in X$ tales que $f^n = 1$.*
Ref.: 3303e_015 SOLUCIÓN

Subgrupos normales y grupos cocientes

Ejercicio. 11.15.
Si A es un grupo abeliano, para cada grupo G se define en $\mathrm{Hom}(G,A)$ *la operación:*

$$(f+g)(x) = f(x)+g(x), \text{ para cada } x \in G.$$

(1) Prueba que $\mathrm{Hom}(G,A)$ *es un grupo abeliano.*
(2) Determinar los siguientes grupos:

$$\mathrm{Hom}(\mathbb{Z},\mathbb{Z}); \quad \mathrm{Hom}(\mathbb{Z},\mathbb{Z}/n\mathbb{Z}); \quad \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}); \quad \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}/m\mathbb{Z}).$$

Ref.: 3303e_022 SOLUCIÓN

Ejercicio. 11.16.
¿En un grupo no abeliano existen subgrupos abelianos no triviales? ¿Y cocientes?
Ref.: 3303e_026 SOLUCIÓN

Producto directo de grupos

Ejercicio. 11.17.
Sean G, H y K grupos. Demostrar que:
(1) $H \times K \cong K \times H$.
(2) $G \times (H \times K) \cong G \times H \times K \cong (G \times H) \times K$.

Ref.: 3303e_086 SOLUCIÓN

Ejercicio. 11.18.
Sean $H \cong J$ y $K \cong L$. Demostrar que $H \times K \cong J \times L$
Ref.: 3303e_087 SOLUCIÓN

Ejercicio. 11.19.
Sea G un grupo y sea $f : G \to G$ un endomorfismo tal que $f^2 = f$ e $\mathrm{Im}(f) \lhd G$.Demuestra que $G = \mathrm{Im}(f) \times \mathrm{Ker}(f)$.
Ref.: 3303e_032 SOLUCIÓN

Ejercicio. 11.20.
Sea G un grupo tal que $G = H \times K$, para H y K subgrupos de G.Si $H' \trianglerighteq H$ y $K' \trianglerighteq K$ son subgrupos normales.
(1) Demuestra que $H' \times K' \trianglerighteq G$ es normal.
(2) Identificando H' con $H' \times \{1\}$ y K' con $\{1\} \times K'$, demuestra que $G/(H'K') \cong H/H' \times K/K'$.

Ref.: 3303e_033 SOLUCIÓN

Ejercicio. 11.21.
Sean H, K dos grupos y sean $H_1 \lhd H$, $K_1 \lhd K$. Demostrar que$H_1 \times K_1 \lhd G$ y que

$$\frac{H \times K}{H_1 \times K_1} \cong \frac{H}{H_1} \times \frac{K}{K_1}$$

Ref.: 3303e_090 SOLUCIÓN

Ejercicio. 11.22.
Sea $\{G_i \mid i \in I\}$ una familia de grupos y $J \subseteq I$ un subconjunto. Definimos una aplicación$f : \prod_J G_j \longrightarrow \prod_I G_i$ mediante

$$f((x_j)_j) = (y_i)_i,$$

con $y_i = x_i$ para todo $i \in J$ e $y_i = e$ si $i \in I \setminus J$.
Demuestra que f es un homomorfismo de grupos y que $\prod_I G_i / \mathrm{Im}(f) \cong \prod_{I \setminus J} G_i$.
Ref.: 3303e_037 SOLUCIÓN

Ejercicio. 11.23.
Sea $\{G_i \mid i \in I\}$ una familia de grupos. Consideramos

$$A = \left\{ (x_i)_i \in \prod_i G_i \mid x_i \neq e \text{ para un número finito de } i \in I \right\}.$$

(1) Demuestra que A es un subgrupo normal de $\prod_i G_i$;
(2) Demuestra que para cada $j \in I$ la aplicación $g_j : G_j \longrightarrow A$, definida $g_j(x) = (x_i)_i$, con

$$x_i = \begin{cases} e & \text{si } i \neq j \\ x & \text{si } i = j \end{cases} \quad \text{es un homomorfismo de grupos.}$$

Ref.: 3303e_038 SOLUCIÓN

Ejercicio. 11.24.
Sea G un grupo abeliano y $f : H \longrightarrow G$, $g : K \longrightarrow G$ dos homomorfismos de grupos.
(1) Demuestra que existe un único homomorfismo de grupos $d : H \times K \longrightarrow G$ que extiende a f y a g.
(2) Da un ejemplo de que este resultado no es cierto cuando G no es abeliano.

Ref.: 3303e_039 SOLUCIÓN

Ejercicio. 11.25.
Sean H y K son grupos y sea $G = H \times K$ el producto directo.
(1) Si $H' \subseteq H$ y $K' \subseteq K$ son subgrupos, demuestra que $H' \times K'$ es un subgrupo de G.
(2) Para cada subgrupo S de G definimos

$$H_S = \{h \in H \mid \text{ existe } k \in K \text{ tal que } (h,k) \in S\}$$
$$K_S = \{k \in K \mid \text{ existe } h \in H \text{ tal que } (h,k) \in S\}$$

Demuestra que H_S y K_S son subgrupos de H y K respectivamente y que $H_S \times K_S$ es el menor subgrupo de la forma $H' \times K'$ contenido en S.
(3) Da un ejemplo que pruebe que no todo subgrupo de G es de la forma $H' \times K'$.

Ref.: 3303e_040 SOLUCIÓN

Ejercicio. 11.26.
Sean H, K, L, M grupos tales que $H \times K \cong L \times M$. ¿Es necesariamente $H \cong L$ y $K \cong M$?
Ref.: 3303e_088 SOLUCIÓN

Automorfismos

Ejercicio. 11.27.
Sea G un grupo tal que $\mathrm{Aut}(G) = \{1\}$. Demostrar que entonces G es abeliano y que cada elemento de G es de orden 2. Si además G es finito, demostrar que G tiene orden uno ó dos.
Ref.: 3303e_036 SOLUCIÓN

Ejercicio. 11.28.
Demostrar que el conjunto de todos los automorfismos de un grupo G (con la composición deaplicaciones) forma un grupo, que se denota por $\mathrm{Aut}(G)$.
Ref.: 3303e_071 SOLUCIÓN

Ejercicio. 11.29.
Sea G un grupo. Demostrar,
(1) Si $\theta : \mathbb{Z}_n \to G$ es un homomorfismo con $\theta(\bar{1}) = x$, entonces$\mathrm{ord}(x) \mid n$ y $\theta(\bar{k}) = x^k$ para todo $0 \le k \le n-1$.
(2) Para cada $x \in G$ tal que $\mathrm{ord}(x) \mid n$ existe un único homomorfismo$\theta_x : \mathbb{Z}_n \to G$ tal que $\theta_x(\bar{1}) = x$.
(3) Si $x \in G$ es tal que $\mathrm{ord}(x) \mid n$, entonces el homomorfismo$\theta_x : \mathbb{Z}_n \to G$ es monomorfismo si y solo si $\mathrm{ord}(x) = n$.
(4) Existe un isomorfismo de grupos

$$U(Z_n) \cong \mathrm{Aut}(\mathbb{Z}_n)$$

definido por $\bar{r} \mapsto f_{\bar{r}}$, $1 \le r \le n$, $\mathrm{mcd}(r,n) = 1$, donde

$$f_{\bar{r}}(\bar{k}) = r\,\bar{k} = \overline{rk},\ \bar{k} \in \mathbb{Z}_n.$$

En particular, $\mathrm{Aut}(\mathbb{Z}_n)$ es un grupo abeliano de orden $\varphi(n)$.

Ref.: 3303e_072 SOLUCIÓN

Ejercicio. 11.30.
Grupos de automorfismos.

(1) Describe explícitamente el grupo $\mathrm{Aut}(\mathbb{Z}_8)$.
(2) Demuestra que $\mathrm{Aut}(\mathbb{Z}_8)$ *es isomorfo al grupo de Klein* $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Ref.: 3303e_073 SOLUCIÓN

Ejercicio. 11.31.
Demostrar que

$$\mathrm{Aut}(\mathbb{Z}) = \{id, -id\} \cong \mathbb{Z}_2 \ ,$$

donde $-id(n) = -n$ *para cada* $n \in \mathbb{Z}$.
Ref.: 3303e_074 SOLUCIÓN

Ejercicio. 11.32.
Sea G *un grupo.*

(1) Demostrar que para cada $a \in G$ *la aplicación* $\varphi_a : G \to G$ *definida por* $\varphi_a(x) = axa^{-1}$ *es un automorfismo de* G*, que se llama automorfismo interno o de conjugación de* G *definido por* a.
(2) Demostrar que la aplicación $G \to \mathrm{Aut}(G)$, $a \mapsto \varphi_a$ *es un homomorfismo.*
(3) Demostrar que el conjunto de automorfismos internos de G*, que se denota* $\mathrm{Int}(G)$*, es un subgrupo normal de* $\mathrm{Aut}(G)$.
(4) Demostrar que $G/Z(G) \cong \mathrm{Int}(G)$.
(5) Demostrar que $\mathrm{Int}(G) = 1$ *si y sólo si* G *es abeliano.*

Ref.: 3303e_075 SOLUCIÓN

Ejercicio. 11.33.
Demostrar que el grupo de automorfismos de un grupo no abeliano no puede ser cíclico.
Ref.: 3303e_076 SOLUCIÓN

Ejercicio. 11.34.
Sea f un automorfismo de un grupo G. Sea $\mathrm{Fix}(f) = \{x \in G \mid f(x) = x\}$.

(1) *Demostrar que* $\mathrm{Fix}(f)$ *es un subgrupo de G, que se llama el* SUBGRUPO DE ELEMENTOS FIJOS *de f.*
(2) *Sea $f = \varphi_a$ el automorfismo interno definido por a. ¿Cual es el subgrupo de elementosfijos de f?*

Ver Ejercicio (9.10.).
Ref.: 3303e_077 *SOLUCIÓN*

Ejercicio. 11.35.
Sea G un grupo finito tal que existe un $f \in \mathrm{Aut}(G)$ *que verifica* $f^2 = id_G$ *y que* $\mathrm{Fix}(f) = 1$.

(1) *Demostrar que la aplicación $x \mapsto x^{-1}f(x)$ establece una biyección de G en sí mismo.*
(2) *Demostrar que f es necesariamente definido por $f(a) = a^{-1}$.*
(3) *Demostrar que G es abeliano.*

Ref.: 3303e_078 *SOLUCIÓN*

Ejercicio. 11.36.
Sean H y K grupos. Consideramos $\mathrm{Aut}(H) \times \mathrm{Aut}(K) \leq \mathrm{Aut}(H \times K)$, *donde cada* $(f, g) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K)$ *es visto como el automorfismo de $H \times K$ tal que* $(f, g)(h, k) = (f(h), g(k))$.

(1) *Demostrar que si H y K son grupos finitos tales que* $\mathrm{mcd}(|H|, |K|) = 1$ *entonces para cada* $\phi \in \mathrm{Aut}(H \times K)$, *se verifica que* $\phi(H \times 1) \subseteq H \times 1$ *y* $\phi(1 \times K) \subseteq 1 \times K$.
(2) *Demostrar que si H y K son grupos finitos tales que* $\mathrm{mcd}(|H|, |K|) = 1$ *entonces*

$$\mathrm{Aut}(H) \times \mathrm{Aut}(K) = \mathrm{Aut}(H \times K).$$

Ref.: 3303e_098 *SOLUCIÓN*

Subgrupo conmutador

Ejercicio. 11.37.
*Dados dos elementos $x, y \in G$ el **conmutador** de x e y es el elemento $[x,y] = xyx^{-1}y^{-1}$.*
*El **subgrupo conmutador** ó **subgrupo derivado** de G, $G' = [G,G]$, es el subgrupo generado por todos los conmutadores de elementos de G,*

$$G' = [G,G] = \langle [x,y] \mid x, y \in G \rangle.$$

(1) Demuestra que $[x,y]^{-1} = [y,x]$.
(2) Demuestra que todo elemento $z \in [G,G]$ es de la forma $z = [x_1,y_1]\cdots[x_n,y_n]$, un producto de conmutadores.
(3) Demuestra que para todo grupo G el conmutador $[G,G]$ es un subgrupo normal de G.
(4) ¿Cuándo es $[G,G] = 1$?

Ref.: 3303e_050 *SOLUCIÓN*

Ejercicio. 11.38.
Abelianizado.

(1) Demostrar que el cociente $G/[G,G]$ es un grupo abeliano.
(2) Sea $f : G \to A$ un homomorfismo de grupos arbitrario con A abeliano. Demostrar que $[G,G] \subset \mathrm{Ker}(f)$. Concluir que existe un único homomorfismo $\bar{f} : G/[G,G] \to A$ tal que $\bar{f}(a[G,G]) = f(a)$, para todo $a \in G$.
(3) Sea $H \leq G$ un subgrupo normal. Demostrar que G/H es abeliano si y solo si $[G,G] \subseteq H$.

Ref.: 3303e_051 *SOLUCIÓN*

Ejercicio. 11.39.
Determinar el subgrupo conmutador de los grupos S_3, A_4, D_4 y Q_2.

Ref.: 3303e_052 *SOLUCIÓN*

Ejercicio. 11.40.
Demostrar que para $n \geq 3$ el derivado de S_n es A_n.
Ref.: 3303e_053 SOLUCIÓN

Ejercicio. 11.41.
Demuestra que, para $n \geq 3$, A_n es el único subgrupo de S_n de orden $n!/2$.
Ref.: 3303e_054 SOLUCIÓN

Ejercicio. 11.42.
Demostrar que para cualesquiera dos grupos G y H se verificaque
(1) $Z(G \times H) = Z(G) \times Z(H)$,
(2) $[G \times H, G \times H] = [G, G] \times [H, H]$.

Ref.: 3303e_091 SOLUCIÓN

Ejercicio. 11.43.
Sea $\{G_1, \ldots, G_t\}$ una familia finita de grupos y consideramos el producto directo $G = G_1 \times \cdots \times G_t$. Demuestra que $[G, G] = [G_1, G_1] \times \cdots \times [G_t, G_t]$.
Ref.: 3303e_035 SOLUCIÓN

Subgrupos especiales

Ejercicio. 11.44.
Dado un grupo G con centro $Z(G)$, prueba que si $G/Z(G)$ es cíclico, entonces G es un grupo abeliano.
Ref.: 3303e_041 SOLUCIÓN

Ejercicio. 11.45.
Determinar el centro del grupo diédrico D_4. Observar que $D_4/Z(D_4)$ es abeliano aunque D_4 no lo es (comparar este hecho con el apartado (3) del Ejercicio (11.44.)).
Ref.: 3303e_042 SOLUCIÓN

Ejercicio. 11.46.
Determinar el centro de los grupos S_n y A_n, $n \geq 2$.
Ref.: 3303e_043 SOLUCIÓN

Ejercicio. 11.47.
Determinar el centro del grupo D_n ,$n \geq 3$.
Ref.: 3303e_044 SOLUCIÓN

Ejercicio. 11.48.
Determinar el centro del grupo Q_2 .
Ref.: 3303e_045 SOLUCIÓN

Ejercicio. 11.49.
Si G es un grupo, para cualquier subconjunto $S \subseteq G$ se llama CENTRALIZADOR *de S en G al conjunto*

$$C_G(S) = \{a \in G \mid \forall x \in S \; ax = xa\}.$$

Y se llama NORMALIZADOR *de S en G al conjunto*

$$N_G(S) = \{a \in G \mid aSa^{-1} = S\}.$$

(1) *Demostrar que el centralizador $C_G(S)$ y el normalizador $N_G(S)$ son subgrupos de G.*
(2) *Demostrar que $C_G(S)$ es un subgrupo normal de $N_G(S)$.*
(3) *Sea H un subgrupo de G. Demostrar que H es un subgrupo normal de $N_G(H)$*
(4) *Sean $H \subseteq K$ subgrupos de G tales que H es un subgrupo normal de K. Demostrar que$K \subseteq N_G(H)$(Los dos últimos puntos caracterizan a $N_G(H)$ como el mayor subgrupo de G en el que H esnormal).*

Ref.: 3303e_046 SOLUCIÓN

Ejercicio. 11.50.
Demuestra que $C_G(Z(G)) = G$, y deduce que $N_G(Z(G)) = G$.
Ref.: 3303e_047 SOLUCIÓN

Ejercicio. 11.51.
Sea G un grupo y sea H un subgrupo suyo. ¿Cuando es $G = N_G(H)$? ¿Y cuando es $G = C_G(H)$?
Ref.: 3303e_048 SOLUCIÓN

Ejercicio. 11.52.
Sea H un subgrupo de orden 2 de un grupo G. Demostrar que $N_G(H) = C_G(H)$. Deducir que H esnormal en G si y sólo si está contenido en $Z(G)$.
Ref.: 3303e_049 SOLUCIÓN

Ejercicio. 11.53.
Sean H y K dos subgrupos finitos de un grupo G, uno de ellos normal. Demostrar que

$$|H|\,|K| = |HK|\,|H \cap K|\,.$$

Ref.: 3303e_061 SOLUCIÓN

Ejercicio. 11.54.
Sean H, K subgrupos de G y sea N un subgrupo normal de G tal que $HN = KN$. Demostrar que

$$\frac{H}{H \cap N} \cong \frac{K}{K \cap N}$$

Ref.: 3303e_062 SOLUCIÓN

Ejercicio. 11.55.
Sea N un subgrupo normal de G tal que N y G/N son abelianos. Sea H un subgrupocualquiera de G. Demostrar que existe un subgrupo normal K de H tal que K y H/K sonabelianos.
Ref.: 3303e_063 SOLUCIÓN

Ejercicio. 11.56.
Sea G un grupo finito y sean H, K subgrupos de G con K normal y tales que $|H|$ y $[G : K]$son primos relativos. Demostrar que H está contenido en K.
Ref.: 3303e_064 SOLUCIÓN

Ejercicio. 11.57.
Un subgrupo H de un grupo finito G se llama SUBGRUPO DE HALL *si $|H|$ y $[G : H]$ sonprimos relativos.Sea G un grupo finito, H un subgrupo de Hall de G. Demostrar que para cualquier subgrupo-normal K de G se verifica que $H \cap K$ es un subgrupo de Hall de K y HK/K es un subgrupode Hall de G/K.*
Ref.: 3303e_065 SOLUCIÓN

Ejercicio. 11.58.
Sea H un subgrupo de Hall normal del grupo finito G. Demostrar que H es el único subgrupo de G de orden $|H|$.
Ref.: 3303e_066 SOLUCIÓN

Descomposición de grupos

Ejercicio. 11.59.
Sean $h \in H$ y $k \in K$ dos elementos de dos grupos H y K, cuyos ordenes respectivos son $\text{ord}(h) = n$ y $\text{ord}(k) = m$ *¿Cual es el orden de $(h,k) \in H \times K$?*
Ref.: 3303e_081 SOLUCIÓN

Ejercicio. 11.60.
Sean H y K grupos cíclicos finitos. Demostrar que $H \times K$ es cíclico si, y sólo si, $(|H|,|K|) = 1$.
Ref.: 3303e_082 SOLUCIÓN

Ejercicio. 11.61.
Demostrar que los grupos $\mathbb{Z} \times \mathbb{Z}_2$ y $\mathbb{Z} \times \mathbb{Z}$ no son cíclicos.
Ref.: 3303e_083 SOLUCIÓN

Ejercicio. 11.62.
Demostrar que los siguientes grupos no son un producto directo interno de subgrupos propios:

$$S_3, \qquad \mathbb{Z}_{p^n} \text{ (con } p \text{ primo)}, \qquad \mathbb{Z}.$$

Ref.: 3303e_084 SOLUCIÓN

Ejercicio. 11.63.
En cada uno de los siguientes casos, decidir si el grupo G es o no producto directo interno delos subgrupos H y K.

(1) $G=\mathbb{R}^\times, H=\{\pm 1\}, K=\{x\in\mathbb{R} \mid x>0\}$.

(2) $G=\left\{\left(\begin{smallmatrix} a & b \\ 0 & c\end{smallmatrix}\right)\in GL_2(\mathbb{R})\right\}, H=\left\{\left(\begin{smallmatrix} a & 0 \\ 0 & c\end{smallmatrix}\right)\in GL_2(\mathbb{R})\right\}, K=\left\{\left(\begin{smallmatrix} 1 & b \\ 0 & 1\end{smallmatrix}\right)\in GL_2(\mathbb{R})\right\}$.

(3) $G=\mathbb{C}^\times, H=\{z\in\mathbb{C} \mid |z|=1\}, K=\{x\in\mathbb{R} \mid x>0\}$.

Ref.: 3303e_085 SOLUCIÓN

Ejercicio. 11.64.
Demostrar que no todo subgrupo de un producto directo $H\times K$ es de la forma $H_1\times K_1$ con H_1 subgrupo de H y K_1 subgrupo de K.
Ref.: 3303e_089 SOLUCIÓN

Ejercicio. 11.65.
Sean $H, K \lhd G$ tales que $H\cap K=1$. Demostrar que G es isomorfo a un subgrupo de$G/H\times G/K$.
Ref.: 3303e_092 SOLUCIÓN

Ejercicio. 11.66.
Sean H y K subgrupos normales de G tales que $HK=G$. Demostrar que

$$G/(H\cap K)\cong H/(H\cap K)\times K/(H\cap K)\cong (G/H)\times(G/K).$$

Ref.: 3303e_093 SOLUCIÓN

Ejercicio. 11.67.
Un grupo G es producto directo interno de subgrupos H y K, y $N \lhd G$ tal que $N \cap H = 1 = N \cap K$. Demostrar que N es abeliano.
Ref.: 3303e_094 SOLUCIÓN

Ejercicio. 11.68.
Dar un ejemplo de un grupo G que es producto directo interno de dos subgrupos propios H y K y que contiene un subgrupo normal no trivial N tal que $N \cap H = N \cap K = 1$. Concluir que para $N \lhd H \times K$ es posible que $N \neq (N \cap (H \times 1)) \times (N \cap (K \times 1))$.
Ref.: 3303e_095 SOLUCIÓN

Ejercicio. 11.69.
Producto directo interno.

(1) Sea G un grupo finito que es producto directo interno de dos subgrupos suyos H y K con $\mathrm{mcd}(|H|, |K|) = 1$. Demostrar que para todo subgrupo $N \leq G$ se verifica que N es producto directo interno de $N \cap H$ y $N \cap K$.
(2) Demostrar que si H y K son grupos finitos tales que $\mathrm{mcd}(|H|, |K|) = 1$, todo subgrupo del grupo $H \times K$ es de la forma $H_1 \times K_1$, con $H_1 \leq H$ y $K_1 \leq K$.

Ref.: 3303e_096 SOLUCIÓN

Capítulo IV

Grupos libres

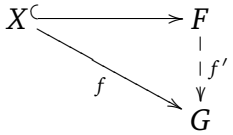
12 Grupos libres 129
13 Ejercicios propuestos 140

Introducción.

12. Grupos libres

Definición de grupo libre

Un grupo F se llama **libre** sobre un subconjunto $X \subseteq F$ si para cada grupo G y cada aplicación $f : X \longrightarrow G$ existe un único homomorfismo de grupos $f' : F \longrightarrow G$ tal que $f'_{|X} = f$.



Un hecho importante es el siguiente:

Proposición. 12.1.
Si F es un grupo libre sobre el subconjunto X, entonces X es un sistema de generadores de F.

3304-02.tex

DEMOSTRACIÓN. Llamamos G al subgrupo de F generado por X, entonces existe una aplicación, la inclusión, $f : X \longrightarrow G$; por ser F libre sobre X, existe un único homomorfismo de grupos $f' : F \longrightarrow G$ tal que $f' \mid X = f$. Ahora componiendo con la inclusión $j : G \hookrightarrow F$ tenemos $j(f' \mid X) = 1_X$, luego $jf' = 1_F$, j es entonces una aplicación sobreyectiva y $G = F$. □

$$\begin{array}{ccccc} X & = & X & = & X \\ \downarrow & & \downarrow & & \downarrow \\ F & \xrightarrow{f'} & G & \xrightarrow{j} & F \end{array}$$

Se dice entonces que X es un **sistema de generadores libre** del grupo F.
Como consecuencia de la definición existe una cierta unicidad de los grupos libres.

Lema. 12.2.
Si F_1 y F_2 son grupos libres sobre subconjuntos X_1, X_2 de F_1 y F_2 respectivamente, para cada aplicación $f : X_1 \longrightarrow X_2$ existe un único homomorfismo de grupos $f' : F_1 \longrightarrow F_2$ tal que $f'_{|X_1} = f$.
Además, si f' es una biyección, entonces f es un isomorfismo de grupos.

DEMOSTRACIÓN. La aplicación f podemos extenderla hasta F_2, la llamamos f_0, entonces existe un único homomorfismo de grupos $f' : F_1 \longrightarrow F_2$ tal que $f'_{|X_1} = f_0$, y si restringimos el codominio a X_2, tenemos $f'_{|X_1} = f$. Por la construcción f' es el único homomorfismo de grupos que verifica las condiciones del enunciado.
Si además f es un biyección, entonces existe $g : X_2 \longrightarrow X_1$ tal que $fg = \mathrm{id}_{X_2}$ y $gf = \mathrm{id}_{X_1}$, luego existe un único homomorfismo de grupos $g' : F_2 \longrightarrow F_1$ tal que $g'_{|X_2} = g$. Se verifica que $f'g'_{|X_2} = fg = \mathrm{id}_{X_1}$, y por la primera parte $f'g'$ es el único homomorfismo de grupos que verifica esto, luego $f'g' = \mathrm{id}_{F_2}$. De forma análoga $g'f' = \mathrm{id}_{F_1}$, y por tanto f' es un isomorfismo de grupo.

$$\begin{array}{ccccccc} X_1 & \xrightarrow{f} & X_2 & \xrightarrow{g} & X_1 & \xrightarrow{f} & X_2 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ F_1 & \xrightarrow{f'} & F_2 & \xrightarrow{g'} & F_1 & \xrightarrow{f'} & F_2 \end{array}$$

□

Vamos a extender la definición de grupo libre para buscar nuevas aplicaciones.
Si X es un conjunto, F un grupo e $i : X \longrightarrow F$ una aplicación, decimos que F es un **grupo libre sobre el conjunto X respecto a la aplicación i**, si para cada grupo G y cada aplicación $f : X \longrightarrow G$, existe un único homomorfismo de grupos $f' : F \longrightarrow G$ tal que $f = f'i$.

$$\begin{array}{ccc} X & \xrightarrow{i} & F \\ & \searrow^{f} & \downarrow{\scriptstyle f'} \\ & & G \end{array}$$

Si no hacemos referencia a la aplicación i, decimos simplemente que F es un **grupo libre sobre el conjunto** X.
De la definición se deduce que i es siempre una aplicación inyectiva.

Lema. 12.3.
En la definición de grupo libre la aplicación i es inyectiva.

DEMOSTRACIÓN. Si i no es inyectiva, existen $y, z \in X$ tales que $i(y) = i(z)$. Definimos $f : X \longrightarrow \mathbb{Z}_2$ mediante $f(y) = 1$, $f(x) = 0$, para todo $x \in X$, $x \neq y$, entonces existe un homomorfismo de grupos $f' : F \longrightarrow \mathbb{Z}_2$ que verifica $f'i = f$, luego $1 = f(y) = f'i(y) = f'i(x) = f(z) = 0$, lo que es una contradicción. □

Como consecuencia inmediata del lema, si un grupo F es libre sobre un conjunto X respecto a una aplicación i, entonces es libre sobre el subconjunto $i(X)$.
Una consecuencia del Lema 12.2. es:

Teorema. 12.4.
Dos grupos libres sobre conjuntos con el mismo cardinal son isomorfos.

El recíproco a este resultado también es cierto, pero para demostrarlo esperaremos a dar una construcción de los grupos libres.

Construcción del grupo libre

Para construir un grupo libre sobre un conjunto dado X vamos a seguir los siguientes pasos:

(1) Definimos un nuevo conjunto X' que tiene como elementos los de X unión disjunta con $\{x^{-1} \mid x \in X\}$.

(2) Llamamos $M(X)$ al conjunto de todas las *palabras* de X', esto es; el conjunto de todas las sucesiones finitas de elementos de X', unión con la palabra vacía

$$M(X) = \{x_1 x_2 \dots x_n \mid \ x_i \in X', 1 \leq i \leq n, n \in \mathbb{N}\}.$$

(3) En $M(X)$ definimos una operación interna $*$, que consiste en yuxtaponer palabras

$$(x_1 x_2 \dots x_n) * (y_1 y_2 \dots y_m) = x_1 x_2 \dots x_n y_1 y_2 \dots y_m.$$

Esta operación es asociativa y tiene un elemento neutro, la palabra vacía. Tenemos pues que $(M(X), *)$ es un monoide no necesariamente conmutativo.

(4) Para obtener un grupo, que es lo que deseamos, definimos en $M(X)$ una relación de equivalencia R mediante:

"*Dos palabras de $M(X)$ están relacionadas por R si son iguales ó una se obtiene de la otra eliminando ó incluyendo expresiones del tipo xx^{-1} ó $x^{-1}x$, con $x \in X$*".

(5) La operación $*$ es compatible con la relación R, esto es; si $p_1, p_2, q_1, q_2 \in M(X)$, $p_1 R q_1$ y $p_2 R q_2$, entonces $(p_1 * p_2) R (q_1 * q_2)$. Luego $*$ define en $F(X) = M(X)/R$ una operación interna mediante

$$[p] * [q] = [p * q],$$

para cada $p, q \in M(X)$. Además esta operación es asociativa y tiene por elemento neutro a $[\varnothing]$, la clase de la palabra vacía.

(6) Para ver que cada elemento tiene un inverso, sea $[p] \in F(X)$, supongamos que

$$p = x_1^{e_1} \dots x_n^{e_n},$$

con $e_i \in \{1, -1\} \subseteq \mathbb{Z}$, para cada $x_i \in X$; definimos

$$q = x_n^{d_n} \dots x_1^{d_1},$$

con $d_i = (-1)e_i \in \{1, -1\} \subseteq \mathbb{Z}$. Se verifica $[p] * [q] = [q * p] = [\varnothing]$.

(7) Definimos ahora una aplicación $i : X \longrightarrow F(X)$ mediante $i(x) = [x]$.

Teorema. 12.5.
En la situación anterior $F(X)$ es un grupo libre sobre el conjunto X respecto a la aplicación i.

DEMOSTRACIÓN. Sea G un grupo y $f : X \longrightarrow G$ una aplicación, definimos $f' : F(X) \longrightarrow G$ mediante $f'([x_1^{e_1} \dots x_n^{e_n}]) = f(x_1)^{e_1} \dots f(x_n)^{e_n}$, tenemos que f' está bién definido y es un homomorfismo de grupos, además $f'i = f$, y f' es el único homomorfismo de grupos que verifica esta igualdad. □

Los elementos de $F(X)$ podemos representarlos en vez de $[x_1^{e_1} \dots x_n^{e_n}]$, simplemente como $x_1^{e_1} \dots x_n^{e_n}$, teniendo en cuenta que ahora dos palabras de X' son iguales si están relacionadas.

Vamos a buscar en cada clase de $F(X)$ un elemento distinguido. Una palabra $x_1^{e_1} \dots x_n^{e_n}$ se llama **reducida** si no existen en ella expresiones del tipo xx^{-1} ó $x^{-1}x$, con $x \in X$. Es claro que cada elemento de $F(X)$ tiene como representante a una palabra reducida, basta eliminar las ocurrencias no deseadas, pero además en cada clase existe una *única* palabra reducida, como nos indica el siguiente teorema.

Teorema. 12.6.
En la situación anterior cada clase del grupo $F(X)$ tiene como representante a una única palabra reducida.

DEMOSTRACIÓN. Dado un elemento de $F(X)$, es claro que éste tiene como representante a una palabra reducida, basta con eliminar una tras otra todas las ocurrencias de las expresiones xx^{-1} ó $x^{-1}x$, con $x \in X$. Para ver que esta palabra reducida es única, supongamos que una clase tiene dos palabras reducidas p y q, siendo

$$p = x_1^{e_1} \dots x_n^{e_n}$$

y

$$q = y_1^{d_1} \dots y_m^{d_m},$$

$e_i, d_j \in \{1, -1\}$, $1 \leq i \leq n$, $1 \leq j \leq m$. Llamamos q^{-1} a la palabra

$$q^{-1} = y_m^{c_m} \dots y_1^{c_1},$$

con $c_j = (-1)d_j$, $1 \leq j \leq m$. Tenemos $[p] = [q]$, luego $[.] = [p] * [q]^{-1} = [p * q^{-1}]$. Se verifica que p y q son palabras distintas si, y sólo si, $p * q^{-1}$; después de suprimir las apariciones de xx^{-1} y $x^{-1}x$, para $x \in X$; no es la palabra vacía. Luego probar que una clase contiene una única palabra reducida es equivalente a demostrar que en $[.]$ la única palabra reducida es la palabra vacía.

Supongamos que $x_1^{e_1} \dots x_n^{e_n}$, $e_i = \pm 1$ es una palabra reducida no vacía equivalente a la palabra vacía, entonces para cada grupo G y cada aplicación $f : X \longrightarrow G$, el elemento $f(x_1)^{e_1} \dots f(x_n)^{e_n}$ es igual a 1. Consideramos el grupo $G = S_{n+1}$ y la aplicación $f : X \longrightarrow S_{n+1}$ definida por $f(x) = 1$ si $x \neq x_i$.

Para cada x_i consideramos todos los $k_1, \dots, k_s$ que verifican $1 \leq k_1 < \dots < k_s \leq n$ y $x_i = x_{k_j}$, $1 \leq j \leq s$. Definimos entonces $f(x_i)$ de forma que

$$\begin{cases} f(x_i)(k_j + 1) = k_j & \text{si } e_{k_j} = 1 \\ f(x_i)(k_j) = k_j + 1 & \text{si } e_{k_j} = -1 \end{cases}$$

Los demás elementos permanecen fijos. Una forma de hacer esto es la siguiente:

1. Si $x_{k_j} - 1 \neq x_{k_j} \neq x_{k_j} + 1$, entonces aparece en $f(x_i)$ el factor $(k_j\, k_j + 1)$.

2. Si $x_{k_j - 1} \neq x_{k_j} = x_{k_j+1} = \dots = x_{k_j+r} \neq x_{k_j} + r + 1$, entonces si $e_{k_j} = 1$, en $f(x_{k_j}) \cdots f(x_{k_j+r})$ aparece el factor $(k_j\, k_j + 1) \cdots (k_j + r\, k_j + r + 1)$; y si $e_{k_j} = -1$, aparece el factor $(k_j + r\, k_j + r + 1) \cdots (k_j\, k_j + 1)$.

Así definido tenemos

$$f(x_i)^{e_{k_j}}(k_j + 1) = k_j,$$

luego

$$f(x_1)^{e_1} \cdots f(x_n)^{e_n}(n + 1) = f(x_1)^{e_1} \cdots f(x_{n-1})^{e_{n-1}}(n) = \dots = f(x_1)^{e_1}(2) = 1,$$

por lo tanto no coincide con la identidad, lo que es una contradicción. □

Teorema. 12.7.
Sean F_1 y F_2 grupos libres sobre los conjuntos X_1 y X_2 respectivamente. Si F_1 y F_2 son isomorfos, entonces X_1 y X_2 tienen el mismo cardinal.

DEMOSTRACIÓN. Basta ver que un grupo libre F determina el cardinal del conjunto X sobre el que es libre. Consideramos el subgrupo

$$N = \langle \{ y^2 \in F ; y \in F \} \rangle .$$

Ya que N es un subgrupo característico, es también un subgrupo normal, y además F/N es un grupo abeliano en el que cada elemento tiene orden 2.
Si X es finito, por ejemplo $X = \{x_1, \ldots, x_n\}$, tenemos que

$$F/N = \{ x_{i_1} \ldots x_{i_r} N \mid \ x_{i_j} \in X, i_j \neq i_k \text{ si } j \neq k \},$$

luego $| F/N | = 1 + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n-1} + \binom{n}{n} = 2^n = 2^{|X|}$.
Si X es infinito, entonces $| F/N | = | P_F(X) | = | X |$. Luego en ambos casos el cardinal de X está determinado por F. □

Si F es un grupo libre sobre un conjunto X respecto a la aplicación $i : X \longrightarrow F$, entonces $i(X)$ se llama una **base** de F. El Teorema nos dice que cada dos bases de un grupo libre tienen el mismo cardinal. Llamamos **rango** de un grupo libre F al cardinal de una base de F.
Otra de las consecuencias de la construcción de grupos libres aparecen en la siguiente sección.

Presentaciones por grupos libres

Proposición. 12.8.
Cada grupo G es un cociente de un grupo libre.

DEMOSTRACIÓN. Sea G un grupo; consideramos el conjunto $X = G$ construimos el grupo libre $F(X)$. Definimos una aplicación $f : X \longrightarrow G$ mediante $f(g) = g$ para cada $g \in X$. Por ser $F(X)$ un grupo libre sobre X existe un único homomorfismo de grupos $f' : F(X) \longrightarrow G$ tal que $f'i = f$. Es claro que f' es una aplicación sobreyectiva. □

Sea G un grupo y S un subconjunto de G no vacío, llamamos **clausura normal** de S en G a la intersección de todos los subgrupos normales de G que contienen a S.

Lema. 12.9.
En la situación anterior, la clausura normal de S es el subgrupo de G generado por todos los conjugados de los elementos de S.

DEMOSTRACIÓN. Llamamos N a la clausura normal de N en G, entonces para cada $s \in S$ y cada $g \in G$ tenemos $gsg^{-1} \in N$, luego $K = \langle \{gsg^{-1} \mid s \in S, g \in G\} \rangle \subseteq N$. Basta entonces ver que K es un subgrupo normal de G, sea $k \in K$, entonces $k = g_1 s_1 g_1^{-1} g_2 s_2 g_2^{-1} \cdots g_r s_r g_r^{-1}$, $s_i \in S$, $g_i \in G$, $1 \leq i \leq r$, sea ahora $g \in G$, entonces

$$gkg^{-1} = (gg_1)s_1(gg_1)^{-1}(gg_2)s_2(gg_2)^{-1} \cdots (gg_r)s_r(gg_r)^{-1} \in K.$$

□

Proposición. 12.10.
Sea F el grupo libre sobre un conjunto X, entonces F' (el subgrupo derivado de F) es la clausura normal en F de $\{[x,y] \mid x,y \in X\}$.

DEMOSTRACIÓN. Llamamos N a la clausura normal de $\{[x,y] \mid x,y \in X\}$ en F, se verifica que $N \subseteq F'$; si consideramos F/N, resulta que un sistema de generadores es $\{xN \mid x \in X\}$, y estos conmutan entre sí, por tanto F/N es un grupo abeliano, luego $F' \subseteq N$. □

Teorema. 12.11.
Sea F el grupo libre sobre un conjunto finito $X = \{x_1, \ldots, x_n\}$, entonces F/F' es el grupo abeliano libre sobre X.

DEMOSTRACIÓN. Llamamos G el grupo abeliano libre sobre X. Ya que $G \cong \mathbb{Z}^n$, sea e_i, $1 \leq i \leq n$, el elemento de G que tiene 1 en el lugar i y 0 en el resto. Definimos $f : F \longrightarrow G$ mediante $f(x_i) = e_i$, $1 \leq i \leq n$. Ya que G es un grupo abeliano, tenemos $F' = [F,F] \subseteq \mathrm{Ker}(f)$. Para probar que $F' = \mathrm{Ker}(f)$, sea $h \notin F'$, existen $y_1, \ldots, y_r \in X$, $y_i \neq y_j$ si $i \neq j$, y $g_1, \ldots, g_r \in \mathbb{Z}^*$ e $y \in F'$ tales que $h = y_1^{g_1} \ldots y_r^{g_r} y$, entonces $f(h) = f(y_1)^{g_1} \ldots f(y_r)^{g_r} \neq 0$, y $h \notin \mathrm{Ker}(f)$. □

Presentaciones de grupos

Sea G un grupo, entonces existe un grupo libre F y un homomorfismo sobreyectivo $p : F \longrightarrow G$. Si llamamos $K = \mathrm{Ker}(p)$ al núcleo de p, se verifica $G \cong F/K$. Llamamos a K el **núcleo definidor** de G con respecto a F.

El **teorema de Nielsen-Schreier** nos asegura que *cada subgrupo de un grupo libre es también un grupo libre*. En particular K es un grupo libre.

Supongamos que X es una base de F y R es una base de K, escrita en función de la base X, entonces X y R determinan completamente a G, ya que determinan a F, a K y ala inclusión.

Si consideramos la proyección $p : F \to G$, entonces $p(X)$ es un conjunto de generadores de G, y para cada $r \in R$ se verifica $p(r) = 1$. Tenemos por tanto una relación que verifican los generadores de G. Por esta razón a los conjuntos $p(X)$ y X se les llama **sistemas de generadores** de G, y al conjunto R se les llama **conjunto de relaciones de definición** de G.

El problema que surge es el siguiente: En general dado G es posible obtener un conjunto X de generadores para G, y por tanto el grupo F. Pero la obtención de K es más complicada. Ya conocemos que si $S \subseteq F$ es un subconjunto de F, entonces S genera un único subgrupo normal de F; su clausura normal; entonces para determinar K basta con dar un subconjunto $S \subseteq F$ cuya clausura normal sea K. (Nota. En este caso K no va a ser el grupo libre generado por S.)

Dar una presentación de G por generadores y relaciones es dar los conjuntos X y S, y se suele escribir $G = \langle X \mid S \rangle$. Por extensión S se llama también el **conjunto de relaciones de definición** de G.

Un grupo G se llama **finitamente presentado** si $G = \langle X \mid S \rangle$, siendo X y S conjuntos finitos.

Lema. 12.12.
Cada grupo finito es finitamente presentado.

DEMOSTRACIÓN. Sea $G = \{g_1, \ldots, g_t\}$ un grupo finito. Consideramos el conjunto $X = \{x_1, \ldots, x_t\}$ y llamamos $F = F(X)$ al grupo libre sobre X. Definimos una aplicación $f : X \to G$ mediante $f(x_i) = g_i$, $i = 1, \ldots, t$, y sea $f' : F \to G$ el homomorfismo inducido.

Llamamos $S = \{x_i x_j x_k^{-1} \mid i, j, k = 1, \ldots, t;\ g_i g_j = g_k\}$. Es claro que $S \subseteq \mathrm{Ker}(f')$, y vamos a ver que $\mathrm{Ker}(f')$ es igual a la clausura normal de S en F. Tenemos que F/N tiene a $\{x_i N \mid i = 1, \ldots, t\}$ como sistema de generadores, y como este conjunto es cerrado para el producto, resulta que $F/N = \{x_i N \mid i = 1, \ldots, t\}$. Entonces como $N \subseteq \mathrm{Ker}(f')$, existe un homomorfismo sobreyectivo $F/N \to F/\mathrm{Ker}(f') \cong G$, y en consecuencia los dos cocientes de F tienen el mismo número de elementos. Se verifica entonces $N = \mathrm{Ker}(f')$. □

Como consecuencia de la introducción anterior tenemos el siguiente teorema, que es una consecuencia inmediata de la propiedad universal del grupo cociente.

Teorema. 12.13. (Teorema de Dyck.)
Sea G un grupo con presentación $\langle a_1, \ldots, a_n \mid r_1, \ldots, r_s \rangle$ y H un grupo con generadores $x_1, \ldots, x_m$, con $m \geq n$, que verifica las relaciones r_j, $1 \leq j \leq s$, cuando se sustituye a_i por x_i, $1 \leq i \leq n$, entonces la asignación $a_i \mapsto x_i$, $1 \leq i \leq n$, se extiende a un único homomorfismo de grupos de G en H.

Aplicaciones del teorema de Dick

Ejemplo. 12.14.
Presentación del grupo cíclico finito C_n. Una presentación de C_n es: $\langle x \mid x^n \rangle$.

Ejemplo. 12.15.
Presentación del grupo diédrico finito. Sea D_n el grupo diédrico de orden 2n, entonces D_n tiene dos generadores σ y τ que verifican: $\sigma^n = 1 = \tau^2 = \sigma\tau\sigma\tau$. Consideramos un grupo G dado por la presentación $\langle x, y \mid x^n, y^2, xyxy\rangle$. Por el teorema de Dick existe un homomorfismo de grupos $f : G \longrightarrow D_n$ definido por $f(x) = \sigma$ y $f(y) = \tau$, que es evidentemente sobreyectivo. Ahora bien, las relaciones para x e y implican que el orden de G está acotado por $2n$, y en consecuencia el homomorfismo f es un isomorfismo.

Ejemplo. 12.16.
Presentación del grupo simétrico S_n. Sea S_n el grupo simétrico de orden $n!$. Es bien conocido que S_n está generado por las trasposiciones, y que éstas verifican las siguientes relaciones:
Ya que $(xx{+}1)(x{+}1x{+}2) = (xx{+}1x{+}2)$*, entonces* $((xx{+}1)(x{+}1x{+}2))^3 = 1$*; y* $[(xx{+}1), (yy{+}1)] = 1$ *si* $\mid x - y \mid \geq 2$.
Consideramos un grupo G dado por la presentación

$$\langle x_1, \ldots, x_n \mid x_i^2,\ (x_i x i + 1)^3,\ [x_i, x_j] = 1 \text{ si } \mid i - j \mid \geq 2\rangle$$

Entonces G es isomorfo a S_n.

Cálculo de grupos de automorfismos

Ejemplo. 12.17. (Automorfismo de C_n)
Supongamos la presentación $C_n = \langle x \mid x^n\rangle$. Si $f \in \mathrm{Aut}(C_n)$, entonces $f(x) = x^i$ ha de ser un generador de C_n, y por tanto i verifica: $0 \leq i < n$, $\mathrm{mcd}\{i, n\} = 1$. Y recíprocamente, para cada i verificando estas condiciones tenemos $f_i \in \mathrm{Aut}(C_n)$, siendo $f_i(x) = x^i$. Existe un isomorfismo de grupos $\mathrm{Aut}(C_n) \longrightarrow \mathbb{Z}_n^\times$ definido por $f_i \mapsto \bar{i}$, y en consecuencia $\mid \mathrm{Aut}(C_n) \mid = \varphi(n)$, la función de Euler.

Ejemplo. 12.18. (Automorfismos de D_n)
Supongamos la presentación

$$D_n = \langle x, y \mid x^n, y^2, xyxy\rangle.$$

Cada automorfismo $f \in \mathrm{Aut}(D_n)$ está definido por las imágenes de x e y, y éstas han de verificar otra vez las condiciones de definición de x e y, entonces tenemos:

$$\begin{aligned} f(x) &= x^i, \quad \text{si } 0 \leq i < n,\ i \text{ primo relativo con } n \\ f(y) &= x^j y, \ \text{si } 0 \leq j < n \end{aligned}$$

ya que para que f sea un automorfismo $f(x) = x^i$ ha de ser un generador del único subgrupo de orden n, esto es, $\langle x\rangle$, y $f(y)$ ha de ser un elemento de orden dos que no pertenezca a $\langle x\rangle$. Y recíprocamente, si tomamos i y j verificando las condiciones anteriores, entonces los elementos $\alpha = x^i$ y $\beta = x^j y$ verifican:

$$\alpha^n = 1 = \beta^2 = \alpha\beta\alpha\beta$$

Luego por el teorema de Dick tenemos un automorfismo $f_{i,j} \in \mathrm{Aut}(D_n)$, definido por:

$$f(x) = x^i, \quad f(y) = x^j y$$

Es claro que tenemos la siguiente fórmula para la composición de dos automorfismos:

$$f_{i,j}f_{h,k} = f_{ih,ik+j}$$

Ejemplo. 12.19.
Dado un anillo R consideramos el conjunto $\mathbb{A}_1(R)$ de aplicaciones

$$f : R \longrightarrow R, \quad f(x) = ux + v,$$

siendo $u \in R^\times$, $v \in R$. Es claro que $\mathbb{A}_1(R)$ es cerrado para la composición y que si $f \in \mathbb{A}_1(R)$, entonces $f^{-1} \in \mathbb{A}_1(R)$, verificándose que si $f(x) = ux + v$, entonces $f^{-1}(x) = u^{-1}x - u^{-1}v$. Se llama el **grupo afín** de R.
Con la anterior notación se existe un isomorfismo $\mathrm{Aut}(D_n) \cong \mathbb{A}_1(\mathbb{Z}_n)$.

Ejemplo. 12.20.
$\mathrm{Aut}(Q_2) \cong S_4$.

Ejemplo. 12.21.
$\mathrm{Aut}(\mathbb{Z}_p^n) \cong \mathrm{GL}(n, \mathbb{Z}_p)$.

Algoritmo de Todd–Coxeter

Dar un grupo mediante una presentación por generadores y relaciones tiene el problema de que no conocemos fácilmente su estructura, y muy poco podemos asegurar sobre la misma. Sin embargo cuando un grupo finito está dado por generadores y relaciones, es posible determinar exactamente su orden mediante el algoritmo de Todd-Coxeter. Vamos a ver una pequeña introducción al mismo.
Supongamos que $G = \langle X \mid R \rangle$ es un grupo dado mediante generadores y relaciones. Elegimos un subgrupo H de G, al que vamos a calcular su índice en G si este es finito.
Para hacer esto seguimos los siguientes pasos:
(1) Construimos una tabla con una fila cero que contiene las relaciones de definición escritas en función de los elementos de X', separadas cada una de ellas por un separador, por ejemplo #. Deben de aparecer *todos los generadores* ya que el grupo por hipótesis es finito.
(2) La tabla se va completando del siguiente modo. La primera posición de cada fila se rellena con el número de orden de la fila. En particular **1** representa a la clase a la izquierda $H \in G/H$.
(3) Bajo el primer elemento, por ejemplo x_1, de la fila cero escribimos $x_1\mathbf{1}$. Si resulta que $x_1H = H$, entonces $x_1\mathbf{1} = \mathbf{1}$, en caso contrario será una nueva clase a la izquierda a la que podemos llamar, por ejemplo **2**.
(4) Bajo el segundo elemento, por ejemplo x_2, de la fila cero escribimos x_2(valor_anterior). Otra vez, si esta clase a la izquierda es conocida, ponemos su valor, en caso contrario le asignamos un valor, por ejemplo **3**. Seguimos de este modo.
(5) Bajo el último elemento antes de un separador el valor que se obtiene es siempre el valor de la fila. De este modo tendremos asignaciones del tipo x_r(valor_anterior)=valor_fila.
(6) Bajo los separadores debemos escribir siempre el número que representa la fila en la que estamos, e iniciamos el proceso en la misma forma que hasta ahora hasta llegar al siguiente separador.

(7) Cuando tengamos que un mismo valor es asignado a dos múltiplos distintos de un mismo elemento de la fila cero, entonces tenemos una coincidencia, que resolvemos del siguiente modo: sea

$$x_r(\text{valor}_1)=\text{valor}=x_r(\text{valor}_2),$$

entonces simplificando por x_r tenemos

$$\text{valor}_1=x_r^{-1}(\text{valor})=\text{valor}_2,$$

luego valor_1 y valor_2 coinciden y podemos identificarlos en toda la tabla.

(8) Com la acción de G sobre G/H es transitiva, el proceso acaba cuando se han obtenidos todos los elementos de la órbita de $\mathbf{1}$, esto es, cuando se ha completado la tabla de multiplicación de los generadores de G por las clases a la izquierda.

(9) El número de valores no coincidentes es el número de clases a la izquierda de H en G, y por tanto tenemos calculado el *índice* de H en G.

Ejemplo. 12.22.

Consideramos el grupo $G=\langle x,y;x^3=y^2=(xy)^2=1\rangle$. Llamamos H al subgrupo generado por y, esto es, $H=\langle y\rangle$, luego $|\,H\,|\leq 2$.

La tabla de multiplicación antes señalada es:

	y	y	#	x	x	x	#	x	y	x	y	#
	$y\mathbf{1}$	$y\mathbf{1}$		$x\mathbf{1}$	$x\mathbf{2}$	$x\mathbf{3}$		$x\mathbf{1}$	$y\mathbf{2}$	$x\mathbf{4}$	$y\mathbf{5}$	
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{3}$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{4}$	$\mathbf{5}$	$\mathbf{1}$	$\mathbf{1}$
	$y\mathbf{2}$	$y\mathbf{3}$		$x\mathbf{2}$	$x\mathbf{3}$	$x\mathbf{1}$		$x\mathbf{2}$	$y\mathbf{3}$	$x\mathbf{2}$	$y\mathbf{3}$	
$\mathbf{2}$	$\mathbf{3}$	$\mathbf{2}$	$\mathbf{2}$	$\mathbf{3}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{2}$	$\mathbf{3}$	$\mathbf{2}$	$\mathbf{3}$	$\mathbf{2}$	$\mathbf{2}$

(Tenemos $y\mathbf{5}=\mathbf{1}=y\mathbf{1}$, luego $\mathbf{5}=y^{-1}\mathbf{1}=\mathbf{1}$. Tenemos $x\mathbf{4}=\mathbf{1}=x\mathbf{3}$, luego $\mathbf{4}=x^{-1}\mathbf{1}=\mathbf{3}$.)

Esto termina la tabla; el número de clases laterales de H en G es igual a 3.

La tabla de multiplicación antes señalada es:

$1\setminus 2$	y	x
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{2}$
$\mathbf{2}$	$\mathbf{3}$	$\mathbf{3}$
$\mathbf{3}$	$\mathbf{2}$	$\mathbf{1}$

que en este caso permite obtener una representación del grupo G, ya que los generadores x e y actúan sobre el conjunto de clases laterales, luego se pueden interpretar como permutaciones de este conjunto. En este caso son $\mathbf{1}$, $\mathbf{2}$ y $\mathbf{3}$. Asignamos a y el elemento $(\mathbf{2\,3})\in S_3$, y a x el elemento $(\mathbf{1\,2\,3})\in S_3$. Entonces existe un homomorfismo, el de la acción, de G a S_3. El núcleo es H_G, el mayor subgrupo normal de G contenido en H, pero como $y\in H\setminus H_G$, resulta que $H_G=\{1\}$, y por tanto G es isomorfo al subgrupo de S_3 generado por $(\mathbf{2\,3})$ y $(\mathbf{1\,2\,3})$, en este caso es todo S_3.

13. Ejercicios propuestos

Grupos libres

Ejercicio. 13.1.
Demuestra que si F es un grupo libre no trivial, entonces F contiene un subgrupo isomorfo a $\mathbb{Z}$, el grupo cíclico infinito.
Ref.: 3304e_001 *SOLUCIÓN.*

Ejercicio. 13.2.
Demuestra que ningún grupo libre no trivial es finito.
Ref.: 3304e_002 *SOLUCIÓN.*

Ejercicio. 13.3.
Demuestra que el centro de un grupo libre sobre un conjunto con dos o más elementos es trivial. Como consecuencia, ningún grupo libre sobre un conjunto con más de dos elementos es abeliano.
Ref.: 3304e_003 *SOLUCIÓN.*

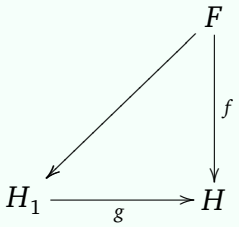
Ejercicio. 13.4.
Demuestra que el producto (directo) de dos grupos cíclicos infinitos no es un grupo libre.
Ref.: 3304e_004 *SOLUCIÓN.*

3304-09.tex

Ejercicio. 13.5.
Demuestra que un grupo libre sobre un conjunto con n elementos no tiene un sistema de generadores formado por $n-1$ elementos.
Ref.: 3304e_005 SOLUCIÓN.

Ejercicio. 13.6.
¿Cuantas palabras reducidas de longitud k hay en un grupo libre de rango n?
Ref.: 3304e_006 SOLUCIÓN.

Ejercicio. 13.7.
Demuestra que un grupo F es libre si, y sólo si, verifica la siguiente propiedad: Para todo homomorfismo $f : F \longrightarrow H$ y todo epimorfismo $g : H_1 \longrightarrow H$ existe un homomorfismo (no necesariamente único) $f_1 : F \longrightarrow H_1$ tal que $f = gf_1$.



Ref.: 3304e_007 SOLUCIÓN.

Ejercicio. 13.8.
Una palabra se llama cíclicamente reducida si no es conjugada a una palabra más corta.

1. *Demuestra que toda palabra es conjugada a otra cíclicamente reducida*
2. *Dos palabras cíclicamente reducidas son conjugadas si, y sólo si, una de ellas es una permutación cíclica de la otra.*

(Esto resuelve el problema de conjugación para grupos libres, es decir, el problema de decidir en un número finito de pasos si un par de palabras representan elementos conjugados).
Ref.: 3304e_008 *SOLUCIÓN.*

Ejercicio. 13.9.
Demuestra que cualquier elemento no trivial de un grupo libre tiene orden infinito.
Ref.: 3304e_009 *SOLUCIÓN.*

Ejercicio. 13.10.
Demuestra que dos elementos de un grupo libre conmutan si, y sólo si, pueden escribirse como potencias del mismo elemento.
Ref.: 3304e_010 *SOLUCIÓN.*

Ejercicio. 13.11.
Sea F libre con base X y sea $Y \subset X$. Demuestra que el grupo $H = \langle Y \rangle$ es libre sobre Y.
Ref.: 3304e_011 *SOLUCIÓN.*

Ejercicio. 13.12.
Sea X un conjunto de generadores para un grupo F. Demuestra que F es libre sobre X si, y sólo si, toda palabra no vacía reducida sobre X es distinta de 1.
Ref.: 3304e_012 *SOLUCIÓN.*

Ejercicio. 13.13.
Sea F un grupo libre sobre X. Demuestra que el conjunto H de las palabras reducidas de longitud par sobre X es un subgrupo normal de F. ¿Cual es el grupo cociente F/H?
Ref.: 3304e_013 *SOLUCIÓN.*

Ejercicio. 13.14.
Sea F libre sobre $X = \{x, y\}$. Demuestra que F tiene tres subgrupos de índice 2. Determina un sistema de generadores para cada uno de ellos.
Ref.: 3304e_014 *SOLUCIÓN.*

Ejercicio. 13.15.
Sea F libre sobre $X = \{x, y\}$. Determina cuántos subgrupos normales de índice tres tiene F.
Ref.: 3304e_015 *SOLUCIÓN.*

Ejercicio. 13.16.
Sea F un grupo libre de rango finito n. Demuestra que para cada $k \in \mathbb{N}$ el conjunto de subgrupos normales de índice k de F es finito.
Ref.: 3304e_016 *SOLUCIÓN.*

Ejercicio. 13.17.
Sea F un grupo libre, sea H un subgrupo de índice finito $m = [F : H]$ y sea $K \neq \{1\}$ un subgrupo no trivial arbitrario de F. Demuestra que $H \cap K \neq \{1\}$.
Ref.: 3304e_017 *SOLUCIÓN.*

Ejercicio. 13.18.
Demuestra que en un grupo libre de rango 3 todo subgrupo de índice finito tiene rango impar.
Ref.: 3304e_018 *SOLUCIÓN.*

Ejercicio. 13.19.
En el grupo libre sobre $\{x, y, z\}$ sea H el subgrupo generado por todos los cuadrados. ¿Cuánto vale el índice $[F : H]$? Halla una base para H.
Ref.: 3304e_019 *SOLUCIÓN.*

Ejercicio. 13.20.
Sea F el grupo libre sobre $X = \{x, y\}$. Para todo $n \in \mathbb{N}$ definimos $y_n = x^n y x^{-n}$.

(1) Demuestra que toda palabra reducida no vacía sobre $\{y_1, y_2, \ldots, y_r\}$ con $r \in \mathbb{N}$ es distinta de 1.
(2) Deduce que el grupo $F_r = \langle y_1, \ldots, y_r \rangle$ es libre sobre $\{y_1, \ldots, y_r\}$.
(3) Deduce también que los elementos $\{y^n x y^{-n} \mid n \in \mathbb{N}\}$ forman una base para el subgrupo que generan.
(4) Concluye que todo grupo libre de rango mayor o igual que 2 contiene un subgrupo libre de rango numerable.

Ref.: 3304e_020 *SOLUCIÓN.*

Ejercicio. 13.21.
Demuestra que el subgrupo conmutador de un grupo libre sobre dos generadores no es finitamente generado. (En consecuencia un subgrupo de un grupo finitamente generado no tiene que ser finitamente generado).
Ref.: 3304e_021 *SOLUCIÓN.*

Ejercicio. 13.22.
Sea S un subconjunto de un grupo G tal que para todo $x \in G$ se verifique que $xSx^{-1} \subset S$. Demuestra que el subgrupo $\langle S \rangle$ generado por S es normal en G.
Sea T cualquier subconjunto de G y sea $S = \cup_{x \in G} xTx^{-1}$. Demuestra que $\langle S \rangle$ es la clausura normal de T en G.
Ref.: 3304e_022 *SOLUCIÓN.*

Ejercicio. 13.23.
Sea $G = \langle X \rangle$ un grupo generado por el conjunto X, sea H un subgrupo de G y sea T una transversal de H en G (en T hay un y sólo un elemento de cada clase de G/H). Sea $TXT^{-1} = \{txs^{-1} \mid t,s \in T,\ x \in X\}$.
Demuestra que $(TXT^{-1}) \cap H$ es un conjunto de generadores de H.
Ref.: 3304e_023 *SOLUCIÓN.*

Ejercicio. 13.24.
Prueba que el grupo $G = \langle x, y \mid x^3, y^4 \rangle$ es un grupo infinito y no abeliano.
Ref.: 3304e_024 *SOLUCIÓN.*

Ejercicio. 13.25.
Prueba que cada grupo libre F finitamente generado y no trivial contiene un subgrupo de índice 2 (y por tanto normal). Prueba que F tiene sólo un número finito de subgrupos de índice dos.
Ref.: 3304e_025 *SOLUCIÓN.*

Ejercicio. 13.26.
Prueba que el grupo $G = \langle x, y \mid x^6, y^6, (xy)^3 \rangle$ es un grupo no abeliano.
Ref.: 3304e_026 *SOLUCIÓN.*

Ejercicio. 13.27.
Describir el producto directo de grupos.

(1) Sean F_1, F_2 grupos libres finitamente generados, describe las relaciones que definen el grupo producto directo $F_1 \times F_2$.
(2) Sean $G_i = \langle F_i \mid R_i \rangle$ grupos finitamente generados, definidos por generadores y relaciones. Describe las relaciones que definen el grupo producto directo $G_1 \times G_2$.

Ref.: 3304e_027 *SOLUCIÓN.*

Capítulo V

Series de composición. Grupos solubles. Teorema de Abel

14 Series de composición 147
15 Teorema de Schreier 150
16 Grupos solubles 152
17 Subgrupo derivado 154
18 Teorema de Abel 157
19 Ejercicios Propuestos 160

Introducción.

14. Series de composición

Si G es un grupo, una cadena de subgrupos

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G, \tag{V.1}$$

donde cada H_{i-1} es un subgrupo normal de H_i, para $1 \leq i \leq n$, se llama una **serie normal** de G. Llamamos **términos** de la serie a los subgrupos H_i, $0 \leq i \leq n$, y **factores** de la serie a los grupos cocientes H_i/H_{i-1}, $1 \leq i \leq n$.

La serie (V.1) se llama **propia** si para cada índice i se tiene $H_i \triangleleft H_{i+1}$. En este caso llamamos a n la **longitud** de la serie.

Si

$$\{1\} = K_0 \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_{m-1} \trianglelefteq K_m = G \tag{V.2}$$

es otra serie normal de G, diremos que (V.2) es un **refinamiento** de (V.1) si $n \leq m$ y existen $0 \leq j_0 < j_1 < j_{n-1} < j_n \leq n$ tales que $H_i = K_{j_i}$, $0 \leq i \leq n$. Como consecuencia la serie (V.1) puede ser obtenida de la (V.2) eliminando algunos términos.

La serie (V.2) se llama un **refinamiento propio** de (V.1) si es un refinamiento y existe algún j tal que $0 \leq j \leq m$ y $H_i \neq K_j$ para todo $0 \leq i \leq n$.
Llamamos **serie de composición** de G a una serie normal propia que no tiene refinamientos propios.
Los factores de una serie de composición de llaman **factores de composición** de la serie.
Un grupo G se llama **simple** si es no trivial y sus únicos subgrupos normales son $\{1\}$ y G. Es claro que si G es un grupo simple, entonces $\{1\} \lhd G$ es una serie de composición de G.
Como aplicación, en los grupos finitos veremos que las series de composición son una herramienta muy efectiva para determinar su estructura.

Teorema. 14.1.
Todo grupo finito G tiene al menos una serie de composición.

DEMOSTRACIÓN. Si G es el grupo trivial, entonces una serie de composición es: $\{1\} = G$. Hacemos la siguiente hipótesis de inducción: todo grupo finito de orden menor ó igual que m tiene una serie de composición. El resultado es cierto para $m = 1$; supongamos que sea cierto para $m = r-1$ y que G es un grupo de orden $r > 1$. Si G es simple entonces tiene una serie de composición. Si G no es simple tomamos un subgrupo normal propio no trivial N de G, con $|N|$ maximal entre los subgrupos normales propios, entonces N tiene una serie de composición, ya que $| N |<| G |$;

$$\{1\} = H_0 \lhd H_1 \lhd \cdots \lhd H_{n-1} \lhd H_n = N,$$

y por la maximalidad de N no existe ningún subgrupo normal N' verificando $N \subseteq N' \subseteq G$, luego

$$\{1\} = H_0 \lhd H_1 \lhd \cdots \lhd H_{n-1} \lhd H_n = N \lhd H_{n+1} = G$$

es una serie de composición para G. □

Teorema. 14.2.
Para una serie normal de un grupo G

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G \tag{V.3}$$

son equivalentes los siguientes enunciados:
(a) Es una serie de composición;
(b) Todos los factores de la serie, H_i/H_{i-1}, $1 \leq i \leq n$, son grupos simples.

DEMOSTRACIÓN. (a)⇒(b). Si (V.3) es una serie de composición, entonces es una serie propia y cada factor es un grupo no trivial. Si un factor H_i/H_{i-1} no es un grupo simple, entonces existe un subgrupo

normal H/H_{i-1} verificando: $\{1\} \subsetneqq H/H_{i-1} \subsetneqq H_i/H_{i-1}$, tenemos que $H_{i-1} \subsetneqq H \subsetneqq H_i$, luego podemos considerar el refinamiento de la serie (V.3)

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_i \lhd H \lhd H_{i+1} \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G,$$

lo que es una contradicción ya que (V.3) es una serie de composición.

(b)⇒(a). Supongamos ahora que la serie normal en (V.3) no es una serie de composición, entonces ó no es una serie propia, ó tiene refinamientos propios. En el primer caso si por ejemplo $H_i = H_{i+1}$, para algún $0 \leq i < n$, es claro que $H_{i+1}/H_i = \{1\}$ no es un grupo simple. En el segundo caso, si

$$\{1\} = K_0 \lhd K_1 \lhd \cdots \lhd K_{m-1} \lhd K_m = G$$

es una serie normal propia que es un refinamiento propio de (V.3), existen, por ejemplo, $0 \leq j_i < j < j_{i+1} \leq m$ tales que $K_{j_i} = H_i$, $K_{j_{i+1}} = H_{i+1}$, y por tanto H_{i+1}/H_i tiene un subgrupo normal, K_j/H_i, distinto del trivial y del total, luego H_{i+1}/H_i no es un grupo simple. □

15. Teorema de Schreier

Sea G un grupo, dos series normales de G

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G \tag{V.4}$$

$$\{1\} = K_0 \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_{m-1} \trianglelefteq K_m = G \tag{V.5}$$

se llaman **equivalentes** si verifican:

(1) $n = m$ y
(2) existe una permutación $\sigma \in S_n$ tal que $H_i/H_{i-1} \cong K_{\sigma(i)}/K_{\sigma(i)-1}$, $1 \leq i \leq n$.

Lema. 15.1.
Toda serie normal de G que es equivalente a una serie de composición de G es una serie de composición de G.

Teorema. 15.2. (Teorema de Schreier)
Cada dos series normales de un grupo G tienen refinamientos equivalentes.

DEMOSTRACIÓN. Supongamos que tenemos las dos series normales de G

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G \tag{V.6}$$

$$\{1\} = K_0 \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_{m-1} \trianglelefteq K_m = G \tag{V.7}$$

Construimos un refinamiento de (V.6) llamando $H_{-1} = \{1\}$ e insertando entre H_{i-1} y H_i un total de $m-1$ subgrupos H_{ij}, para $0 \leq i \leq n$, $0 \leq j \leq m$, definidos mediante

$$H_{ij} = (H_i \cap K_j)H_{i-1}.$$

Para cada i tenemos una cadena de subgrupos

$$H_{i-1} = H_{i0} \trianglelefteq H_{i1} \trianglelefteq H_{i2} \trianglelefteq \cdots \trianglelefteq H_{im-1} \trianglelefteq H_{im} = H_i;$$

3306-02.tex

por el Lema de Zassenhaus cada uno es normal en el siguiente; y se verifica:

$$H_{i0} = (H_i \cap K_0)H_i = (H_i \cap \{1\})H_{i-1} = H_{i-1},$$

$$H_{im} = (H_i \cap K_m)H_{i-1} = (H_i \cap G)H_{i-1} = H_iH_{i-1} = H_i.$$

El refinamiento es:

$$\{1\} = H_{00} \trianglelefteq \cdots \trianglelefteq H_{i-1} = H_{i0} \trianglelefteq H_{i1} \trianglelefteq \cdots \trianglelefteq H_{in-1} \trianglelefteq H_{in} = H_i \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G.$$

También construimos un refinamiento de (V.7) insertando entre K_{j-1} y K_j un total de $n-1$ subgrupos K_{ji}, para $0 \leq j \leq m$, $0 \leq i \leq n$, definidos por

$$K_{ji} = (K_j \cap H_i)K_{j-1}.$$

Este refinamiento verifica las mismas propiedades que el anterior. Para ver que estos refinamientos son equivalentes tenemos por el Lema de Zassenhaus

$$\frac{H_{ij}}{H_{ij-1}} = \frac{(H_i \cap K_j)H_{i-1}}{(H_i \cap K_{j-i})H_{i-1}} \cong \frac{(K_j \cap H_i)K_{j-1}}{(K_j \cap H_{i-1})K_{j-1}} = \frac{K_{ji}}{K_{ji-1}}.$$

□

Teorema. 15.3. (Teorema de Jordan-Hölder)
Si un grupo G tiene una serie de composición, entonces se verifica:

(1) Toda serie normal propia de G tiene un refinamiento que es una serie de composición.
(2) Cada dos series de composición de G son equivalentes.

DEMOSTRACIÓN. (1). Supongamos que

$$\{1\} = H_0 \lhd H_1 \lhd \cdots \lhd H_{n-1} \lhd H_n = G \tag{V.8}$$

es una serie normal propia de G y que

$$\{1\} = K_0 \lhd K_1 \lhd \cdots \lhd K_{m-1} \lhd K_m = G \tag{V.9}$$

es una serie de composición de G. Aplicando el teorema de Schreier, existen refinamientos equivalentes de estas dos series, si eliminamos términos repetidos en estos refinamientos, obtenemos dos series normales propias equivalentes, llamémoslas $*$ y $**$. Ya que (V.9) es una serie de composición no tiene refinamientos propios, luego la serie obtenida a partir de (V.9) ha de coincidir con (V.9), sea por ejemplo $**$, entonces (V.8) tiene un refinamiento, $*$, equivalente a la serie de composición (V.9). (2). Si en el apartado anterior las dos series son de composición, entonces (V.8) no tiene refinamientos propios, y por lo tanto las dos series son equivalentes. □

Ya que cada dos series de composición de un grupo G son equivalentes, los factores de composición están determinados de forma única y los llamaremos **factores de composición** de G.

16. Grupos solubles

Sea G un grupo, una serie normal de G se llama **abeliana** ó **soluble** si todos sus factores son grupos abelianos. Un grupo G se llama **soluble** si tiene una serie normal abeliana.

Teorema. 16.1.
Todo grupo abeliano es soluble.

DEMOSTRACIÓN. Si G es un grupo abeliano, una serie normal abeliana es $\{1\} \lhd G$. □

Proposición. 16.2.
Si G es un grupo soluble, entonces todo subgrupo y todo grupo cociente de G es también soluble.

DEMOSTRACIÓN. Sea $\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G$ una serie normal abeliana de G. Si H es un subgrupo de G, entonces

$$\{1\} = H_0 \cap H \trianglelefteq H_1 \cap H \trianglelefteq \cdots \trianglelefteq H_{n-1} \cap H \trianglelefteq H_n \cap H = H,$$

es una serie normal de H. Si analizamos un factor tenemos, por el segundo teorema de isomorfía,

$$\frac{H \cap H_i}{H \cap H_{i-1}} \cong \frac{H \cap H_i}{(H \cap H_i) \cap H_{i-1}} \cong \frac{(H \cap H_i)H_{i-1}}{H_{i-1}} \leq \frac{H_i}{H_{i-1}},$$

y es un grupo abeliano. Si K es un subgrupo normal de G, entonces

$$\{1\} = H_0K/K \trianglelefteq H_1K/K \trianglelefteq \cdots \trianglelefteq H_{n-1}K/K \trianglelefteq H_nK/K = G/K,$$

es una serie normal de G/K. Si analizamos un factor tenemos, por el Lema de Zassenhaus y la regla de Dedekind,

$$\frac{H_iK/K}{H_{i-1}K/K} \cong \frac{H_iK}{H_{i-1}K} \cong \frac{H_i(H_{i-1}K)}{H_{i-1}K} \cong \frac{H_i}{(H_{i-1}K) \cap H_i} \cong \frac{H_i}{H_{i-1}(K \cap H_i)},$$

ya que $H_{i-1} \subseteq H_{i-1}(H_i \cap K)$, resulta que es un cociente de H_i/H_{i-1}, y por tanto es un grupo abeliano. □

3306-03.tex

Teorema. 16.3.
Sea K un subgrupo normal de un grupo G, si K y G/K son grupos solubles, entonces G es también soluble.

DEMOSTRACIÓN. Supongamos que

$$\{1\} = K_0 \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_{m-1} \trianglelefteq K_m = K$$

es una serie normal abeliana de K, y que

$$\{1\} = H_0/K \trianglelefteq H_1/K \trianglelefteq \cdots \trianglelefteq H_{n-1}/K \trianglelefteq H_n/K = G/K$$

es una serie normal abeliana de G/K, entonces $H_0 = K$, y si consideramos la serie

$$\{1\} = K_0 \trianglelefteq K_1 \trianglelefteq \cdots K_m = K = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G,$$

tenemos una serie normal de G que además es abeliana. Luego G es un grupo soluble. □

Este Teorema es una de la motivaciones para introducir los grupos solubles; es claro que si G es un grupo abeliano, entonces cada subgrupo y cada grupo cociente es también abeliano. En cambio, si G es un grupo que contiene un subgrupo normal abeliano N tal que el cociente G/N es abeliano, no necesariamente G es un grupo abeliano; ver por ejemplo el grupo simétrico S_3; en cambio G es siempre un grupo soluble.

17. Subgrupo derivado

Vamos ahora a buscar otra aproximación a los grupos solubles. Si G es un grupo y $a, b \in G$ son elementos de G, llamamos **conmutador** de a y b al elemento

$$[a,b] = aba^{-1}b^{-1},$$

esto es, se tiene $ab = [a,b]ba$.

Si A y B son subgrupos de G, definimos $[A,B]$ como el subgrupo de G *generado* por los elementos $[a,b]$, con $a \in A$ y $b \in B$.

Llamamos **subgrupo conmutador** ó **derivado** de G al subgrupo $G' = [G,G]$.

Lema. 17.1.
Para todo grupo G el subgrupo derivado G' es un subgrupo normal de G. (En realidad es un grupo totalmente invariante, y por lo tanto característico).

DEMOSTRACIÓN. Basta comprobar que es un subgrupo característico; sea $[a,b]$ un generador de G', para cada automorfismo f de G se verifica $f([a,b]) = [f(a), f(b)] \in G'$, luego se tiene el resultado. □

Teorema. 17.2.
*Si G es un grupo, el subgrupo derivado es el menor subgrupo normal N de G tal que G/N es un grupo abeliano. Como consecuencia de esto el grupo G/G' se llama el **grupo abelianizado** de G.*

DEMOSTRACIÓN. Es claro que G/G' es un grupo abeliano, ya que si $a, b \in G$, entonces

$$(bG')(aG') = ([a,b]G')(bG')(aG') = (aG')(bG').$$

Sea ahora un subgrupo N de G tal que G/N es abeliano, entonces para $a, b \in G$ se verifica

$$(aN)(bN) = (bN)(aN),$$

luego $[a,b] = aba^{-1}b^{-1} \in N$, y por tanto $G' \subseteq N$. □

3306-04.tex

Para caracterizar los grupos solubles a partir del subgrupo derivado, vamos a construir una serie normal. Para esto definimos los subgrupos derivados de orden superior de un grupo. Sea G un grupo, definimos por recurrencia

$$\begin{cases} G^{(0)} = G, \\ G^{(n+1)} = [G^{(n)}, G^{(n)}], \text{ para cada } n \in \mathbb{N}. \end{cases}$$

Tenemos que $G^{(n+1)}$ es un subgrupo normal de $G^{(n)}$, y que

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq \cdots \trianglerighteq G^{(n)} \trianglerighteq \cdots$$

es una cadena descendente de subgrupos normales de G, a la que vamos a llamar la **serie derivada** de G. La serie derivada se estabiliza si existe n tal que $G^{(n)} = G^{(n+1)}$.

Teorema. 17.3.
Un grupo G es soluble si, y sólo si, existe n tal que $G^{(n)} = \{1\}$.

DEMOSTRACIÓN. $\Leftarrow$). Si existe n tal que $G^{(n)} = \{1\}$, entonces

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq \cdots \trianglerighteq G^{(n)} = \{1\}.$$

es una serie normal abeliana de G, luego G es un grupo soluble.
$\Rightarrow$). Si G es un grupo soluble, con

$$G = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_{n-1} \trianglerighteq H_n = \{1\}$$

una serie normal abeliana de G, vamos a probar por inducción sobre i que $G^{(i)} \leq H_i$, para $1 \leq i \leq n$, y como resultado tendremos que $G^{(n)} = \{1\}$. Para $i = 0$ el resultado es claro, $G^{(0)} = H_0$. Supongamos que sea cierto para $i-1$ y vamos a probarlo para i; tenemos por hipótesis que $G^{(i-1)} \leq H_{i-1}$; ya que H_{i-1}/H_i es abeliano, tenemos que $[H_{i-1}, H_{i-1}] \leq H_i$, luego

$$G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \leq [H_{i-1}, H_{i-1}] \leq H_i.$$

□

Cuando G es un grupo soluble, el menor entero positivo n tal que $G^{(n)} = \{1\}$ se llama la **longitud derivada** de G.

Lema. 17.4.
Si G es un grupo simple y soluble, entonces G es un grupo cíclico de orden un número primo.

DEMOSTRACIÓN. Por ser simple tenemos que $G \neq \{1\}$. Por ser soluble existe n tal que $G^{(n)} = \{1\}$, luego G' es un subgrupo propio de G, y por ser normal y G simple ha de ser el subgrupo trivial; entonces G es un grupo abeliano, como es simple, necesariamente es de orden un número primo. □

Teorema. 17.5.
Sea G un grupo con una serie de composición; G es soluble si, y sólo si, cada factor de composición es cíclico de orden un número primo.

DEMOSTRACIÓN. $\Rightarrow$). Si G es soluble, entonces cada factor de composición es un grupo cociente de un subgrupo de G, por tanto es también un grupo soluble, ya que es un grupo simple, ha de ser cíclico de orden un número primo.
$\Leftarrow$). Si cada factor de composición de G es un grupo cíclico de orden un número primo, entonces existe una serie de composición que es abeliana, y por tanto G es un grupo soluble. □

Corolario. 17.6.
Todo grupo soluble con una serie de composición es un grupo finito.

18. Teorema de Abel

Recordemos que el grupo alternado A_n es el subgrupo de S_n formado por las permutaciones pares, vamos a ver que los grupos A_n, para n mayor ó igual que 5, son grupos simples no abelianos.

Lema. 18.1.
Para $n \geq 3$, A_n está generado por los ciclos (123), (124), $\ldots$,$(12n)$.

DEMOSTRACIÓN. Para el caso $n = 3$ es evidente, ya que

$$A_3 = \{1, (123), (132) = (123)^2\}.$$

Supongamos que $n > 3$; todo elemento de A_n es un producto de elementos de la forma $(ij)(hk)$ ó $(ij)(ih)$, siendo i, j, h y k elementos distintos de $\{1, \ldots, n\}$. Se verifica:

$$(ij)(hk) = (ihj)(ihk) \; y \; (ij)(ih) = (ihj),$$

Entonces A_n está generado por los ciclos de longitud tres. Basta ver que todo ciclo de longitud tres se escribe en función de los elementos del enunciado; pero esto es claro, ya que:

$$\begin{array}{l} (ijh) = (12i)(2jh)(1i2) = (12i)(2jh)(12i)^{-1}, \; i,j,h \neq 1,2 \\ (2jh) = (12j)(12h)(1j2) = (12j)(12h)(12j)^{-1}, \; j,h \neq 1,2 \\ (1jh) = (1h2)(12j)(12h) = (12h)^{-1}(12j)(12h), \; j,h \neq 1,2 \end{array}$$

□

Teorema. 18.2. (Teorema de Abel)
Para $n \geq 5$, A_n es un grupo simple.

DEMOSTRACIÓN. Supongamos que N es un subgrupo normal no trivial de A_n; vamos a ver que $N = A_n$. Consideramos $1 \neq \sigma \in N$, que mueve el menor número de elementos. Por ser σ una permutación par ha de mover más de dos elementos, vamos a probar que mueve exactamente tres. Supongamos que σ mueve más de tres elementos, se presentan los dos casos siguientes:

Caso 1. σ es un producto de ciclos disjuntos de longitud 2.

Caso 2. σ tiene un ciclo de longitud mayor ó igual que 3.

3306-05.tex

Caso 1. Suponemos que los elementos que mueve σ son x_1, x_2, ...
Sea $\sigma = (x_1x_2)(x_3x_4)\cdots$. Llamamos $\tau = (x_3x_4x_5)$, y definimos

$$\sigma_1 = (x_3x_4x_5)\sigma(x_3x_4x_5)^{-1},$$

entonces $\sigma_1 \in N$, luego

$$[\tau,\sigma] = (x_3x_4x_5)\sigma(x_3x_4x_5)^{-1}\sigma^{-1} = \sigma_1\sigma^{-1} \in N.$$

Si σ mueve también a x_5, entonces tenemos que

$$\sigma_1 = (x_1x_2)(x_3\sigma(x_5))(x_4x_5)\ldots,$$

luego

$$[\tau,\sigma] = (x_3\sigma(x_5))(x_4x_5)(x_3x_4)(x_5\sigma(x_5)),$$

y fija a x_1 y x_2 y sólo mueve a x_3, x_4, x_5 y $\sigma(x_5)$ más los otros elementos que movía σ. Si σ deja fijo a x_5, entonces tenemos que $\sigma_1 = (x_1x_2)(x_4x_5)$, luego $[\tau,\sigma] = (x_4x_5)(x_3x_4) = (x_3x_5x_4)$. En cualquier caso encontramos un elemento no trivial de N que mueve menos elementos que σ, lo que es una contradicción.
Caso 2. Al igual que antes podemos suponer que σ mueve los elementos $x_1, x_2, \ldots$ Supongamos que $\sigma = (x_1x_2x_3\ldots)\ldots$ Llamamos $\tau = (x_3x_4x_5)$, y definimos $\sigma_1 = (x_3x_4x_5)\sigma(x_3x_4x_5)^{-1}$. Entonces $\sigma_1 \in N$, luego

$$[\tau,\sigma] = (x_3x_4x_5)\sigma(x_3x_4x_5)^{-1}\sigma^{-1} = \sigma_1\sigma^{-1} \in N.$$

Vamos a suponer que σ mueve más de tres elementos. Ya que σ mueve más de tres elementos, si mueve solamente cuatro, tenemos que no sería una permutación par, luego ha de mover necesariamente cinco o más; así tenemos que $\sigma_1 = (x_1x_2x_4\ldots)$, luego $\sigma \neq \sigma_1$. El elemento $[\tau,\sigma] = \tau\sigma\tau^{-1}\sigma^{-1} = \sigma_1\sigma^{-1} \in N$ y no es la identidad, además $[\tau,\sigma]$ deja fijos todos los elementos que dejaba fijos σ, (ya que τ no mueve ninguno de ellos), y fija también el elemento x_2. Tenemos así un elemento no trivial de N que mueve menos elementos que σ, lo que es una contradicción.
Entonces N contiene un ciclo de longitud 3, supongamos que es (ijk), con i, j y k distintos, entonces:
1.) Si i, j, k, 1, 2 son distintos, tenemos que

$$(1i)(2j)(ijk)(1i)(2j) = (12k) \in N.$$

2.) Si $i = 1$, j, k, 2 son distintos, tenemos que existe h distinto de los anteriores y

$$(2j)(kh)(1jk)(2j)(kh) = (12h) \in N.$$

3.) Si $i = 2$, j, k y 1 son distintos, tenemos que existe h distinto de los anteriores y

$$(1k)(jh)(2jk)(1k)(jh) = (2h1) = (12h) \in N.$$

En cualquier otro caso tenemos que N también contiene un elemento de la forma $(12i)$ con $i \neq 1, 2$.
Si $j \neq 1$, 2, i, entonces

$$(12j) = (12)(ij)(12i)^{-1}(12)(ij),$$

y N contiene un conjunto de generadores de A_n, y por tanto coincide con A_n. □

Corolario. 18.3.
Para $n \geq 5$, el grupo S_n no es soluble.

DEMOSTRACIÓN. Tenemos una serie de composición de S_n,

$$\{1\} \lhd A_n \lhd S_n,$$

entonces por el teorema de Jordan-Hölder toda serie de composición es equivalente a la serie anterior, y los factores de composición no son cíclicos de orden un número primo, entonces por el Teorema (18.2.), S_n no es soluble. □

19. Ejercicios Propuestos

Series de composición

Ejercicio. 19.1.
Determinar todas las series de composición del grupo S_3.
Ref.: 3306e_001 *SOLUCIÓN*

Grupos solubles

Ejercicio. 19.2.
Demostrar que el grupo S_3 es soluble.
Ref.: 3306e_002 *SOLUCIÓN*

3306-09.tex

Capítulo VI

Producto directo de grupos

20 Producto directo finito de grupos 161
21 Producto directo de una familia de grupos 163
22 Producto directo interno 166
23 Ejercicios Propuestos 169

Introducción.

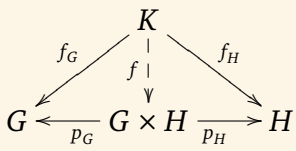
20. Producto directo finito de grupos

Sean G y H dos grupos. En el conjunto $G \times H$ se define una operación mediante

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

De esta forma $G \times H$ tiene estructura de grupo y las proyecciones e inclusiones canónicas son homomorfismos de grupos.

Proposición. 20.1. (Propiedad universal del producto directo)
Para cada terna de grupos G, H y K y cada par de homomorfismos $f_G : K \to G$ y $f_H : K \to H$ existe un único homomorfismo de grupos $f : K \to G \times H$ tal que $f_G = p_G f$ y $f_H = p_H f$.



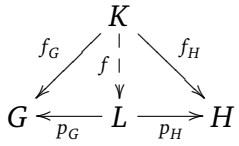
3305-01.tex

DEMOSTRACIÓN. *Unicidad.* Supongamos que existe algún f que verifica las condiciones del teorema. Calculemos cuanto puede valer. Para cada $k \in K$ se tiene

$$f(k) = (g,h), \text{ con } g = p_G f(k) = f_G(k), \text{ y } h = p_H f(k) = f_H(k).$$

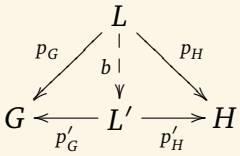
Así que la única forma de definir f es hacerlo como $f(k) = (f_G(k), f_H(k))$.
Existencia. Definimos para cada $k \in K$, la aplicación f mediante $f(k) = (f_G(k), f_H(k))$ según el punto anterior. Es inmediato comprobar que f es un homomorfismo de grupos y que verifica las condiciones exigidas. □

Se define entonces un **producto directo** de dos grupos G y H como un grupo L, junto con dos homomorfismos $p_G : L \to G$ y $p_H : L \to H$, verificando que para cada grupo K y para cada par de homomorfismo $f_G : K \to G$ y $f_H : K \to H$ existe un único homomorfismo de grupos $f : K \to L$ tal que $f_G = p_G f$ y $f_H = p_H f$.



Una consecuencia inmediata de la definición es:

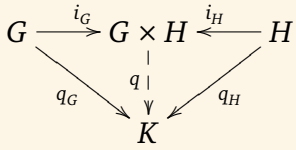
Proposición. 20.2.
Para cada par de grupos G y H si (L, p_G, p_H) y (L', p'_G, p'_H) son productos directos de G y H, entonces existe un isomorfismo $b : L \to L'$ tal que $p_G = p'_G b$ y $p_H = p'_H b$.



En particular tenemos un isomorfismo $L \cong G \times H$.

Finalmente veamos otra propiedad que verifica el producto directo.

Proposición. 20.3.
Sean G y H grupos y sea K un grupo tal que existen homomorfismos $q_G : G \to K$ y $q_H : H \to K$ verificando $q_G(g)q_H(h) = q_H(h)q_G(g)$ para todos $g \in G$ y $h \in H$. Entonces existe un único homomorfismo de grupos $q : G \times H \to K$ tal que $qi_G = q_G$ y $qi_H = q_H$



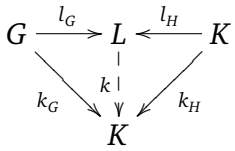
DEMOSTRACIÓN. *Unicidad.* Si q existe, verifica:

$$q(g,h) = q(g,1)q(1,h) = qi_G(g)qi_H(h) = q_G(g)q_H(h).$$

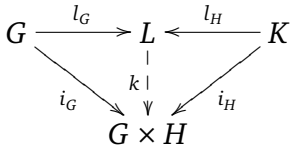
Luego en caso de existir es único.
Existencia. Definimos una aplicación $q : G \times H \longrightarrow K$ mediante: $q(g,h) = q_G(g)q_H(h)$. Se comprueba de inmediato que q es un homomorfismo de grupos y que verifica la conmutatividad del diagrama. □

Para este caso también tenemos un resultado sobre la unicidad del producto directo.

Proposición. 20.4.
Sean G y H grupos y L un grupo con dos homomorfismos $l_G : G \to L$ y $l_H : H \to L$ tales que $l_G(g)l_H(h) = l_H(h)l_G(g)$ para cada $g \in G$ y $h \in H$. Verificando que para cada grupo K y cada par de homomorfismos $k_G : G \to K$ y $k_H : H \to K$ tales que $k_G(g)k_H(h) = k_H(h)k_G(g)$ para cada $g \in G$ y $h \in H$ existe un único homomorfismo $k : L \to K$ tal que $kl_G = k_G$ y $kl_H = k_H$,



entonces existe un isomorfismo de grupos $b : L \cong G \times H$ tal que $bl_G = i_G$ y $bl_H = i_H$.
Podemos entonces aplicar el resultado a la terna $(G \times H, i_G, i_H)$ y obtenemos que existe un único isomorfismo que hace conmutar el diagrama siguiente:

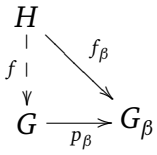


21. Producto directo de una familia de grupos

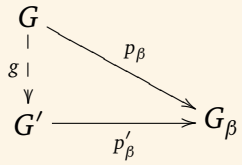
En esta sección pretendemos hacer una construcción universal en grupos, al estilo de la realizada para el grupo cociente, que sirve de ejemplo de como es posible obtener nuevos grupos a partir de grupos dados. Vamos a extender a una familia arbitraria la construcción anterior para dos grupos.

Dada una familia de grupos $\{G_\alpha \mid \alpha \in \Lambda\}$, llamamos **producto directo** de la familia a un par $(G; \{p_\alpha : G \longrightarrow G_\alpha \mid \alpha \in \Lambda\})$ formado por un grupo G y una familia de homomorfismos de grupos $\{p_\alpha\}_\alpha$, verificando la siguiente propiedad: Para cada grupo H y cada familia de homomorfismos de

grupos $\{f_\alpha : H \longrightarrow G_\alpha \mid \ \alpha \in \Lambda\}$, existe un único homomorfismo de grupos $f : H \longrightarrow G$ tal que $p_\beta f = f_\beta$, para cada $\beta \in \Lambda$.



Lema. 21.1.
Sea $\{G_\alpha \mid \ \alpha \in \Lambda\}$ una familia de grupos, si $(G; \{p_\alpha\}_\alpha)$ y $(G'; \{p'_\alpha\}_\alpha)$ son dos productos directos de la familia, entonces existe un isomorfismo de grupos $g : G \longrightarrow G'$ tal que $p'_\beta g = p_\beta$, para cada $\beta \in \Lambda$.



DEMOSTRACIÓN. Aplicando al par $(G, \{p_\alpha\}_\alpha)$ la definición de producto directo con el par $(G', \{p'_\alpha\}_\alpha)$, existe un único homomorfismo de grupos $h : G' \longrightarrow G$ verificando $p_\beta h = p'_\beta$ para cada $\beta \in \Lambda$. Aplicando la definición permutando los pares tenemos que existe un único homomorfismo $g : G \longrightarrow G'$ tal que $p'_\beta g = p_\beta$ para cada $\beta \in \Lambda$. Falta comprobar que $gh = 1_{G'}$ (resp. $hg = 1_G$); aplicamos la definición de producto directo al par $(G', \{p\}_\alpha)$ (resp. al par $(G, \{p_\alpha\}_\alpha)$) con él mismo y tenemos que existe un único homomorfismo $f : G' \longrightarrow G'$ verificando $p'_\beta f = p'_\beta$, para cada $\beta \in \Lambda$, pero $p'_\beta(hg) = p'_\beta = p'_\beta 1_{G'}$, luego $hg = 1_{G'}$, (resp. $gh = 1_G$). □

Este resultado nos asegura que, si existe, el producto directo de una familia de grupos, éste está determinado de forma única salvo isomorfismo. A continuación vamos a probar la existencia.

Lema. 21.2.
Para cada familia de grupos $\{G_\alpha \mid \ \alpha \in \Lambda\}$, el par

$$(\prod\{G_\alpha \mid \ \alpha \in \Lambda\}; \{p_\alpha : \prod\{G_\alpha \mid \ \alpha \in \Lambda\} \longrightarrow G_\alpha\})$$

es un producto directo de la familia.

DEMOSTRACIÓN. Consideramos el par $(H, \{f_\alpha : F \longrightarrow G_\alpha \mid \ \alpha \in \Lambda\})$ formado por un grupo H y una familia de homomorfismos de grupos. Definimos $f : H \longrightarrow \prod\{G_\alpha \mid \ \alpha \in \Lambda\}$ mediante $f(x) =$

$(f_\alpha(x))_\alpha$, para $x \in H$. Así definido f es un homomorfismo de grupos. Además verifica $p_\beta f = f_\beta$ para cada $\beta \in \Lambda$. Supongamos que existe otro homomorfismo de grupos f' verificando estas condiciones, entonces si $f'(x) = (x_\alpha)_\alpha$, para $\beta \in \Lambda$, se tiene $f_\beta(x) = (p_\beta f')(x) = p_\beta(f'(x)) = p_\beta((x_\alpha)_\alpha) = x_\beta$, luego $f = f'$ y el par $(\prod\{G_\alpha \mid \alpha \in \Lambda\}; \{p_\alpha \mid \alpha \in \Lambda\})$ verifica la definición de producto directo. □

Aunque para una familia $\{G_\alpha \mid \alpha \in \Lambda\}$ se ha definido el producto directo como un par, por abuso de lenguaje, se llama **grupo producto directo** ó simplemente **producto directo** al grupo $\prod\{G_\alpha \mid \alpha \in \Lambda\}$ y se representa abreviadamente por $\prod_\alpha G_\alpha$. Los homomorfismos p_α se llaman **proyecciones canónicas** del producto directo, y cada grupo G_α se llama **grupo factor**.

Lema. 21.3.
Sean $\{G_\alpha \mid \alpha \in \Lambda\}$ y $\{H_\alpha \mid \alpha \in \Lambda\}$ dos familias de grupos con el mismo conjunto de índices Λ, tales que para cada $\alpha \in \Lambda$ existe un homomorfismo de grupos $f_\alpha : H_\alpha \longrightarrow G_\alpha$, entonces existe un único homomorfismo de grupos $f : \prod_\alpha H_\alpha \longrightarrow \prod_\alpha G_\alpha$ verificando $f_\beta p_\beta = q_\beta f$ para cada $\beta \in \Lambda$, siendo p_β y q_β las proyecciones canónicas de los grupos productos $\prod_\alpha G_\alpha$ y $\prod_\alpha H_\alpha$ respectivamente. Además $\mathrm{Ker}(f) = \prod_\alpha \mathrm{Ker}(f_\alpha)$.

$$\begin{array}{ccc} \prod_\alpha G_\alpha & \overset{f}{\dashrightarrow} & \prod_\alpha H_\alpha \\ {\scriptstyle p_\beta}\downarrow & & \downarrow{\scriptstyle q_\beta} \\ G_\beta & \xrightarrow[f_\beta]{} & H_\beta \end{array}$$

DEMOSTRACIÓN. Basta aplicar la propiedad que define al producto directo de la familia $\{G_\alpha \mid \alpha \in \Lambda\}$ al par $(H_\alpha; \{f_\beta q_\beta : H_\alpha \longrightarrow G_\beta \mid \beta \in \Lambda\})$. □

El homomorfismo f del Lema 21.3. se representa por $\prod_\alpha f_\alpha$.

Corolario. 21.4.
Si $\{G_\alpha \mid \alpha \in \Lambda\}$ y $\{H_\alpha \mid \alpha \in \Lambda\}$ son dos familias de grupos, tales que para cada índice $\alpha \in \Lambda$ se tiene que H_α es un subgrupo (resp. subgrupo normal) de G_α, entonces $\prod_\alpha H_\alpha$ es un subgrupo (resp. subgrupo normal) de $\prod_\alpha G_\alpha$. Además en el caso en que sean normales se tiene un isomorfismo de grupos

$$\frac{\prod_\alpha G_\alpha}{\prod_\alpha H_\alpha} \cong \prod_\alpha \frac{G_\alpha}{H_\alpha}.$$

DEMOSTRACIÓN. Por el Lema (21.3.) la primera parte es inmediata. Para la segunda parte consideramos el homomorfismo de grupos $f_\alpha : G_\alpha \longrightarrow \frac{G_\alpha}{H_\alpha}$, donde f_α es la proyección canónica de G_α en el

grupo cociente G_α/H_α para cada $\alpha \in \Lambda$. El núcleo de $\prod_\alpha f_\alpha$ es:

$$\mathrm{Ker}(\prod_\alpha f_\alpha) = \prod_\alpha \mathrm{Ker}(f_\alpha) = \prod_\alpha H_\alpha.$$

y aplicando el Primer Teorema de Isomorfía, tenemos el resultado. □

22. Producto directo interno

Sea G un grupo y H, K subgrupos de G, entonces se puede definir una *aplicación* $f : H \times K \to G$ mediante $f(h,k) = hk$. Como se puede comprobar fácilmente esta aplicación no es necesariamente un homomorfismo de grupos. Una condición necesaria y suficiente para que f sea un homomorfismo de grupos es que los elementos de H conmuten con los de K, ver Proposición 20.3.. Podemos entonces establecer el siguiente resultado:

Proposición. 22.1.
Sea G y grupo y H, K subgrupos de G. Son equivalentes los siguientes enunciados:

(a) $f : H \times K \to G$ es un isomorfismo de grupos;
(b) H y K son subgrupos normales y verifican $HK = G$ y $H \cap K = 1$;
(c) Los elementos de H conmutan con los elementos de K, $H \vee K = G$ y $H \cap K = 1$;
(d) Los elementos de H conmutan con los elementos de K y para cada $g \in G$ existen $h \in H$ y $k \in K$, únicos verificando $g = hk$.

DEMOSTRACIÓN. (a) ⇒ (b). f es sobreyectiva, luego para cada $g \in G$ existen $h \in H$, $k \in K$ tales que $g = f(h,k) = hk$, entonces $G = HK$. Para $g \in H \cap K$ se verifica $g = f(g,1) = f(1,g)$; como f es inyectiva obtenemos $g = 1$. Además $H = \mathrm{Ker}(p_2 f^{-1}) \triangleleft G$ y $K = \mathrm{Ker}(p_1 f^{-1}) \triangleleft G$.
(b) ⇒ (c). Para cada $h \in H$, y para cada $k \in K$ se tiene $[h,k] = hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}) \in H \cap K = 1$ ya que $H, K \triangleleft G$.
(c) ⇒ (d). Cada $g \in G$ se puede escribir en la forma $g = h_1k_1 \cdots h_nk_n$. Como los elementos de H y K conmutan se tiene $g = (h_1 \cdots h_n)(k_1 \cdots k_n) = hk$.
Supongamos ahora dos expresiones $g = h_1k_1 = h_2k_2$. Entonces $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = 1$, luego $h_1 = h_2$ y $k_1 = k_2$.
(d) ⇒ (a). f es biyectiva porque cada $g \in G$ se expresa de manera única como un producto $g = hk$. Por otra parte,

$$f[(h_1,k_1)(h_2,k_2)] = f(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = f(h_1,k_1)f(h_2k_2),$$

y f es un homomorfismo. □

Si G, H y K verifican las condiciones equivalentes de la Proposición, entonces decimos que G es el **producto directo interno** de H y K.

Este resultado podemos extenderlo a un grupo G con una familia *finita* de subgrupos normales como sigue:

Proposición. 22.2.
Sea G un grupo y $N_1, \ldots, N_r$ subgrupos normales de G verificando $G = N_1 \ldots N_r$, y tal que para cada índice $i = 1, \ldots, r$, se tiene

$$N_i \cap (N_1 \ldots N_{i-1} N_{i+1} \ldots N_r) = \{1\},$$

entonces G es isomorfo al producto directo de la familia $\{N_i \mid i = 1, \ldots, r\}$.

DEMOSTRACIÓN. Dado $(n_i)_i \in N_1 \times \ldots \times N_r$, entonces $n_1 \ldots n_r \in G$. Definimos $f : N_1 \times \ldots \times N_r \longrightarrow G$ mediante $f((n_i)_i) = n_1 \ldots n_r$. Tenemos que f es un homomorfismo de grupos, ya que si $n_i \in N_i$ y $n_j \in N_j$, entonces $n_i n_j = n_j n_i$. Por ser $G = N_1 \ldots N_r$, entonces f es sobreyectiva. Supongamos que $f((n_i)_i) = e$, entonces $n_1 \ldots n_r = e$, luego $n_1^{-1} = n_2 \ldots n_r \in N_1 \cap (N_2 \ldots N_r) = \{e\}$, de donde $n_1 = e$ y $n_2 \ldots n_r = e$. Procediendo de la misma forma tenemos que $n_1 = n_2 = \ldots = n_r = e$, luego $(n_i)_i = e$ y $\mathrm{Ker}(f) = \{e\}$, y f es un homomorfismo inyectivo. □

En la situación anterior diremos que G es el **producto directo interno** de la familia $\{N_i \mid i = 1, \ldots, N_r\}$.

Aplicaciones

Proposición. 22.3.
Sean G y H grupos finitos con órdenes primos relativos, entonces se verifica:

(1) Para cada subgrupo L de $G \times H$ existen subgrupos $G' \leq G$ y $H' \leq H$ únicos verificando $L = G' \times H'$;
(2) $\mathrm{Aut}(G \times H) = \mathrm{Aut}(G) \times \mathrm{Aut}(H)$.

DEMOSTRACIÓN. (1). Definimos $G' = p_G(L)$ y $H' = p_H(L)$, entonces tenemos la siguiente inclusión $L \subseteq G' \times H'$. Sean ahora $g = \mid G \mid$ y $h = \mid H \mid$, existen $a, b \in \mathbb{Z}$ tales que $ag + bh = 1$; si tomamos $x \in G'$ resulta que existe $y \in H$ tal que $(x, y) \in L$, verificándose entonces

$$(x, y)^{bh} = (x^{bh}, y^{bh}) = (x^{1-ag}, 1) = (x, 1)$$

Luego $G' \times \{1\} \subseteq L$ y de forma análoga se tiene que $\{1\} \times H' \subseteq L$, luego $G' \times H' \in L$.

(2). Como consecuencia de (1) resulta que el único subgrupo de $G \times H$ de orden g es $G' = \mathrm{Im}(i_G)$, entonces para cada automorfismo φ de $G \times H$ resulta que $\varphi(H') = H'$, e igual ocurre para $H' = \mathrm{Im}(i_H)$. Luego φ define automorfismos de G y de H, por ejemplo

$$\begin{array}{ll} \varphi_G : G \longrightarrow G, & \varphi_G = p_G \varphi i_G; \\ \varphi_H : H \longrightarrow H, & \varphi_H = p_H \varphi i_H. \end{array}$$

Entonces $\varphi \longleftrightarrow (\varphi_G, \varphi_H)$ define un isomorfismo entre $\mathrm{Aut}(G \times H)$ y $\mathrm{Aut}(G) \times \mathrm{Aut}(H)$. □

En realidad la parte (2) de la anterior proposición es consecuencia del siguiente resultado más general.

Lema. 22.4.
Sea G un grupo y H, K subgrupos característicos de G verificando $H \cap K = 1$ y $HK = G$, entonces $\mathrm{Aut}(G) = \mathrm{Aut}(H) \times \mathrm{Aut}(K)$.

23. Ejercicios Propuestos

Ejercicio. 23.1.
Sea G el producto directo interno de dos subgrupos H y K. Demostrar que $G/H \cong K$ y $G/K \cong H$.
Ref.: 3305e_001 SOLUCIÓN

Ejercicio. 23.2.
.
(1) *Sea $N \lhd G = H \times K$ tal que $N \cap H = 1 = N \cap K$. Demostrar que N es abeliano.*
(2) *Dar un ejemplo de un grupo $H \times K$ que contiene un subgrupo normal no trivial N tal que $N \cap H = N \cap K = 1$. Concluir que para $N \lhd H \times K$ es posible que $N \neq (N \cap H) \times (N \cap K)$.*
(3) *Sean H, K dos grupos finitos con $(|H|, |K|) = 1$. Demostrar que para todo $N < H \times K$ se verifica que $N = (N \cap H) \times (N \cap K)$.*

Ref.: 3305e_002 SOLUCIÓN

Ejercicio. 23.3.
Sea $G = H \times K$ y sea $H < N < G$. Demostrar que existe un $K_1 < K$ tal que $N = H \times K_1$. (Pista: $K_1 = N \cap K$)
Ref.: 3305e_003 SOLUCIÓN

Ejercicio. 23.4.
Sean $\{H_i \mid i \in I\}$ y $\{G_i \mid i \in I\}$ dos familias de grupos y sea $\{f_i : H_i \to G_i \mid i \in I\}$ una familia de homomorfismos de grupos.
(1) *Demostrar que existe un único homomorfismo $\prod_i f_i : \prod_i H_i \to \prod_i G_i$ tal que para todo $j \in I$ se verifique $f_j p_j = p_j \prod_i f_i$ (en ambos miembros p_j denota la proyección canónica).*

3305-09.tex

(2) *Demostrar que* $\mathrm{Ker}(\prod_i f_i) = \prod_i \ker(f_i)$.
(3) *Para todo* $i \in I$ *sea* H_i *un subgrupo (normal) de* G_i. *Demostrar que* $\prod H_i$ *es un subgrupo (normal) de* $\prod_i G_i$. *En el caso normal demostrar que*

$$\frac{\prod_i G_i}{\prod_i H_i} \cong \prod_i \frac{G_i}{H_i}.$$

Ref.: 3305e_004 SOLUCIÓN

Ejercicio. 23.5.
Sea G *un grupo soluble finito que tiene una serie de composición en que los factores aparecen en orden arbitrario prescrito. Demostrar que* G *es el producto directo de sus subgrupos de Sylow.*
Ref.: 3305e_005 SOLUCIÓN

Ejercicio. 23.6.
Sea G *un grupo. Son equivalentes:*
(1) *Para todo* $H \lhd G$ *existe un* $K < G$ *tal que* $G = H \times K$.
(2) *Existe una familia* $\{H_i \mid i \in I\}$ *de subgrupos de* G *tales que* $G = \sum_i H_i$, *los* H_i *son todos simples y los* H_i *abelianos diferentes son no isomorfos.*

Ref.: 3305e_006 SOLUCIÓN

Ejercicio. 23.7.
Mostrar un subgrupo no normal de $Q_2 \times \mathbb{Z}_4$ *(nótese que todo subgrupo de cada factor es normal).*
Ref.: 3305e_007 SOLUCIÓN

Ejercicio. 23.8.
Demostrar que todos los subgrupos de $Q_2 \times \mathbb{Z}_2^n$ son normales.
Ref.: 3305e_008 SOLUCIÓN

Ejercicio. 23.9.
Demostrar que todo grupo abeliano finito es el producto directo de sus subgrupos de Sylow.
Ref.: 3305e_009 SOLUCIÓN

Ejercicio. 23.10.
Sea $G = HK$ donde H y K son subgrupos característicos de G y $H \cap K = 1$. Demostrar que $\mathrm{Aut}(G) = \mathrm{Aut}(H) \times \mathrm{Aut}(K)$. *Deducir que si G es un grupo abeliano de orden finito, entonces* $\mathrm{Aut}(G)$ *es isomorfo al producto directo de de los grupos de automorfismos de sus subgrupos de Sylow.*
Ref.: 3305e_010 SOLUCIÓN

Ejercicio. 23.11.
Sea K un subgrupo normal y cíclico de G. Demostrar que $G' \subset C_G(K)$
(Pista: El grupo de automorfismos de un grupo cíclico es abeliano).
Ref.: 3305e_011 SOLUCIÓN

Ejercicio. 23.12.
Sea H un subgrupo de un grupo G y sea $\varphi : G \to H$ un homomorfismo cuya restricción a H es la identidad. Sea $N = \mathrm{Ker}(\varphi)$.

(1) *Si G es abeliano, demostrar que $G \cong H \times N$.*
(2) *Para G arbitrario, encontrar una aplicación biyectiva $G \to H \times N$, y mostrar con un ejemplo que G no tiene que ser isomorfo a $H \times N$.*

Ref.: 3305e_012 SOLUCIÓN

Capítulo VII

Grupos de operadores. Teoremas de Sylow

24 Grupos de operadores 174
25 Teoremas de Sylow 187
26 Ejercicios propuestos 199

La teoría de grupos que hasta ahora hemos estudiado se conoce como *teoría de grupos abstractos*. En ella el punto de mayor interés es la operación de grupo y las propiedades que podemos deducir de esta operación; los elementos del grupo no tienen otra propiedad que la de ser elementos de un conjunto. Sin embargo la introducción de los grupos en la Matemática está muy lejos de la aproximación que hasta el momento hemos hecho. Históricamente la teoría de grupos trataba de grupos de transformaciones, y aún en algunas disciplinas, como la Geometría, este es el enfoque que se mantiene.

El tratar un grupo como un grupo de transformaciones tiene ventajas; sobretodo por que podemos derivar propiedades del grupo y de sus elementos a partir de los objetos sobre los que actúa. En el desarrollo que hemos hecho hasta el momento, el teorema de Lagrange se puede considerar un resultado de este enfoque. El objetivo que pretendemos ahora es estudiar con mayor detalle los grupos abstractos, viéndolos como grupos de transformaciones.

Para pasar de la teoría de grupos abstractos a grupos de transformaciones introducimos el concepto de grupo actuando sobre un conjunto.

24. Grupos de operadores

Sea G un grupo y X un conjunto, se dice que G **actúa a la izquierda** sobre X si existe una aplicación

$$\alpha : G \times X \longrightarrow X; \quad (g,x) \mapsto \alpha(g,x) = g \cdot x,$$

para todo $g \in G$ y $x \in X$, verificando las propiedades:

(I) $1 \cdot x = x$, para todo $x \in X$;
(II) $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$, para todo $g_1, g_2 \in G$, $x \in X$.

La aplicación α se llama **acción (a la izquierda)** de G sobre X. Se dice que G **actúa a la izquierda** sobre X. El conjunto X se llama un **G–conjunto a izquierda** y G se llama el **dominio de operadores** de la acción.

Lema. 24.1.
En la situación anterior son equivalentes los siguientes enunciados:

(a) Existe una acción a la izquierda α de G sobre X;
(b) Existe un homomorfismo de grupos $\phi : G \longrightarrow P(X)$, donde $P(X)$ es el grupo de todas las aplicaciones biyectivas de X en X (permutaciones de X).

Además en este caso α y ϕ están determinadas de forma unívoca, cada una por la otra, mediante la siguiente relación

$$\phi(g)(x) = \alpha(g,x) \text{ para } g \in G \text{ y } x \in X.$$

Ejemplo. 24.2.
Para un conjunto arbitrario X, $P(X)$ actúa de forma natural sobre X por acción dada mediante el homomorfismo identidad de $P(X)$. Si G es un subgrupo de $P(X)$, entonces de forma natural G actúa sobre X por la acción dada por la inclusión de G en $P(X)$.

Ejemplo. 24.3.
Si H es un subgrupo de G y G actúa sobre un conjunto X, entonces el homomorfismo $H \hookrightarrow G \xrightarrow{\phi} P(X)$ define una acción de H sobre X; llamamos a esta acción la **restricción de la acción** de G a H.

Ejemplo. 24.4. (Acción trivial)
La acción de G sobre X se llama **trivial** si $g \cdot x = x$ para todo $g \in G$ y todo $x \in X$.

Ejemplo. 24.5. (Acción por conjugación)
Si G es un grupo, una acción de G sobre el conjunto subyacente a G está dada por:

$$\alpha : G \times G \longrightarrow G; \quad \alpha(g,x) = gxg^{-1}, \text{ para todos } g, x \in G.$$

3308-01.tex

En este caso decimos que G **actúa sobre sí mismo por conjugación**. Si H es un subgrupo de G, también existe la consiguiente acción de H sobre el conjunto subyacente a G

$$\alpha : H \times G \longrightarrow G; \quad \alpha(h,g) = hgh^{-1}, \text{ para todos } h \in H, g \in G.$$

Ejemplo. 24.6. (Acción por traslaciones a la izquierda)
Si G es un grupo, otra acción de G sobre el conjunto subyacente a G está dada por:

$$\lambda : G \times G \longrightarrow G; \quad \lambda(g,x) = gx,$$

el producto en G para $g, x \in G$. Se dice que G **actúa sobre sí mismo por traslaciones a la izquierda**. Si H es un subgrupo de G, podemos considerar la acción de H sobre G por traslaciones a la izquierda.
También podemos establecer la acción de G en sí mismo por traslaciones a la derecha mediante la aplicación:

$$\rho : G \times G \longrightarrow G; \quad \rho(g,x) = xg^{-1},$$

el producto en G para $g, x \in G$.

Ejemplo. 24.7. (Acción por traslaciones a la izquierda)
Si G es un grupo y H un subgrupo de G, no necesariamente normal, sobre el conjunto de las clases a la izquierda G/H, definimos una acción de G sobre G/H mediante:

$$\lambda : G \times (G/H) \longrightarrow G/H; \quad \lambda(g, xH) = (gx)H,$$

para $g, x \in G$. Diremos que G **actúa por traslaciones a la izquierda** sobre G/H. Si consideramos ahora G/H como el conjunto de clases a la derecha de G sobre H, podemos definir una acción de G sobre G/H mediante:

$$\rho : G \times (G/H) \longrightarrow G/H; \quad \rho(g, Hx) = H(xg^{-1}), \text{ para } g, x \in G.$$

Ejemplo. 24.8. (Acción por conjugación)
Si G es un grupo y X es el conjunto de los subgrupos de G, definimos una acción de G sobre X mediante

$$\alpha : G \times X \longrightarrow X; \quad \alpha(g,H) = gHg^{-1}, \quad \text{para todos } g \in G \text{ y } H \in X.$$

Decimos que G **actúa por conjugación sobre los subgrupos** de G.

Para dar nombre a los conceptos anteriores, supongamos que tenemos una acción α de un grupo G sobre un conjunto X, que induce el homomorfismo

$$\phi : G \longrightarrow P(X),$$

entonces ϕ se dice que es una **representación por permutaciones** de G; llamamos **núcleo de la acción** al núcleo de ϕ; llamamos **grupo de transformaciones asociado a la acción** a la imagen de ϕ. El núcleo de la acción es:

$$\text{Ker}(\phi) = \{g \in G \mid \ g \cdot x = x, \text{ para todo } x \in X\};$$

esto es, el conjunto de los elementos de G que dejan fijo a cada elemento de X. La acción se dice que es **fiel** ó **acción efectiva** si su núcleo es $\{1\}$.

(•) En el Ejemplo 24.5., el núcleo de la acción es $Z(G)$, el **centro** de G; el conjunto de los elementos de G que conmutan con todos, y su grupo de trasformaciones es el grupo $\mathrm{Int}(G)$ de todos los **automorfismos interiores** de G.

(•) En el ejemplo 24.6., si G actúa sobre sí mismo a la izquierda, el núcleo es $\{1\}$, luego se trata de una acción fiel.

Lema. 24.9. (Teorema de Cayley)
Todo grupo G es isomorfo a un subgrupo en $P(G)$. En consecuencia todo grupo finito es un grupo de permutaciones.

(•) En el ejemplo 24.7., si consideramos las clases a la izquierda, el núcleo de la acción es el conjunto

$$\begin{aligned}\{a \in G \mid\ agH = gH,\ \forall g \in G\} &= \{a \in G \mid\ g^{-1}agH = H,\ \forall g \in G\}\\ &= \{a \in G \mid\ a \in gHg^{-1},\ \forall g \in G\}\\ &= \cap\{gHg^{-1} \mid\ g \in G\},\end{aligned}$$

que es el **mayor subgrupo normal de G contenido** en H. Lo representamos por H_G.

G–conjuntos

Sea G un grupo actuando sobre un conjunto X con acción α, decimos que (X, α), o simplemente X, si α se sobre-entiende, es un G-**conjunto**, con estructura dada por α.

En esta definición vez de α podemos utilizar el morfismo de grupos asociado $\phi : G \longrightarrow P(X)$.

Si (X_1, α_1) y (X_2, α_2) son dos G-conjuntos, una aplicación $\gamma : X_1 \longrightarrow X_2$ se llama un **homomorfismo de G-conjuntos** si hace conmutar el siguiente diagrama:

$$\begin{array}{ccc} G \times X_1 & \xrightarrow{\alpha_1} & X_1 \\ {\scriptstyle 1\times\gamma}\downarrow & & \downarrow{\scriptstyle \gamma} \\ G \times X_2 & \xrightarrow{\alpha_2} & X_2, \end{array}$$

ó equivalentemente, $\gamma(g \cdot x_1) = g \cdot \gamma(x_1)$, para todos $g \in G$, $x_1 \in X_1$.

Dos G-conjuntos (X_1, α_1) y (X_2, α_2) se llaman **equivalentes ó isomorfos**, si existe un homomorfismo de G-conjuntos $\gamma : X_1 \longrightarrow X_2$ que es una aplicación biyectiva.

Si (X_1, α_1) y (X_2, α_2) son G conjuntos, decimos que X_1 es un G**–subconjunto** de X_2 si $X_1 \subseteq X_2$ y la aplicación inclusión es un homomorfismo de G–conjuntos.

Acciones transitivas

Sea G un grupo actuando sobre un conjunto X; en X definimos la relación R_G mediante:

$$xR_Gy \text{ si existe } g \in G \text{ tal que } y = g{\cdot}x.$$

Lema. 24.10.
La relación R_G es una relación de equivalencia.

Cada clase de equivalencia para la relación R_G se llama una **órbita de la acción**. Para un elemento $x \in X$, la órbita de x se representa por $\mathrm{Orb}_G(x)$, $\mathrm{Orb}_G(x)$ ó $G{\cdot}x$, y es igual a

$$\mathrm{Orb}_G(x) = \{g{\cdot}x \in X \mid \ g \in G\}.$$

El conjunto de todas las orbitas se representa por X/G.

El grupo G **actúa transitivamente** sobre el conjunto X cuando X/G sólo tiene un elemento; esto es, cuando para cada par de elementos x, $y \in X$, existe $g \in G$ tal que $y = g{\cdot}x$ (Existe únicamente una órbita). También se dice que la acción de G sobre X es **transitiva**.

Una acción de un grupo G sobre un conjunto X es transitiva si, y sólo si, los únicos G-subconjuntos de X son X y el subconjunto vacío.

Ejemplos. 24.11.

(1) Supongamos que X es el conjunto de todos los puntos del espacio afín euclídeo real de dimensión 3, y que G es el grupo de las rotaciones con eje una recta dada r. Entonces para cada punto $x \in X$ su órbita es una circunferencia que pasa por x y está contenida en un plano perpendicular a la recta r.

(2) Sea X igual que en el ejemplo anterior, $\vec{v}$ un vector de $\mathbb{R}^3$ no nulo y G el grupo de las traslaciones definidas por los vectores $\lambda\vec{v}$, donde $\lambda \in \mathbb{R}$, entonces para cada punto $x \in X$ su órbita es una recta que pasa por x y cuyo vector de dirección es $\vec{v}$.

(3) Sea $X = E^3$ el espacio euclídeo tridimensional, G el grupo de las rotaciones alrededor de un punto fijo. La acción de G sobre E^3 es la natural. Las órbitas son las esferas con centro O y el estabilizador de un punto $Q \neq O$ es el subgrupo de las rotaciones de eje $\overline{OQ}$. El estabilizador de O es el mismo G.

(4) Consideramos $0, 1 \neq n \in \mathbb{N}$, $1 \neq \sigma \in S_n$, con descomposición en ciclos disjuntos dada por $\sigma = (x_{1_1}x_{1_2}\dots x_{1_{n_1}})\dots(x_{r_1}x_{r_2}\dots x_{r_{n_r}})$, entonces al actuar $G = \langle\sigma\rangle$ sobre $\{1, 2, \dots, n\}$, en la forma obvia, sus órbitas son $\{x_{1_1}x_{1_2}\dots x_{1_{n_1}}\}, \dots, \{x_{r_1}x_{r_2}\dots x_{r_{n_r}}\}$.

(5) Sea X un conjunto arbitrario no vacío, $n > 0$ un natural y sea $Y = X^n = X \times \cdots \times X$. Sea $G = S_n$ el grupo de permutaciones de n elementos. Definimos $G \times Y \to Y$ mediante:

$$\sigma \cdot (x_1, \dots, x_n) = (x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

Es inmediato comprobar que X es un G-conjunto.

Acciones primitivas

Otro concepto útil para el estudio de grupos de permutaciones es el de acción primitiva ó G-conjunto primitivo. Para ello necesitamos algunas definiciones.

Sea X un G-conjunto transitivo y R una relación de equivalencia en X; decimos que R es **compatible con la acción** ó que es una **congruencia**,

$$\text{si para cualesquiera } x, y \in X \text{ tales que } xRy \text{ y cualquier } g \in G \text{ se tiene } (g\cdot x)R(g\cdot y).$$

Si R es una relación compatible, el conjunto cociente $X/R = \{[x_\alpha] \mid \alpha \in \Lambda\}$ es una partición de X verificando que para cada $[x_\alpha] \in X/R$ y cada $g \in G$, existe $[x_\phi] \in X/R$ tal que $g\cdot[x_\alpha] = [x_\phi]$. Esto es, X/R admite una acción de G inducida por la acción sobre X.

Una partición $\{X_\alpha \mid \alpha \in A\}$ del conjunto X que cumple: para cada $\alpha \in A$ y cada $g \in G$ existe $\beta \in A$ tal que $g.X_\alpha = X_\beta$, se llama una **partición en bloques** de X, y es claro que para un G-conjunto X es equivalente dar una partición en bloques y dar una relación compatible con la acción.

Cada uno de los elementos B de una partición en bloques se llama un **bloque** ó **bloque de imprimitividad**, y verifica

$$g \cdot B = B \text{ ó } g \cdot B \cap B = \emptyset \text{ para cada } g \in G.$$

Por extensión un subconjunto B de X que cumple esta propiedad se llama un **bloque (de imprimitividad)** de X. Los bloques, X y $\{x\}$, para cada $x \in X$, se llaman **bloques impropios**, y forman las dos particiones en bloques impropios que existen de X.

Un G-conjunto X se llama **primitivo**, (ó bien la acción de G sobre X es **primitiva**,) si las únicas particiones en bloques que existen son las impropias, ó equivalentemente, las únicas relaciones de equivalencia compatibles son la total y la de igualdad.

Lema. 24.12.
Toda acción primitiva no trivial es transitiva.

DEMOSTRACIÓN. Tenemos que las órbitas forman una partición en bloques ya que para cada $x \in X$ y cada $g \in G$ se verifica:

$$g\cdot(G\cdot x) = G\cdot x.$$

Entonces si la acción es no trivial, resulta que $\mathrm{Orb}(x) = X$ para cada $x \in X$. □

Ejemplos. 24.13.

(1) Hacemos actuar al grupo D_4 sobre los cuatro vértices del cuadrado. Numeramos estos vértices sucesivamente 1, 2, 3, 4. Sea $r \in D_4$ la rotación de ángulo $\pi/2$ radianes, y sea s la reflexión en la línea diagonal que pasa por 1 y 3. Entonces las permutaciones de los vértices correspondientes son:

$$r \mapsto \rho = (1\ 2\ 3\ 4), \qquad s \mapsto \sigma = (2\ 4).$$

Ya que la representación por permutaciones es un homomorfismo, la permutación correspondiente a sr es $\sigma\rho = (1\ 4)(2\ 3)$. La acción de D_4 sobre los cuatro vértices del cuadrado es fiel ya que sólo la identidad fija todos los vértices. El estabilizador de cualquier vértice i es el subgrupo de orden 2 generado por la reflexión sobre la diagonal que pasa por i.

(2) Sea ahora $T = \{\{1,3\},\{2,4\}\}$ (conjunto cociente de $\{1,2,3,4\}$). La relación de equivalencia que define T es una congruencia y D_4 actúa sobre este conjunto:

(•) r intercambia los pares $\mathbf{1} = \{1,3\}$ y $\mathbf{2} = \{2,4\}$ y

(•) la reflexión s fija ambos pares.

Así que las permutaciones correspondientes son

$$r \mapsto (\mathbf{1}\ \mathbf{2}), \qquad s \mapsto (\mathbf{1}).$$

Esta acción no es fiel, su núcleo es $\langle r^2, s\rangle$. Para cada $\mathbf{i} \in T$ el estabilizador es el mismo núcleo.

(3) Consideramos ahora el conjunto $B = \{\{1,2\},\{3,4\}\}$. El grupo D_4 <u>no actúa</u> sobre B ya que $\{1,2\} \in B$ pero $r \cdot \{1,2\} = \{2,3\} \notin B$.

Estabilizadores

Sea G un grupo que actúa sobre un conjunto X, para cada elemento $x \in X$ consideramos el conjunto de los elementos de G que dejan fijo a x.

Lema. 24.14.
Para cada $x \in X$ el conjunto

$$\mathrm{Stab}_G(x) = \{g \in G \mid\ g \cdot x = x\} = G_x$$

*es un subgrupo de G, al que llamaremos **estabilizador** o **grupo de isotropía** de $x \in G$.*

DEMOSTRACIÓN. Ya que $1 \cdot x = x$ para todo $x \in X$, tenemos que $1 \in X$. Sean $g, f \in \mathrm{Stab}_G(x)$, entonces $g \cdot x = x = f \cdot x$, tenemos pues:

$$(gf^{-1}) \cdot x = g \cdot (f^{-1} \cdot x) = g \cdot (f^{-1} \cdot (f \cdot x)) = g \cdot ((f^{-1}f) \cdot x) = g \cdot (1 \cdot x) = g \cdot x = x,$$

luego $gf^{-1} \in \mathrm{Stab}_G(x)$. □

Corolario. 24.15.
Sea G un grupo actuando sobre un conjunto X mediante el homomorfismo de grupos ϕ, entonces

$$\mathrm{Ker}(\phi) = \cap\{\mathrm{Stab}_G(x) \mid\ x \in X\}.$$

DEMOSTRACIÓN. Tenemos $g \in \mathrm{Ker}(\phi)$ si, y sólo si, $\phi(g) = 1_X$ si, y sólo si, para todo $x \in X$ se tiene $g \cdot x = x$ si, y sólo si, $x \in \cap\{\mathrm{Stab}_G(x) \mid x \in X\}$. □

Lema. 24.16.
Sea G un grupo, si $x, y \in X$ están en la misma órbita, entonces $\mathrm{Stab}_G(x)$ y $\mathrm{Stab}_G(y)$ son subgrupos conjugados.

DEMOSTRACIÓN. Existe $g \in G$ tal que $y = g \cdot x$ y $x = g^{-1} \cdot y$. Dado $h \in \mathrm{Stab}_G(y)$ se verifica:

$$\begin{aligned} h \cdot y &= y \\ h \cdot (g \cdot x) &= g \cdot x \\ (g^{-1} h g) \cdot x &= x \end{aligned}$$

Entonces $g^{-1} h g \in \mathrm{Stab}_G(x)$. La otra inclusión es obvia. □

Ejemplos. 24.17.

(1) **Acción por traslaciones a la izquierda.** Supongamos que H es un subgrupo de un grupo G, y que H actúa por **traslaciones a la izquierda** sobre G. Para cada $g \in G$ su órbita es:

$$\mathrm{Orb}(g) = \{hg \in G \mid h \in H\} = Hg,$$

la clase a la derecha de H en G que contiene a g, y su estabilizador en H es:

$$\mathrm{Stab}_H(g) = \{h \in H \mid hg = g\} = \{1\}.$$

(2) En el Ejemplo 24.11..4 el estabilizador del elemento x_{1_1} es el subgrupo de G generado por σ^{n_1}.

(3) **Acción por conjugación.** Si consideramos la acción de un grupo G sobre sí mismo por **conjugación**, entonces para un elemento $x \in G$ tenemos que la órbita de x es:

$$\mathrm{Orb}_G(x) = \{gxg^{-1} \in G \mid g \in G\},$$

que se llama la **clase de conjugación** de x y se representa por $\mathrm{Cl}(x)$. El estabilizador de x es:

$$\mathrm{Stab}_G(x) = \{g \in G \mid gxg^{-1} = x\},$$

que se llama el **centralizador** de x en G, y se representa por $C_G(x)$; el núcleo de la acción resulta ser:

$$\cap\{\mathrm{Stab}_G(x) \mid x \in G\} = \{g \in G \mid gx = xg \ \forall x \in G\},$$

que es precisamente el **centro** de G, y se representa por $Z(G)$.

En S_n dos elementos son conjugados si y sólo si sus descomposiciones en ciclos disjuntos *son del mismo tipo*.

En $GL_n(\mathbb{F})$ dos matrices son conjugadas si y solo si *son semejantes*, esto es, representan el mismo isomorfismo respecto a dos bases.

Veamos una aplicación de la teoría. Recordemos que H_G es el mayor subgrupo normal de G contenido en H. El siguiente Lema nos dice cómo de cerca está H_G de H para cada subgrupo H de G.

Lema. 24.18.
Sea H un subgrupo de índice n de un grupo G, entonces G/H_G es isomorfo a un subgrupo de S_n.

DEMOSTRACIÓN. Ya que $[G:H]=n$, existe una biyección entre G/H y $\{1,2,\ldots,n\}$, y un isomorfismo de grupos entre $P(G/H)$ y S_n. El morfismo $\phi: G \longrightarrow P(G/H)$ asociado a la acción por traslaciones a la izquierda tiene núcleo igual a H_G, y por tanto, aplicando el primer teorema de isomorfía, se tiene el resultado. □

Corolario. 24.19.
Sea G un grupo finito y p el menor entero primo positivo que divide al orden de G; si H es un subgrupo de G de índice p, entonces H es un subgrupo normal de G.

DEMOSTRACIÓN. Llamamos G/H al conjunto de clases a la izquierda de H en G, entonces $P(G/H)$ es isomorfo a S_p. Tenemos por el Lema 24.18. que G/H_G, es isomorfo a un subgrupo de S_p, y por tanto $|\, G/H_G \,|$ divide a $|\, S_p \,| = p!$ Además $|\, G/H_G \,| = [G:H_G]$ divide a $|\, G \,|$, luego todo divisor de $|\, G/H_G \,|$ divide a $|\, G \,|$, y por tanto $|\, G/H_G \,|$ es p ó 1. Si $|\, G/H_G \,| = 1$, entonces $|\, G/H \,| = 1$, lo que es una contradicción; si $|\, G/H_G \,| = p$, entonces ya que $|\, G/H_G \,| = |\, G/H \,|\,|\, H/H_G \,|$ y $|\, G/H \,| = p$, tenemos que $|\, H/H_G \,| = 1$ y $H = H_G$ es un subgrupo normal. □

Reducción del estudio de acciones transitivas

Vamos a ver que cuando la acción es transitiva, entonces el G-conjunto en estudio es equivalente ó isomorfo a un G-conjunto formado por las clases a la izquierda de un subgrupo H en G.

Teorema. 24.20.
Sea G un grupo que actúa sobre un conjunto X, para cada $x \in X$ se tiene que $\mathrm{Orb}_G(x)$ y $G/\mathrm{Stab}_G(x)$ son G–conjuntos isomorfos, en donde la acción de G sobre $G/\mathrm{Stab}_G(x)$ es la acción por traslaciones a la izquierda.

En particular si G actúa transitivamente sobre X, y $x \in X$, $H = \mathrm{Stab}_G(x)$, entonces el G-conjunto X es isomorfo al G-conjunto G/H de las clases a la izquierda con acción dada por la traslación a la izquierda.

DEMOSTRACIÓN. Llamamos Y al conjunto de clases a la izquierda de $\mathrm{Stab}_G(x)$ en G, y definimos un aplicación

$$\phi : \mathrm{Orb}(x) \longrightarrow Y; \quad \phi(g\cdot x) = g\,\mathrm{Stab}_G(x).$$

(1). ϕ está bien definida. Sean $g_1, g_2 \in G$ tales que $g_1\cdot x = g_2\cdot x$, entonces

$$(g_1^{-1}g_2)\cdot x = g_1^{-1}\cdot(g_2\cdot x) = g_1^{-1}\cdot(g_1\cdot x) = (g_1^{-1}g_1)\cdot x = x,$$

luego $g_1^{-1}g_2 \in \mathrm{Stab}_G(x)$ y tenemos $g_1\,\mathrm{Stab}_G(x) = g_2\,\mathrm{Stab}_G(x)$.
(2). ϕ es una aplicación inyectiva. Si $g_1\,\mathrm{Stab}_G(x) = g_2\,\mathrm{Stab}_G(x)$, entonces $g_1^{-1}g_2 \in \mathrm{Stab}_G(x)$ y tenemos $(g_1^{-1}g_2)\cdot x = x$, luego $g_1^{-1}\cdot(g_2\cdot x) = x$, y por tanto $g_2\cdot x = g_1\cdot x$.
(3). ϕ es una aplicación sobreyectiva. Es claro por la definición.
Luego ambos conjuntos tienen el mismo cardinal.
En el segundo caso, por ser la acción transitiva, para cada $x \in X$ tenemos $X = \mathrm{Orb}(x) = \{g\cdot x \mid g \in G\}$. Al igual que antes, definimos $\phi : X \longrightarrow G/H$ mediante $\phi(g\cdot x) = gH$, para todo $g \in G$. Solo falta ver que ϕ es un homomorfismo de G–conjuntos.
(4). ϕ es un morfismo de G-conjuntos. Dados $g_1, g_2 \in G$ se verifica:

$$\phi(g_1\cdot(g_2\cdot x)) = \phi((g_1g_2)\cdot x) = (g_1g_2)H = g_1(g_2H) = g_1\cdot\cdot(g_2\cdot x).$$

Recordar que los elementos de X son todos de la forma gx, $g \in G$, $x \in X$ fijo. □

Corolario. 24.21.
Si G actúa sobre X y $x \in X$, entonces $|\,\mathrm{Orb}_G(x)\,| = [G : \mathrm{Stab}_G(x)]$.

Corolario. 24.22.
Si H es un subgrupo de un grupo G y $x \in G$, entonces el G-conjunto de las clases a la izquierda de H en G, con acción dada por traslación a la izquierda, es equivalente al G-conjunto de clases a la izquierda de xHx^{-1} en G con acción dada por traslación a la izquierda.

DEMOSTRACIÓN. Tenemos que G actúa transitivamente sobre G/H. Si $xH \in G/H$, entonces el estabilizador es xHx^{-1}

$$\begin{aligned}\mathrm{Stab}_G(xH) &= \{a \in G \mid axH = gH\}\\ &= \{a \in G \mid x^{-1}axH = H\}\\ &= \{a \in G \mid x^{-1}ax \in H\}\\ &= xHx^{-1},\end{aligned}$$

y G/H es isomorfo a G/xHx^{-1}. En particular tenemos

$$[G:H] = |\, X \,| = [G:gHg^{-1}].$$

□

Teorema. 24.23.
Si la acción de G sobre X es transitiva y no trivial, son equivalentes:
(a) La acción es primitiva;
(b) Para todo $x \in X$ el grupo $\mathrm{Stab}_G(x)$ es maximal.

DEMOSTRACIÓN. Dado $x \in X$, tenemos $X = \mathrm{Orb}(x)$ y $H = \mathrm{Stab}_G(X) \subsetneqq G$ es un subgrupo propio por ser la acción, respectivamente, transitiva y no trivial. Podemos suponer que X es el G–conjunto G/H con acción la traslación a la izquierda.
(a) $\Rightarrow$ (b). Supongamos un subgrupo $H \subsetneqq L \subsetneqq G$, entonces tenemos que G/L produce una descomposición propio en bloques de G/H, lo que es una contradicción.
(b) $\Rightarrow$ (a). Consideramos una descomposición propia en bloques de G/H, y sea B una bloque no trivial. Es claro que $\cup\{g.B \mid g \in G\}$ es una partición de G/H en bloques (si B es un bloque, también $g.B$ es un bloque). Tenemos que $\mathrm{Stab}_G(B) \subsetneqq G$, y podemos suponer que $1H \in B$, entonces $H \subseteq \mathrm{Stab}_G(B)$, pues para todo $h \in H$ se verifica $1H \in h.B \cap B$. Entonces de $H \subseteq \mathrm{Stab}_G(B) \subsetneqq G$, por la maximalidad de H, se deduce que $H = \mathrm{Stab}_G(B)$, pero entonces $B = \{1H\}$, lo que es una contradicción. □

Fórmula de clases

Supongamos que un grupo G actúa sobre sí mismo por conjugación, entonces como consecuencia del Corolario 24.21. tenemos:

Corolario. 24.24.
Si G es un grupo finito se verifica:

$$|\, \mathrm{Cl}(x) \,| = [G : C_G(x)].$$

DEMOSTRACIÓN. Para la acción por conjugación tenemos $\mathrm{Cl}(x) = \mathrm{Orb}_G(x)$, y $\mathrm{Stab}_G(x) = C_G(x)$ es el centralizador de x en G. □

Vamos ahora a contar los elementos de un grupo finito usando las clases de conjugación.

Proposición. 24.25. (Fórmula de clases)
Si G es un grupo finito, se verifican:
(1) $\mid G \mid = \sum\{\mid \mathrm{Cl}(x)\mid \mid \ x \in \Delta\}$,
(2) $\mid G \mid = \mid Z(G) \mid + \sum\{\mid \mathrm{Cl}(x)\mid \mid \ x \in C,\ x \notin Z(G)\}$.

Donde C es un conjunto de representantes de clases de conjugación.

DEMOSTRACIÓN. (1). Tenemos que G es la unión disjunta de las clases de conjugación de sus elementos, ya que la relación de conjugación es de equivalencia, entonces la suma de los cardinales de todas las clases es el orden de G, para dar una buena expresión de $\mid G \mid$ basta tomar un representante de cada clase y escribir

$$\mid G \mid = \sum\{\mid \mathrm{Cl}(x) \mid \ x \in C\}.$$

(2). Tenemos $\mid \mathrm{Cl}(x) \mid = 1$ si, y sólo si, $[G : C_G(x)] = 1$ si, y sólo si $G = C_G(x)$ si, y sólo si, $x \in Z(G)$; entonces tenemos

$$\begin{aligned} \mid G \mid &= \sum\{\mid \mathrm{Cl}(x) \mid\mid \ x \in C,\ x \in Z(G)\} + \sum\{\mid \mathrm{Cl}(x) \mid\mid \ x \in C,\ x \notin Z(G)\} \\ &= \mid Z(G) \mid + \Sigma\{\mid \mathrm{Cl}(x) \mid \ x \in C,\ x \notin Z(G)\}. \end{aligned}$$

□

Observación. 24.26. (Generalización de la fórmula de clases)
Sea H un subgrupo normal de G. Hacemos actuar G sobre H por conjugación. El estabilizador de un elemento $h \in H$ es:

$$\mathrm{Stab}_G(h) = \{x \in G \mid \ xhx^{-1} = h\} = C_G(h).$$

La fórmula de descomposición en órbitas nos proporciona la siguiente igualdad:

$$\begin{aligned} \mid H \mid &= \sum\{\mid \mathrm{Orb}(h) \mid \ h \in C\} \\ &= \sum\{[G : \mathrm{Stab}_G(h)] \mid \ h \in C\} \\ &= \sum\{[G : C_G(h)] \mid \ h \in C\}. \end{aligned}$$

siendo C un conjunto de representantes de clases de conjugación. Para que una órbita tenga sólo un elemento ha de ser $C_G(h) = G$, o equivalentemente $h \in Z(G) \cap H$. Obtenemos entonces la fórmula:

$$\mid H \mid = \mid Z(G) \cap H \mid + \sum\{[G : C_G(h)] \mid \ h \in C,\ x \notin Z(G) \cap H\}.$$

Ejemplo. 24.27.
Consideramos un grupo G, llamamos $L(G)$ al conjunto de todos los subgrupos de G, y hacemos actuar G sobre $L(G)$ por conjugación. Si tomamos $H \in L(G)$, la *órbita* de H es:

$$\mathrm{Orb}(H) = \{gHg^{-1} \mid \ g \in G\},$$

la llamamos *clase de conjugación* de H y la representamos por $\mathrm{Cl}(H)$. El *estabilizador* de H es:

$$\mathrm{Stab}_G(H) = \{g \in G \mid \ gHg^{-1} = H\},$$

lo llamamos el *normalizador* de H en G, y lo representamos por $N_G(H)$, es el *mayor subgrupo de G en el que H es un subgrupo normal*.

Corolario. 24.28.
Para cada grupo finito G y cada subgrupo H de G se verifica:

$$|\ \mathrm{Cl}(H)\ | = [G : N_G(H)].$$

Teorema de Polya–Burnside

Consideramos un grupo finito G actuando sobre un conjunto finito X. Para cada $g \in G$ sea $c(g) = |\ \{x \in X \mid \ g{\cdot}x = x\}\ |$, y sea R la relación de equivalencia en X definida por la acción (xRy si existe $g \in G$ tal que $y = gx$).

Teorema. 24.29. (Polya–Burnside)
$|\ G\ ||\ X/G\ | = \sum_{g\in G} c(g)$.

DEMOSTRACIÓN. Consideramos una tabla rectangular en la que las filas están indizadas por los elementos de X y las columnas por los de G. Dados $x \in X$ y $g \in G$ colocamos un uno en la posición (x, g) si $g{\cdot}x = x$, y la dejamos vacía en caso contrario. El número total de unos es $\sum_{g\in G} c(g)$.
Otra forma de contar los unos es la siguiente: tomamos la clase $[x]$ de un elemento x en X/R. Para cada $y \in [x]$, sea $y = g{\cdot}x$, en la fila de y tenemos $|\ \mathrm{Stab}_G(y)\ |$ unos, pero se verifica $|\ \mathrm{Stab}_G(y)\ | = |\ \mathrm{Stab}_G(x)\ |$ ya que $g\ \mathrm{Stab}_G(y)g^{-1} = \mathrm{Stab}_G(x)$. Además el número de elementos en $[x]$ es: $|\ \mathrm{Orb}(x)\ | = [G : \mathrm{Stab}_G(x)]$. Luego el número de unos que aparecen en las filas de $[x]$ es: $[G : \mathrm{Stab}_G(x)]\ |\ \mathrm{Stab}_G(x)\ | = |\ G\ |$. Entonces el número total de unos que tenemos es: $|\ G\ ||\ X/R\ |$. □

Corolario. 24.30.
Sea G un grupo finito, entonces el número de clases de conjugación de G es:

$$\sum_{g\in G} \frac{1}{[G : C_G(g)]}.$$

DEMOSTRACIÓN. Hacemos actuar G sobre sí mismo por conjugación, se verifica que $\{x \in G \mid g \cdot x = x\} = \{x \in G \mid gx = xg\} = C_G(g)$. Aplicamos ahora el teorema de Polya–Burnside. Si llamamos t al número de clases de conjugación obtenemos:

$$|G| t = \sum_{g \in G} |C_G(g)|$$

Y desarrollando se tiene:

$$t = \sum_{g \in G} \frac{|G|}{|C_G(g)|} = \sum_{g \in G} \frac{1}{[G : C_G(g)]}.$$

□

Polya enunció su teorema para determinar el número de isómeros de un compuesto químico. Una ilustración sencilla sería la siguiente:

Ejemplo. 24.31.
Vamos a determinar el número de maneras distintas de colocar cuatro bolas blancas y otras cuatro negras en los vértices de un cubo.

En este caso el conjunto X es el número total de elecciones de cuatro vértices (las bolas blancas) del conjunto de los ocho vértices del cubo, así que $|S| = \binom{8}{4} = 70$.

El grupo G es el grupo de rotaciones del cubo. Este grupo es isomorfo a S_4, así que $|G| = 24$. Los elementos del grupo G son:

- La identidad, para la cual $c(g) = |S| = 70$.
- Ocho rotaciones de ángulo $2\pi/3$ alrededor de las diagonales del cubo. Cada una de ellas descompone el conjunto de vértices en cuatro órbitas, dos de cardinal uno y dos de cardinal tres. Como los elementos de cada órbita deben ser del mismo color para que s sea fijo bajo está rotaciones, obtenemos que $c(g) = 4$ para cada una de ellas.
- Seis rotaciones de ángulo $2\pi/4$ alrededor de los ejes que unen los puntos medios de las caras. Para cada una de ellas $c(g) = 2$.
- Tres rotaciones de ángulo π alrededor de los mismos ejes del apartado anterior. Para estas rotaciones $c(g) = \binom{4}{2} = 6$
- Seis rotaciones de ángulo π alrededor de los ejes que unen los puntos medios de aristas opuestas. También para estas rotaciones se verifica que $c(g) = \binom{4}{2} = 6$

Sumándolo todo obtenemos

$$\sum_{g \in G} c(g) = 70 + 8 \cdot 4 + 6 \cdot 2 + 3 \cdot 6 + 6 \cdot 6 = 168$$

Aplicando el teorema de Polya existen $|S/G| = 168/24 = 7$ órbitas (que son las configuraciones no equivalentes).

25. Teoremas de Sylow

p–subgrupos

Sea p un número entero positivo primo, un grupo finito G es un **p-grupo** si $|\ G\ |$ es una potencia de p, entonces, por el teorema de Lagrange, cada elemento de G tiene por orden una potencia de p. El recíproco también es cierto como veremos a continuación en un corolario al teorema de Cauchy.

Un subgrupo finito H de un grupo G se llama un **p-subgrupo** de G si es un p-grupo.

Teorema. 25.1. (Teorema de Cauchy)
Si p es un número entero positivo primo que divide al orden de un grupo finito G, entonces existe, al menos, un subgrupo de G de orden p.

DEMOSTRACIÓN. Si G es un grupo abeliano, por el teorema de estructura de grupos abelianos finitos tenemos que G es un producto de grupos cíclicos, siendo el orden de G el producto de los ordenes de sus grupos factores, luego p ha de dividir al orden de un subgrupo cíclico de G, y por tanto G contiene un subgrupo de orden p.

Para el caso general vamos a hacer la demostración por inducción sobre el orden de G. Supongamos que todo grupo de orden menor que $|\ G\ |$, cuyo orden sea múltiplo de p, contiene un subgrupo de orden p. Si G contiene un subgrupo propio cuyo orden es un múltiplo de p, entonces, aplicando la hipótesis, G contiene un subgrupo de orden p. En caso contrario, ningún subgrupo propio de G tiene orden múltiplo de p; sea H un subgrupo propio de G, entonces $p \nmid |\ H\ |$, y por tanto de $|\ G\ | = [G : H]\ |\ H\ |$ deducimos que p divide a $[G : H]$. Consideremos la fórmula de clases (para la acción por conjugación)

$$\begin{aligned} |\ G\ | &= |\ Z(G)\ | + \sum\{|\ \mathrm{Cl}(x)\ |\ \ x \in C,\ x \notin Z(G)\} \\ &= |\ Z(G)\ | + \sum\{[G : C_G(x)]\ |\ \ x \in C,\ x \notin Z(G)\}. \end{aligned}$$

Ya que $C_G(x)$, $x \in C$, $x \notin Z(G)$, es un subgrupo propio; p divide a $|\ G\ |$ y a cada $[G : C_G(x)]$ en la suma, luego necesariamente p divide a $|\ Z(G)\ |$. Entonces $Z(G)$ no es un subgrupo propio de G, y tenemos $G = Z(G)$. Esto es, G es un grupo abeliano finito, y por tanto, aplicando la primera parte de la demostración, contiene un elemento de orden p, entonces $Z(G) \cong \mathbb{Z}_p$ y tenemos el resultado. □

3308-02.tex

Corolario. 25.2.
Sea G un grupo finito. Son equivalentes las siguientes condiciones
(a) G es un p-grupo;
(b) cada elemento tiene por orden una potencia de p.

DEMOSTRACIÓN. Supongamos que cada elemento de G tiene por orden una potencia de p, y sea q un entero positivo primo que divide a $|\, G \,|$. Por el teorema de Cauchy existe un elemento de G cuyo orden es q, y por tanto $q = p^r$, $r \in \mathbb{N}$. Luego ha de ser $r = 1$ y $q = p$. □

Teorema. 25.3. (Teorema de Burnside)
Si G es un p-grupo finito no trivial, entonces $Z(G)$ es un subgrupo no trivial y $|\, Z(G) \,| \geq p$.

DEMOSTRACIÓN. Si $G = Z(G)$, entonces el resultado es cierto. Supongamos que $G \neq Z(G)$, entonces aplicando la fórmula de clases (para la acción por conjugación), tenemos:

$$|\, G \,| = |\, Z(G) \,| + \sum \{|\, \mathrm{Cl}(x) \,| \;\; x \in C,\, x \notin Z(G)\}.$$

Tenemos $|\, \mathrm{Cl}(x) \,| > 1$ si $x \in C \setminus Z(G)$, y ya que $|\, \mathrm{Cl}(x) \,| = [G : C_G(x)]$, entonces $|\, \mathrm{Cl}(x) \,|$ divide a $|\, G \,| = p^n$. Luego p divide a $|\, G \,|$ y a cada miembro de la suma, y por tanto necesariamente divide a $|\, Z(G) \,|$. Como $1 \in Z(G)$, tenemos que $|\, Z(G) \,| \geq p$, y es no trivial. □

Lema. 25.4.
Si $G/Z(G)$ es un grupo cíclico, entonces G es un grupo abeliano.

DEMOSTRACIÓN. Supongamos que $gZ(G)$ es un generador del grupo cíclico $G/Z(G)$, entonces para cada dos elementos $x, y \in G$ existen $r, s \in \mathbb{N}$ con $xZ(G) = g^r Z(G)$ e $yZ(G) = g^s Z(G)$, y existen $x', y' \in Z(G)$ tales que $x = g^r x'$ e $y = g^s y'$. Tenemos entonces:

$$xy = (g^r x')(g^s y') = g^r g^s x' y' = g^s g^r y' x' = (g^s y')(g^r x') = yx.$$

□

Corolario. 25.5.
Todo grupo G de orden p^2 es abeliano.

DEMOSTRACIÓN. Si G no es abeliano, entonces $G \neq Z(G)$, y por el teorema de Burnside $| Z(G) | \geq p$, luego necesariamente $| Z(G) | = p$. Así $G/Z(G)$ es un grupo de orden p, por tanto cíclico. Por el Lema 25.4. ha de ser G un grupo abeliano, lo que es una contradicción. □

Primer teorema de Sylow.

Si G es un grupo que actúa sobre un conjunto X, llamamos $\mathrm{Fix}_X(G)$ al conjunto de los puntos fijos de X, esto es:

$$\begin{aligned}\mathrm{Fix}_X(G) &= \{x \in X \mid \ gx = x \text{ para todo } g \in G\} \\ &= \{x \in X \mid \ \mathrm{Stab}_G(x) = G\}.\end{aligned}$$

Si K es un subgrupo de G, entonces podemos definir una acción de K sobre X mediante $(k, x) \mapsto k \cdot x$, así el homomorfismo de grupos asociado es la restricción a K del homomorfismo de la acción. Como consecuencia si la acción de G es fiel, también la restricción a K es fiel.
Para cada $x \in X$ tenemos

$$\mathrm{Stab}_K(x) = \{k \in K \mid \ kx = x\} = \mathrm{Stab}_G(x) \cap K,$$

y para en elemento $x \in X$ tenemos

$$x \in \mathrm{Fix}_X(K) \text{ si, y sólo si, } K \subseteq \mathrm{Stab}_G(x).$$

Ejemplo. 25.6.
Supongamos que H y K son subgrupos de G y que G actúa por traslaciones a la izquierda sobre el conjunto G/H de clases a la izquierda de H en G. La restricción de la acción a K verifica para cada $g \in G$:

$$\mathrm{Stab}_K(gH) = gHg^{-1} \cap K$$

$$gH \in \mathrm{Fix}_X(K) \text{ si y sólo si } K \subseteq gHg^{-1}.$$

Lema. 25.7.
Si G es un p-grupo finito que actúa sobre un conjunto finito X, entonces se verifica:

$$| \mathrm{Fix}_X(G) | \equiv | X | \pmod{p}.$$

DEMOSTRACIÓN. Supongamos que las órbitas de la acción son $X_1,\dots,X_r$, entonces

$$|X| = \sum\{|X_i| \mid 1 \le i \le r\},$$

si $|X_j| > 1$ con $X_j = \mathrm{Orb}(x_j)$, tenemos $|X_j| = [G : \mathrm{Stab}_G(x_j)]$, luego es un múltiplo de p.
Si $|\mathrm{Fix}_X(G)| = s$, entonces existen exactamente s órbitas, por ejemplo $X_1,\dots,X_s$, con un sólo elemento; tenemos

$$|X| = s + \sum\{|X_i| \mid s < j \le r\},$$

entonces $|\mathrm{Fix}_X(G)| \equiv |X| \pmod p$. □

Lema. 25.8.
Si H es un p-subgrupo de un grupo finito G tal que p divide a $[G : H]$, entonces p divide a $[N_G(H) : H]$.

DEMOSTRACIÓN. Consideramos el conjunto $X = G/H$ de las clases a la izquierda de H en G, y la acción de H sobre G/H por traslación a la izquierda, entonces $|\mathrm{Fix}_X(H)| \equiv |G/H| = [G : H] \pmod p$.
Para cada $g \in G$ se verifica:

$$\begin{array}{ll} gH \in \mathrm{Fix}_X(H) & \text{si y sólo si} \\ H \le \mathrm{Stab}_H(gH) & \text{si y sólo si} \\ H \le gHg^{-1} & \text{si y sólo si (por ser } G \text{ finito} \\ H = gHg^{-1} & \text{si y sólo si} \\ g \in N_G(H) & \text{si y sólo si} \\ gH \in N_G(H)/H. & \end{array}$$

Como consecuencia $|\mathrm{Fix}_X(H)| = |N_G(H)/H|$, y tenemos el resultado. □

Corolario. 25.9.
Si G es un p-grupo finito, entonces todo subgrupo propio H de G es un subgrupo propio de $N_G(H)$.

Teorema. 25.10. (Primer teorema de Sylow)
Sea G un grupo de orden $p^n m$, tal que $n \in \mathbb{N}$, $n \ge 1$, p entero primo positivo y $p \nmid m$. Entonces

(1) G contiene un subgrupo de orden p^k para cada $1 \le k \le n$, y
(2) todo subgrupo de G de orden p^{k-1} es normal en algún subgrupo de orden p^k.

DEMOSTRACIÓN. Ya que p divide a $|\ G\ |$, existe, por el teorema de Cauchy, un subgrupo de G de orden p. Supongamos que H es un subgrupo de G de orden p^{k-1}, con $1 \leq k \leq n$, entonces p divide a $[G:H]$, y por el lema 25.8., p divide a $|\ N_G(H)/H\ |$. Entonces, por el teorema de Cauchy, existe un subgrupo K/H de $N_G(H)/H$ de orden p, siendo K un subgrupo de G contenido en $N_G(H)$. El orden de K es entonces

$$|\ K\ | = [K:H]\,|\ H\ | = p \cdot p^{k-1} = p^k.$$

Luego K es un p-subgrupo de G. Ya que H es normal en $N_G(H)$ y $H \subseteq K \subseteq N_G(H)$, tenemos que H es normal en K.

Procediendo de esta forma llegamos a encontrar un subgrupo de G de orden p^k para cada $1 \leq k \leq n$. □

Si p es un entero positivo primo y G un grupo finito, un **p-subgrupo de Sylow** de G es un p-subgrupo maximal (entre los p–subgrupos) de G.

Corolario. 25.11.
Sea G un grupo de orden $p^n m$ en las condiciones anteriores, entonces se verifica:

(1) Existe un p–subgrupo de Sylow de G.
(2) Si P un subgrupo de G, entonces P es un p-subgrupo de Sylow de G si, y sólo si, $|\ P\ | = p^n$.
(3) Todo subgrupo conjugado de un p-subgrupo de Sylow de G es un p-subgrupo de Sylow de G.
(4) Si existe un único p-subgrupo de Sylow de G, entonces este es un subgrupo normal de G.
(5) Todo p-subgrupo de G está contenido en un p-subgrupo de Sylow de G.

Segundo teorema de Sylow

Teorema. 25.12. (Segundo teorema de Sylow)
Sea G un grupo de orden $p^n m$ en las condiciones anteriores. Si P es un p-subgrupo de Sylow de G y K es un p-subgrupo de G, entonces existe $g \in G$ tal que $K \leq gPg^{-1}$.
En particular cada dos p-subgrupos de Sylow de G son conjugados.

DEMOSTRACIÓN. Llamamos $X = G/P$ al conjunto de clases a la izquierda de P en G. El cardinal de X es: $|\ X\ | = [G:P] = |\ G\ |\ /\ |\ P\ | = m$.

Si hacemos actuar K por traslación a la izquierda sobre X, se verifica:

$$|\ \mathrm{Fix}_X(K)\ | \equiv |\ X\ | \equiv m \pmod{p}.$$

Ya que p no divide a m tenemos que $|\operatorname{Fix}_X(K)| \neq 0$, y por tanto $\operatorname{Fix}_X(K) \neq \varnothing$. Sea $gP \in \operatorname{Fix}_X(K)$. Por el ejemplo 25.6. esto ocurre si, y sólo si, $K \subseteq gPg^{-1}$.
En el caso particular en que K es un p-subgrupo de Sylow de G tenemos $|K| = |P| = |gPg^{-1}|$; entonces $K = gPg^{-1}$ y P y K son subgrupos conjugados. □

Aplicaciones del segundo teorema de Sylow

Corolario. 25.13.
Sea G un grupo finito y P un p-subgrupo de Sylow de G, entonces

$$N_G(N_G(P)) = N_G(P).$$

DEMOSTRACIÓN. Siempre se tienen las inclusiones $P \subseteq N_G(P) \subseteq N_G(N_G(P))$. Si consideramos $x \in N_G(N_G(P))$, entonces $xPx^{-1} \subseteq xN_G(P)x^{-1} \subseteq N_G(P)$. Como P y xPx^{-1} son p-subgrupos de Sylow de $N_G(P)$, son conjugados en $N_G(P)$; pero como P es normal en $N_G(P)$, se tiene $P = xPx^{-1}$ y $x \in N_G(P)$. □

Proposición. 25.14. (Lema de Frattini)
Sea G un grupo finito, N un subgrupo normal de G y P un p-subgrupo Sylow de N con normalizador $N_G(P)$, entonces $NN_G(P) = G$.

DEMOSTRACIÓN. Para cada $g \in G$ tenemos $gPg^{-1} \subseteq N$. Tenemos que P y gPg^{-1} son p-subgrupos de Sylow de N. Por el segundo teorema de Sylow son subgrupos conjugados en N, luego existe $n \in N$ tal que $nPn^{-1} = gPg^{-1}$. Como consecuencia $P = n^{-1}gPg^{-1}n$, y por tanto $n^{-1}g = h \in N_G(P)$, entonces $g = nh \in NN_G(P)$. □

Tercer teorema de Sylow

Teorema. 25.15. (Tercer teorema de Sylow.)
Sea G un grupo de orden $p^n m$ en las condiciones anteriores. Si n_p es el número de p-subgrupos de Sylow de G, entonces:
(1) $n_p = [G : N_G(P)]$ donde P es cualquier p-subgrupo de Sylow de G;
(2) n_p divide a m y
(3) $n_p \equiv 1$ (mód p).

DEMOSTRACIÓN. Llamamos $X = \mathrm{Syl}_p(G)$ al conjunto de todos los p-subgrupos de Sylow de G.
(1). Hacemos actuar G por conjugación sobre X. Com esta acción es transitiva, si $P \in X$, entonces el número de elementos de X es igual al número de conjugados, distintos, de P, entonces

$$n_p = |\ \mathrm{Syl}_p(G)\ | = [G : \mathrm{Stab}_G(P)] = [G : N_G(P)].$$

(2). Tenemos

$$m = [G : P] = [G : N_G(P)][N_G(P) : P] = n_p[N_G(P) : P],$$

luego n_p divide a m.
(3). Consideramos la acción por conjugación de P sobre X. Se verifica $|\ \mathrm{Fix}_X(P)\ | \equiv |\ X\ |\ \pmod p$. Para $Q \in X$ tenemos $Q \in \mathrm{Fix}_X(P)$ si, y sólo si, $P \subseteq \mathrm{Stab}_P(Q) \subseteq \mathrm{Stab}_G(Q) = N_G(Q)$. Entonces que P y Q están contenidos en $N_G(Q)$; ambos son p-subgrupos de Sylow de G, y por tanto también de $N_G(Q)$, y por tanto son conjugados en $N_G(Q)$; además Q es normal en $N_G(Q)$, entonces $P = Q$ y se verifica que $\mathrm{Fix}_X(P) = \{P\}$, entonces $n_p = |\ X\ | \equiv |\ \mathrm{Fix}_X(P)\ | = 1\ \pmod p$. □

Aplicaciones

Proposición. 25.16.
Sea G un grupo y P un p–subgrupo de Sylow de G. Son equivalentes los siguientes enunciados:
(a) P es el único p–subgrupo de Sylow;
(b) P es un subgrupo normal de G;
(c) P es un subgrupo característico de G.

Proposición. 25.17.
Si G es un p–grupo de orden p^n, entonces
(1) Todo subgrupo maximal de G es de orden p^{n-1};
(2) Todo subgrupo maximal de G es un subgrupo normal.

Corolario. 25.18.
Todo p–grupo es un grupo soluble.

Los siguientes tres resultados son útiles consecuencias de los teoremas de Sylow.

(1) Si p no divide al orden de G, el único p-subgrupo de Sylow de G es el grupo trivial (y todas las partes del segundo y tercer teorema de Sylow son triviales).
(2) Si $|G| = p^k$, entonces el mismo G es su único p-subgrupo de Sylow.
(3) Un grupo abeliano finito tiene un único p-subgrupo de Sylow para cada primo p. Este subgrupo está formado por todos los elementos cuyo orden es una potencia de p y se llama la **componente p–primaria** del grupo abeliano.

REVISAR

En el primer caso el estabilizador de $x \in G$, $G_x = \{g \in G \mid gxg^{-1} = x\}$ es el **centralizador** de x en G mientras que la órbita $Gs = \{xsx^{-1} \mid x \in G\}$ es la *clase conjugada* de s en G.

En el segundo caso el estabilizador de $x \in G$, $G_x = \{g \in G \mid gx = x\} = 1$ se reduce al subgrupo trivial, mientras que la órbita $Gx = \{gx \mid g \in G\}$ es el grupo total. Igual ocurre en la traslación por la derecha.

En S_n dos elementos son conjugados si y sólo si al descomponerlo en ciclos disjuntos tienen el mismo tipo. En $GL_n(F)$ dos matrices son conjugadas si y sólo si son semejantes.

El homomorfismo $\phi : G \to P(G)$ obtenido para la traslación por la izquierda se llama **representación regular por la izquierda** de G y es inyectivo. Nos identifica G con un subgrupo de $P(G)$ y permite enunciar el conocido:

Teorema. 25.19. (Cayley)
Todo grupo finito es isomorfo a un grupo de permutaciones.

Ejemplo. 25.20.
Las tres operaciones del Ejemplo (**??**) pueden generalizarse al conjunto $X = \mathscr{P}(G)$ (*Booleano* de G o conjunto de las partes de G):

(1) Sea $T \subset G$; $g * T = gTg^{-1}$.
El estabilizador es el normalizador de T en G: $N_G(T) = \{g \in G \mid gTg^{-1} = T\}$.
La órbita es la **clase conjugada** de T en G: $G * T = \{gTg^{-1} \mid g \in G\}$.

(2) Sea $T \subset G$; $x * T = xT = \{xt \mid t \in T\}$. Es particularmente interesante el caso en que T es un subgrupo de G.
Entonces el estabilizador de T es $\{g \in G \mid gT = T\} = T$ y la órbita es $G * T = \{gT \mid g \in G\} = G/T$, el conjunto de clases por la izquierda de T en G. A un conjunto de representantes de estas órbitas (es decir, un conjunto con un y sólo un elemento de cada órbita) le llamamos **transversal** de T en G. Un análisis análogo podemos hacer en el tercer caso. El caso que acabamos de ver es especialmente típico, como veremos a continuación.

Fórmula de clases

Teorema. 25.21.
Sea X un G-conjunto, $x \in X$ con estabilizador $H = G_x$ y órbita $T = Gx$.

(1) T es un G-subconjunto de X.
(2) Existe un isomorfismo de G-conjuntos $f : T \cong G/H$

3308-05.tex

Corolario. 25.22.
Llamamos $|Gx|$ al cardinal de la órbita Gx. Entonces

$$|Gx| = [G : G_x]$$

Corolario. 25.23.
El número de conjugados de x en G es igual a

$$|G|/|N_G(x)| = [G : N_G(x)].$$

Teorema. 25.24.
Supongamos que la acción de G sobre X es transitiva y no trivial. La acción es primitiva si y sólo si para todo $x \in X$ el grupo G_x es maximal en G.

Llamemos ahora $|X|$ al cardinal del conjunto X. Sea Δ un conjunto de representantes de las órbitas. Obtenemos:

Teorema. 25.25. (Fórmula de descomposición en órbitas)

$$|S| = \sum_{x \in \Delta} [G : G_x].$$

Aplicando el anterior corolario al primero de los ejemplos **??**, las órbitas con un sólo elemento serán los $x \in G$ tales que $gxg^{-1} = x$ para todo $g \in G$, lo cual se verifica si y sólo si $x \in Z(G)$. Separando estas órbitas tenemos:

Corolario. 25.26. (Fórmula de clases)

$$|G| = |Z(G)| + \sum_{s \in \Delta'} [G : C_G(s)].$$

donde la suma se toma sobre el conjunto Δ' de representantes de clases que tienen mas de un elemento.

La fórmula de clases admite una generalización bastante útil: Sea $H \triangleleft G$. Hacemos actuar a G sobre H por conjugación: $g * h = ghg^{-1}$. El estabilizador de un elemento $h \in H$ es $G_h = \{g \in G \mid ghg^{-1} = 0\} = C_G(h)$. La fórmula de descomposición en órbitas nos da:

$$|H| = \sum_{h \in \Delta} [G : C_G(h)]$$

donde Δ es un conjunto de representantes de órbitas. Una órbita tendrá un sólo elemento cuando $G = C_G(h)$ o sea cuando $h \in Z = Z(G)$. Así que el conjunto de órbitas con un elemento corresponden a los elementos de $H \cap Z$. Obtenemos

$$|H| = |H \cap Z| + \sum_{h \in \Delta'} [G : C_G(h)]$$

donde Δ' es un conjunto de representantes de órbitas con mas de un elemento. En particular si H es finito, $[G : C_G(h)]$ es finito para todo $h \in H$, aunque G no lo sea.

El teorema de Polya-Burnside

Vamos a obtener un resultado muy útil en la matemática combinatoria: Sea G un grupo y S un G-conjunto, ambos finitos. Para cada $x \in G$ llamamos $c(x)$ al cardinal del conjunto $\{s \in S \mid xs = s\}$ y llamamos S/G al conjunto cociente de S por la relación $s \sim t \Leftrightarrow \exists x \in G$ tal que $s = xt$. Entonces

Teorema. 25.27. (Polya-Burnside)

$$|G| \cdot |S/G| = \sum_{x \in G} c(x)$$

DEMOSTRACIÓN. Consideramos el conjunto $X = \{(x,s) \in G \times S \mid x * s = s\}$. Calculamos su cardinal de dos maneras:
Sumando primero en $g \in G$ obtenemos

$$|X| = \sum_{x \in G} |\{s \in S \mid x * s = s\}| = \sum_{x \in G} c(x).$$

Al sumar primero en $s \in S$ obtenemos

$$|X| = \sum_{s \in S} |\{x \in G \mid x * s = s\}| = \sum_{s \in S} |\operatorname{Stab}_G(s)|.$$

Pero los estabilizadores de elementos de la misma órbita son conjugados, por tanto isomorfos y tienen el mismo orden. Además, el orden de la órbita de todo $s \in S$ es $[G : \operatorname{Stab}(s)]$. Agrupamos en la última suma los elementos de la misma órbita y obtenemos:

$$|X| = \sum_{\bar{s} \in S/G} \sum_{t \in \bar{s}} |\operatorname{Stab}(s)| = \sum_{\bar{s} \in S/G} [G : \operatorname{Stab}(s)] \cdot |\operatorname{Stab}(s)|$$

$$= \sum_{\bar{s} \in S/G} |G| = |S/G| \cdot |G|$$

□

Corolario. 25.28.
El número de clases conjugadas en un grupo finito G es

$$\sum_{x \in G} \frac{1}{[G : C_G(x)]}$$

DEMOSTRACIÓN. Aplicar el teorema 25.27. al primero de los ejemplos **??**. Entonces $c(x) = |\{g \in G \mid gx = xg\}| = |C_G(x)|$. Así que el número de clases de conjugación es

$$|S/G| = \frac{1}{|G|} \sum_{x \in G} |C_G(x)| = \sum_{x \in G} \frac{|C_G(x)|}{|G|} = \sum_{x \in G} \frac{1}{[G : C_G(x)]}$$

□

Polya enunció su teorema para determinar el número de isómeros de un compuesto químico. Una ilustración sencilla sería la siguiente:

Ejemplo. 25.29.
Vamos a determinar el número de maneras distintas de colocar cuatro bolas blancas y otras cuatro negras en los vértices de un cubo.

En este caso el conjunto S es el número total de elecciones de cuatro vértices (las bolas blancas) del conjunto de los ocho vértices del cubo, así que $|S| = \binom{8}{4} = 70$.

El grupo G es el grupo de rotaciones del cubo. Este grupo es isomorfo a S_4, así que $|G| = 24$. Los elementos del grupo G son:

- La identidad, para la cual $c(g) = |S| = 70$.
- Ocho rotaciones de ángulo $2\pi/3$ alrededor de las diagonales del cubo. Cada una de ellas descompone el conjunto de vértices en cuatro órbitas, dos de cardinal uno y dos de cardinal tres. Como los elementos de cada órbita deben ser del mismo color para que s sea fijo bajo está rotaciones, obtenemos que $c(g) = 4$ para cada una de ellas.
- Seis rotaciones de ángulo $2\pi/4$ alrededor de los ejes que unen los puntos medios de las caras. Para cada una de ellas $c(g) = 2$.
- Tres rotaciones de ángulo π alrededor de los mismos ejes del apartado anterior. Para estas rotaciones $c(g) = \binom{4}{2} = 6$
- Seis rotaciones de ángulo π alrededor de los ejes que unen los puntos medios de aristas opuestas. También para estas rotaciones se verifica que $c(g) = \binom{4}{2} = 6$

Sumándolo todo obtenemos

$$\sum_{g \in G} c(g) = 70 + 8 \cdot 4 + 6 \cdot 2 + 3 \cdot 6 + 6 \cdot 6 = 168$$

Aplicando el teorema de Polya existen $|S/G| = 168/24 = 7$ órbitas (que son las configuraciones no equivalentes).

26. Ejercicios propuestos

Ejercicio. 26.1.
Sea G un grupo que actúa sobre un conjunto X, demostrar que es posible definir una acción $*$de G sobre X a la derecha mediante

$$X \times G \to X : (x, g) \mapsto x * g = g^{-1}x,$$

para todo $x \in X$ y $g \in G$.
Ref.: 3308e_001 SOLUCIÓN

Ejercicio. 26.2.
Si G es un grupo que actúa sobre un conjunto X con acción α, demostrar que G tambiénactúa sobre el conjunto $\mathscr{P}(X)$, de las partes de X, con la acción definida por:

$$G \times \mathscr{P}(X) \to \mathscr{P}(X); \quad (g, Y) \mapsto g{\cdot}Y,$$

para $g \in G$ e $Y \in P(X)$, siendo $g{\cdot}Y = \{g{\cdot}y \in X : \ y \in Y\}$. Aplicarlo al caso en queG actúa sobre sí mismo por conjugación y tomamos en vez de $\mathscr{P}(X)$ el conjunto desubgrupos de G.
Ref.: 3308e_002 SOLUCIÓN

Ejercicio. 26.3.
Sea G el grupo S_4, y $X = \{1,2,3,4\}$. Consideramos la acción natural de S_4 sobreX, y los subgrupos de S_4 siguientes:
(1) $H_1 = \langle(123)\rangle$;
(2) $H_2 = \langle(1234)\rangle$;
(3) $H_3 = \{1,(12)(34),(13)(24),(14)(23)\}$;
(4) $H_4 = \{1,(12),(12)(34),(34)\}$;
(5) $H_5 = A_4$.

Describir las órbitas y estabilizadores cuando actúan por restricción sobre X.
Ref.: 3308e_003 SOLUCIÓN

3308-09.tex

Ejercicio. 26.4.
Sea G el grupo S_5 y $X = \{1,2,3,4,5\}$. Consideramos la acción natural de S_5 sobre X, ylos subgrupos de S_5 siguientes:
(1) $H = \langle(124)\rangle$;
(2) $H = A_4$;
(3) $H = \langle(12)(34)\rangle$;
(4) $H = S_3$

Describir las órbitas y estabilizadores cuando actúan por restricción sobre X.
Ref.: 3308e_004 SOLUCIÓN

Ejercicio. 26.5.
Si un grupo G contiene un elemento a con exactamente dos conjugados. Demostrar que entoncesG contiene un subgrupo normal propio no trivial.
Ref.: 3308e_005 SOLUCIÓN

Ejercicio. 26.6.
Sea G un grupo, demostrar:
(1) Si $N \subseteq Z(G)$, entonces N es un subgrupo normal de G.
(2) Si $N \subseteq Z(G)$ y G/N es un grupo cíclico, entonces G es un grupo abeliano.

Ref.: 3308e_006 SOLUCIÓN

Ejercicio. 26.7.
Sea G un grupo que actúa transitivamente sobre un conjunto X que contiene al menos a 2elementos. Demostrar que:
(1) Si la acción es fiel, el núcleo es trivial, entonces para un subgrupo normal N de G tal que $N \subseteq \mathrm{Stab}_G(x)$ para algún $x \in X$, se tiene $N = \{1\}$.
(2) Para cada $x \in X$ se tiene $\mathscr{C}ard(\mathrm{Orb}(x)) = [G : \mathrm{Stab}_G(x)]$, luego $\mathscr{C}ard(\mathrm{Orb}(x))$ divide a$|\ G\ |$ si éste es finito.

Ref.: 3308e_007 SOLUCIÓN

Ejercicio. 26.8.
Sea G un grupo no abeliano, si $|\operatorname{Int}(G)| = 4$, *demostrar que G tiene exactamente tressubgrupos abelianos de índice 2.*
Ref.: 3308e_008 SOLUCIÓN

Ejercicio. 26.9.
Sea H un subgrupo de un grupo G. Demostrar que:
(1) $C_G(H)$ es un subgrupo normal de $N_G(H)$.
(2) $N_G(H)/C_G(H)$ es isomorfo a un subgrupo de $\operatorname{Aut}(H)$.

Ref.: 3308e_009 SOLUCIÓN

Ejercicio. 26.10.
Sea G un grupo que contiene un elemento g de orden distinto de 1 y 2. Demostrar que $\operatorname{Aut}(G) \neq \{1\}$.
Ref.: 3308e_010 SOLUCIÓN

Ejercicio. 26.11.
Sea G un grupo y N un subgrupo normal abeliano, demostrar que G/N actúa sobre N por conjugación y dar un morfismo de G/N en $\operatorname{Aut}(N)$.
Ref.: 3308e_011 SOLUCIÓN

Ejercicio. 26.12.
Sea G un grupo que actúa transitivamente sobre un conjunto X, y sea H un subgrupo normal de G. Sean $\mathcal{O}_1, \ldots, \mathcal{O}_k$ las órbitas distintas en la acción de H sobre X.

(1) Demostrar que G actúa transitivamente sobre el conjunto $\{\mathcal{O}_1, \ldots, \mathcal{O}_k\}$;
(2) Demostrar que todos los $\mathcal{O}_i$ tienen el mismo cardinal;
(3) Sea $x \in \mathcal{O}_1$ un elemento arbitrario. Demostrar que $|\mathcal{O}_1| = [G : H \cap \mathrm{Stab}_G(x)]$ y deducir que $k = [G : H \cdot \mathrm{Stab}_G(x)]$.

Ref.: 3308e_012 SOLUCIÓN

Ejercicio. 26.13.
Sea G un grupo finito de orden compuesto n con la propiedad de que G tiene un subgrupo de orden d para cada entero positivo d que divida a n. Demostrar que G tiene un subgrupo normal propio.
Ref.: 3308e_013 SOLUCIÓN

Ejercicio. 26.14.
Sean S y T dos G–conjuntos. Definimos una acción de G sobre el producto cartesiano $S \times T$ mediante:

$$g \cdot (s,t) = (g \cdot s, g \cdot t).$$

Demostrar que para esta acción el estabilizador de (s,t) es la intersección de los estabilizadores de s y t en las acciones dadas.
Ref.: 3308e_014 SOLUCIÓN

Ejercicio. 26.15.
Sea G un grupo y H, K subgrupos de G de índices r y s respectivamente. Demostrar que $[G : H \cap K] \leq rs$. [Teorema de Poincaré]
Ref.: 3308e_015 SOLUCIÓN

Ejercicio. 26.16.
Sea G un grupo y H, K subgrupos de G conjugados de índice r. Demostrar que $[G : H \cap K] \leq r(r-1)$. (Pista. hallar una acción transitiva de G sobre un conjunto der elementos y considerar la acción de G sobre pares ordenados.)
Ref.: 3308e_016 SOLUCIÓN

Ejercicio. 26.17.
Sea G un grupo finito que actúa transitivamente sobre un conjunto X con más de un elemento.Demostrar que existe un $g \in G$ que mueve todos los puntos de X. (El enunciado equivale a quepara $H \lneqq G$ se tiene $\cup_{g\in G} gHg^{-1} \lneqq G$.)
Ref.: 3308e_017 SOLUCIÓN

Ejercicio. 26.18.
Sea $n > 0$ un número entero positivo. Una partición de n es una sucesión $i_1 \leq \cdots \leq i_k$de números enteros positivos tales que $i_1 + \cdots + i_k = n$. Dada una permutación $\sigma \in S_n$,la descomposición de σ en ciclos disjuntos (incluyendo los de longitud uno)$\sigma = \gamma_1 \cdots \gamma_k$ determina una partición $i_1, \ldots, i_k$ de n, donde cada $i_j$es la longitud del ciclo γ_j. Dos permutaciones en S_n se dicen del ***mismotipo*** *si determinan la misma partición de n. Demostrar que:*

(1) Dos elementos de S_n son conjugados si y sólo si son del mismo tipo;
(2) El número de clases de conjugación de S_n es igual al número de particiones de n.

Ref.: 3308e_018 SOLUCIÓN

Ejercicio. 26.19.
Calcular el número de clases de conjugación de S_5. Dar un representante de cada una y encontrarel orden de cada clase. Calcular el estabilizador de (123) *para la acción por conjugación deS_5 sobre sí mismo.*
Ref.: 3308e_019 SOLUCIÓN

Ejercicio. 26.20.
Un subgrupo G de S_n se llama ***transitivo*** *si la acción de$G$ sobre el conjunto $\{1,\dots,n\}$ es transitiva. Determinar los subgrupos transitivos deS_n, para $n \leq 5$.*
Ref.: 3308e_020 *SOLUCIÓN*

Ejercicio. 26.21.
Sea G un grupo finito y x e y elementos de G conjugados. Demostrar que $\mid C_G(x) \mid$es el número de elementos $g \in G$ que verifican $gxg^{-1} = y$.
Ref.: 3308e_021 *SOLUCIÓN*

Ejercicio. 26.22.
Encontrar todos los grupos finitos que tienen exactamente dos clases de conjugación.
Ref.: 3308e_022 *SOLUCIÓN*

Ejercicio. 26.23.
Sea G un grupo que contiene un subgrupo $H \neq G$ con $[G : H]$ finito, demostrar que existe unsubgrupo normal propio K de G con $[G : K]$ finito.
Ref.: 3308e_023 *SOLUCIÓN*

Ejercicio. 26.24.
Sea X un G-conjunto finito transitivo y $B \subseteq X$ un bloque para la acción, demostrarque se verifica:
(1) Para todo $g \in G$, $g \cdot B$ es también un bloque.
(2) Si $B \neq \emptyset$, entonces $\mathscr{C}ard(B)$ divide a $\mathscr{C}ard(X)$.

Ref.: 3308e_024 *SOLUCIÓN*

Ejercicio. 26.25.
Sea X un G-conjunto finito y transitivo, y $x \in X$, llamamos $H = \mathrm{Stab}_G(x)$. Demostrar quese verifica:

(1) Para cada subgrupo K de G tal que $H \subseteq K$, $K{\cdot}x$ es un bloque.
(2) Cada bloque que contiene a x es de la forma $K{\cdot}x$ con $H \leq K \leq G$, con K un subgrupo de G.
(3) Si $\mathscr{C}ard(X) > 1$, demostrar que la acción es primitiva si, y sólo si, H es un subgrupo propiomaximal de G.

Ref.: 3308e_025 SOLUCIÓN

Ejercicio. 26.26.
Sea X un G-conjunto transitivo con $\mathscr{C}ard(X) = p$ un número entero primo positivo, demostrarque X es primitivo.
Ref.: 3308e_026 SOLUCIÓN

Ejercicio. 26.27.
Sea X un G-conjunto finito transitivo, N un subgrupo normal de G y β el morfismo dela acción. Si la acción es primitiva, demostrar que $N \subseteq \mathrm{Ker}(\beta)$ ó la acción de Nsobre X (por restricción) es transitiva.
Ref.: 3308e_027 SOLUCIÓN

Ejercicio. 26.28.
Demostrar que si la acción de G sobre X es primitiva y fiel, entonces la acción inducida sobre$X$ por cualquier subgrupo normal no trivial N de G es transitiva.
Ref.: 3308e_028 SOLUCIÓN

Ejercicio. 26.29.
Sea G un grupo finito y $\phi : G \to S(G)$ la representación regular por la izquierda de$G$.

(1) Demostrar que si $g \in G$ tiene orden n y $\mid G \mid = nm$, entonces $\phi(g)$ es un producto de$m$ ciclos de longitud n.
(2) Deducir que $\phi(g)$ es una permutación impar si y sólo si g es par y el orden del cociente$m = \mid G/\langle x \rangle \mid$ es impar.
(3) Demostrar que si $\phi(G)$ tiene una permutación impar, entonces G tiene un subgrupo de índice2.

Ref.: 3308e_029 SOLUCIÓN

Ejercicio. 26.30.
*Una acción de un grupo G sobre un conjunto X se llama k–**mente transitiva**, para $k \in \mathbb{N}^*$, si para cualesquiera elementos $s_1, \ldots, s_k$ y $t_1, \ldots, t_k$ de X tales que $s_i \neq s_j$ y $t_i \neq t_j$ si $i \neq j$, existe un $g \in G$ tal que $g \cdot s_i = t_i$, $i = 1, \ldots, k$. Demostrar que toda acción doblemente transitiva es primitiva.*
Ref.: 3308e_030 SOLUCIÓN

Ejercicio. 26.31.
Sea G un grupo finito que actúa fiel y transitivamente sobre un conjunto X, y sea $H = \mathrm{Stab}_G(x)$ el estabilizador de un elemento $x \in X$. Demostrar que se verifica:

(1) La acción de G sobre X es doblemente transitiva si y sólo si H actúa transitivamente sobre el complemento de x en X;
(2) La acción de G sobre X es doblemente transitiva si y sólo si $G = HTH$, donde T es un subgrupo de G de orden 2 no contenido en H;
(3) Si la acción de G es doblemente transitiva y $[G : H] = n$, entonces $\mid G \mid = d(n-1)n$, donde d es el orden del subgrupo que fija dos elementos. Además H es un subgrupo maximal de G, es decir, la acción es primitiva.

Ref.: 3308e_031 SOLUCIÓN

Teorema de Polya–Burnside

Ejercicio. 26.32.
Sea G un grupo actuando transitivamente sobre un conjunto X. Demostrar que se verifica:
(1) $\sum_{g\in G} c(g) = \mid G \mid$;
(2) G es doblemente transitivo si, y sólo si, $\sum_{g\in G} c(g)^2 = 2 \mid G \mid$.

Ref.: 3308e_032 SOLUCIÓN

Ejercicio. 26.33.
Determinar el número de maneras distintas en que se pueden pintar los borden de una tarjeta cuadrada si se dispone de seis colores de pintura y no se puede utilizar un mismo color para dos bordes diferentes.
Ref.: 3308e_033 SOLUCIÓN

Ejercicio. 26.34.
Cuatro esferas están fijas en las esquinas de un cuadrado. Se quiere pintar cada una bien de color rojo, blanco o azul. ¿De cuántas maneras puede hacerse?
Ref.: 3308e_034 SOLUCIÓN

Teoremas de Sylow

En lo que sigue p es un número entero positivo primo.

Ejercicio. 26.35.
Demostrar que todo grupo no abeliano de orden p^3 tiene centro de orden p.
Ref.: 3308e_035 SOLUCIÓN

Ejercicio. 26.36.
Demostrar que existen únicamente dos grupos de orden p^2 no isomorfos.
Ref.: 3308e_036 SOLUCIÓN

Ejercicio. 26.37.
Sea G un grupo finito de orden pn, siendo $p > n$, demostrar que G contiene un subgrupo normal de orden p, y que cada subgrupo de G de orden p es normal en G.
Ref.: 3308e_037 SOLUCIÓN

Ejercicio. 26.38.
Sea G un grupo finito y N un subgrupo normal de G, demostrar que si N y G/N son p-grupos, entonces G es un p-grupo.
Ref.: 3308e_038 SOLUCIÓN

Ejercicio. 26.39.
Sean G un grupo finito, P un p–subgrupo de Sylow de G y H un p–subgrupo de $N_G(P)$. Demostrar que $H \subseteq P$.
Ref.: 3308e_039 SOLUCIÓN

Ejercicio. 26.40.
Sea G un grupo finito, N un subgrupo normal de G y P un p-subgrupo de Sylow de G. Demostrar que si $|N| \not\equiv 1 \pmod{p}$, entonces $H \cap C_G(P) \neq \{1\}$.
Como consecuencia, si G además es un p-grupo y $N \neq 1$, entonces $N \cap Z(G) \neq \{1\}$.
Ref.: 3308e_040 SOLUCIÓN

Ejercicio. 26.41.
Sea G un grupo de orden p^n y N un subgrupo normal de G de orden p, demostrar que N está contenido en el centro de G.
Ref.: 3308e_041 SOLUCIÓN

Ejercicio. 26.42.
Sea G un grupo infinito en el que cada elemento tiene orden una potencia de p. Demostrar que para cada $n \in \mathbb{N}^*$ existe un subgrupo de G de orden p^n ó existe $m \in \mathbb{N}^*$ tal que cada subgrupo finito tiene orden menor ó igual que p^m.
Ref.: 3308e_042 SOLUCIÓN

Ejercicio. 26.43.
Sea G un grupo finito y N un subgrupo normal de orden p^n, demostrar que N está contenido en todo p-subgrupo de Sylow de G.
Ref.: 3308e_043 SOLUCIÓN

Ejercicio. 26.44.
Hallar los p-subgrupos de Sylow de S_3, S_4, A_4, S_5 y A_5 para $p = 2$, 3 y 5.
Ref.: 3308e_044 SOLUCIÓN

Ejercicio. 26.45.
Demostrar que todo p-subgrupo de Sylow de S_{2p} es abeliano de orden p^2. Hallar los generadores para cada uno de ellos.
Ref.: 3308e_045 SOLUCIÓN

Ejercicio. 26.46.
Demostrar que el subgrupo de $SL(2,\mathbb{Z}_3)$ *generado por* $\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ *y* $\begin{pmatrix}1&1\\1&-1\end{pmatrix}$ *es el único2–subgrupo de Sylow de* $SL(2,\mathbb{Z}_3)$.
Ref.: 3308e_046 SOLUCIÓN

Ejercicio. 26.47.
Para cualquier cuerpo F *una matriz* $(a_{ij}) \in GL(n,F)$ *se llama* ***triangular superior estricta*** *si* $a_{ij} = 0$ *siempre que* $i > j$ *y* $a_{ii} = 1$ *para todo índice* i.

(1) *Comprobar que las matrices triangulares superiores estrictas forman un subgrupo* P *de* $GL(n,F)$.
(2) *Sea* $F = \mathbb{Z}_p$. *Demostrar que* P *es un* p*–subgrupo de Sylow del grupo* $GL(n,\mathbb{Z}_p)$.
(3) *Demostrar que el número de* p*–subgrupos de Sylow de* $GL(2,\mathbb{Z}_p)$ *es* $p+1$ *(Pista. Encontrar dos* p*–subgrupos de Sylow distintos.)*

Ref.: 3308e_047 SOLUCIÓN

Ejercicio. 26.48.
Para cada entero primo positivo que divida al orden del grupo hallar todos los p*–subgrupos de Sylow de* G *en cada uno de los siguientes casos:* $\mathbb{Z}_{600}$, D_5, D_6, $SL(2,\mathbb{Z}_3)$ *y* $SL(3,\mathbb{Z}_2)$.
Ref.: 3308e_048 SOLUCIÓN

Ejercicio. 26.49.
.

(1) *Sea* p *un entero primo positivo impar que divide a* n. *Demostrar que* D_n *tiene un único* p*–subgrupo de Sylow que es normal y cíclico.*
(2) *Sea* $n = 2^k m$, m *impar. Demostrar que el número de 2–subgrupos de Sylow de* D_n *es* m *(Pista. Utilizar que si* P *es un 2–subgrupo de Sylow de* D_n, *entonces* $N_{D_n}(P) = P$.*)*

Ref.: 3308e_049 SOLUCIÓN

Ejercicio. 26.50.
Un subgrupo H de un grupo G se llama ***totalmente invariante*** *si para todo endomorfismo $f : G \to G$ se tiene $f(H) \subseteq H$.*
Demostrar que si P es un p-subgrupo de Sylow de un grupo finito G, entonces P es un subgrupo totalmente invariante de G si y sólo si P es el único p–subgrupo de Sylow de G.
Ref.: 3308e_050 SOLUCIÓN

Ejercicio. 26.51.
Sea G un p-grupo no trivial de orden p^n. Demostrar que para cada $1 \leq k \leq n$, existe un subgrupo normal de G, N_k, de orden p^k.
Ref.: 3308e_051 SOLUCIÓN

Ejercicio. 26.52.
Sea G un grupo finito, N un subgrupo normal de G y P un p-subgrupo de Sylow de G. Demostrar que $P \cap N$ es un p-subgrupo de Sylow de N y que PN/N es un p-subgrupo de Sylow de G/N.
Ref.: 3308e_052 SOLUCIÓN

Ejercicio. 26.53.
Demostrar que todo grupo de orden 12, 28, 56, 148, 200, 312 y 351 contiene un subgrupo de Sylow normal y por tanto no pueden ser grupos simples.
Ref.: 3308e_053 SOLUCIÓN

Ejercicio. 26.54.
¿Cuantos elementos de orden 5 tiene un grupo simple de orden 60?
Ref.: 3308e_054 SOLUCIÓN

Ejercicio. 26.55.
¿Cuántos elementos de orden 7 tiene un grupo simple de orden 168?
Ref.: 3308e_055 SOLUCIÓN

Ejercicio. 26.56.
Sea G un grupo finito, si para todo número entero primo positivo p, que divida al orden de G, todo p-subgrupo de Sylow de G es un subgrupo normal, demostrar que G es el producto directo de sus subgrupos de Sylow.
Ref.: 3308e_056 SOLUCIÓN

Ejercicio. 26.57.
Demostrar que $Z(S_n) = \{1\}$ para $n \geq 3$. Demostrar que todo automorfismo de S_4 es un automorfismo interno, y por tanto $S_4 \cong \mathrm{Aut}(S_4) = \mathrm{Int}(S_4)$.
Ref.: 3308e_057 SOLUCIÓN

Ejercicio. 26.58.
Sea p un número entero primo positivo y G un grupo de orden $p+1$ que tiene un automorfismo de orden p. Demostrar que G es un grupo abeliano y que existe un número entero primo positivo q tal que $x^q = 1$ para todo $x \in G$.
Ref.: 3308e_058 SOLUCIÓN

Ejercicio. 26.59.
Si un grupo finito G actúa transitivamente sobre un conjunto X con más de un elemento, demostrar que existe algún $g \in G$ que mueve todos los elementos de X.
Ref.: 3308e_059 SOLUCIÓN

Ejercicio. 26.60.
Sea G un grupo finito y H, K subgrupos de G no triviales verificando $|H|+|K|=|G|$, demostrar que $G=HK$.
Ref.: 3308e_060 SOLUCIÓN

Ejercicio. 26.61.
Si G es un grupo de orden $2n$, con n un número entero positivo impar, demostrar que G contiene un subgrupo de índice 2.
Ref.: 3308e_061 SOLUCIÓN

Ejercicio. 26.62.
Demostrar que si un grupo finito G contiene un subgrupo H de índice n, entonces H contiene un subgrupo normal de G de índice un divisor de $n!$
Ref.: 3308e_062 SOLUCIÓN

Ejercicio. 26.63.
Sea S un p-subgrupo de un grupo finito G que no es un p-subgrupo de Sylow, demostrar que S es un subgrupo propio de $N_G(S)$.
Ref.: 3308e_063 SOLUCIÓN

Ejercicio. 26.64.
Sea G un grupo finito y N el normalizador en G de un p-subgrupo de Sylow de G. Si S y T son subgrupos de G tales que $N \subseteq S \subseteq T \subseteq G$, demostrar que:
(1) $N_G(S)=S$.
(2) $[T:S] \equiv 1 \pmod{p}$.

Ref.: 3308e_064 SOLUCIÓN

Ejercicio. 26.65.
Demostrar que un grupo abeliano de orden finito y libre de cuadrados es cíclico, y que por tanto tiene un único p-subgrupo de Sylow para cada número entero primo positivo p que divida al orden.
Ref.: 3308e_065 SOLUCIÓN

Ejercicio. 26.66.
Sea G un grupo finito, H un subgrupo de G y $N = N_G(H)$, demostrar que H tiene exactamente $[G : N]$ conjugados en G. Demostrar que si H es un subgrupo propio de G, entonces G contiene un elemento que no está en ningún conjugado de H.
Ref.: 3308e_066 SOLUCIÓN

Ejercicio. 26.67.
Sea G un grupo finito verificando:
"Para todo número entero positivo primo p que divide al orden de $\mid G \mid$, y todo p-subgrupo de Sylow P, la acción de G sobre G/P, el conjunto de las clases a la izquierda, por traslación es primitivo".
Demostrar que se verifica una de las condiciones siguientes:
(1) Existe un número entero positivo primo p que divide a $\mid G \mid$, y existe un único p-subgrupo de Sylow.
(2) Todo p-subgrupo de Sylow de G coincide con su normalizador.
Ref.: 3308e_067 SOLUCIÓN

Ejercicio. 26.68.
Demostrar que todo grupo de orden 35 es cíclico.
Ref.: 3308e_068 SOLUCIÓN

Ejercicio. 26.69.
Demostrar que no existen grupos simples de orden 42. *Demostrar que todo grupo de orden* 42 *contiene un subgrupo normal de orden* 21.
Ref.: 3308e_069 *SOLUCIÓN*

Ejercicio. 26.70.
Demostrar que todo grupo de orden 99 *es abeliano.*
Ref.: 3308e_070 *SOLUCIÓN*

Ejercicio. 26.71.
Sea G *un grupo de orden finito* n, *y* H *un subgrupo de* G *que verifica* $n \nmid [G : H]!$, *entonces existe un subgrupo normal* N *de* G *verificando* $1 \neq N \subseteq H$.
Ref.: 3308e_071 *SOLUCIÓN*

Ejercicio. 26.72.
Demostrar que si G *es un grupo de orden* 36, *entonces contiene un subgrupo normal de orden* 3 *ó* 9.
Ref.: 3308e_072 *SOLUCIÓN*

Ejercicio. 26.73.
Demostrar que si G *es un grupo de orden* 108, *entonces contiene un subgrupo normal de orden* 9 *ó* 27.
Ref.: 3308e_073 *SOLUCIÓN*

Ejercicio. 26.74.
Usar el método de demostración de los teoremas de Sylow para probar que si $s_p(G)$ no es congruente con 1 módulo p^2, entonces existen dos p–subgrupo de Sylow distintos, P y Q, de G tales que $[P : P \cap Q] = [Q : P \cap Q] = p$.
Ref.: 3308e_074 SOLUCIÓN

Ejercicio. 26.75.
Demostrar que el centro de $SL(2, \mathbb{Z}_3)$ es el grupo de orden dos formado por los elementos $\pm I$, siendo I la matriz identidad. Demostrar que $SL(2, \mathbb{Z}_3)/Z(SL(2, \mathbb{Z}_3)) \cong A_4$.
Ref.: 3308e_075 SOLUCIÓN

Ejercicio. 26.76.
Sea G_1 el grupo de las rotaciones del tetraedro, G_2 el grupo de las rotaciones del cubo y G_3 el grupo de las rotaciones del icosaedro. Calcular los órdenes de cada uno de estos grupos. Determinar en cada caso los p–subgrupos de Sylow para cada entero primo positivo que divida al orden del grupo, y deducir que $G_1 \cong A_4$, $G_2 \cong S_4$ y $G_3 \cong A_5$.
Ref.: 3308e_076 SOLUCIÓN

Capítulo VIII

Producto semidirecto de grupos

27 Productos semidirectos 218
28 Aplicaciones. Ejemplos de grupos 222

Introducción.

27. Productos semidirectos

Si H y N son grupos, decimos que H **actúa por automorfismos** sobre N si el homomorfismo asociado a la acción tiene su imagen en $\mathrm{Aut}(N) \subseteq P(N)$, ó equivalentemente si existe un homomorfismo de grupos $\beta : H \longrightarrow \mathrm{Aut}(N)$.
Por simplicidad, el elemento $\beta(h)(n)$ lo representamos por $h \cdot n$.
Si H actúa por automorfismos sobre N, es posible definir una estructura de grupo en el conjunto producto cartesiano $N \times H$ mediante:

$$(n_1, h_1)(n_2, h_2) = (n_1(h_1 \cdot n_2), h_1 h_2).$$

Lema. 27.1.
Con la operación anterior el conjunto $N \times H$ es un grupo.

DEMOSTRACIÓN. Para ver que la operación es asociativa, dados $(n_1, h_1), (n_2, h_2), (n_3, h_3) \in N \times H$, tenemos

$$\begin{aligned}(n_1, h_1)[(n_2, h_2)(n_3, h_3)] &= (n_1, h_1)(n_2(h_2 \cdot n_3), h_2 h_3) \\ &= (n_1(h_1 \cdot (n_2(h_2 \cdot n_3))), h_1(h_2 h_3)) \\ &= (n_1(h_1 \cdot n_2)(h_1 \cdot (h_2 \cdot (n_3))), (h_1 h_2)h_3) \\ &= (n_1(h_1 \cdot n_2)((h_1 h_2) \cdot (n_3)), (h_1 h_2)h_3) \\ &= (n_1(h_1 \cdot n_2), h_1 h_2)(n_3, h_3) \\ &= [(n_1, h_1)(n_2, h_2)](n_3, h_3)\end{aligned}$$

El elemento neutro es $(1, 1)$, ya que dado $(n, h) \in N \times H$, tenemos:

$$(1, 1)(n, h) = (1(1 \cdot n), 1h) = (n, h)$$

y

$$(n, h)(1, 1) = (n(h \cdot 1), h1) = (n, h).$$

Para $(n, h) \in N \times H$, un inverso es: $(h^{-1} \cdot n^{-1}, h^{-1})$, ya que:

$$(n, h)(h^{-1} \cdot n^{-1}, h^{-1}) = (n(h \cdot (h^{-1} \cdot n^{-1})), hh^{-1}) = (n((hh^{-1}) \cdot n^{-1}), 1) = (1, 1)$$

y

$$(h^{-1} \cdot n^{-1}, h^{-1})(n, h) = ((h^{-1} \cdot n^{-1})(h^{-1} \cdot n), h^{-1}h) = (1, 1).$$

□

El grupo así definido se llama **producto semidirecto** de N por H respecto a la acción β, y se representa por $N \rtimes_\beta H$ o simplemente $N \rtimes H$ si la acción β se deduce del contexto.

3309-01.tex

Ejemplo. 27.2.
Cuando $\beta : H \longrightarrow \mathrm{Aut}(N)$ es el homomorfismo trivial, el producto semidirecto de N por H respecto a la acción β es isomorfo al producto directo de N por H.

Llamamos G al grupo producto $N \times H$, e identificamos N con $N \times \{1\}$ y H con $\{1\} \times H$, entonces cada elemento de G es de la forma nh para algún $n \in N$ y algún $h \in H$. El producto está definido mediante

$$(n_1h_1)(n_2h_2) = (n_1n_2)(h_1h_2).$$

De la misma forma, si consideramos G el grupo $N \rtimes_\beta H$, e identificamos N con $N \times \{1\}$ y H con $\{1\} \times H$, los elementos de G admiten una representación en la forma nh para algún $n \in N$ y algún $h \in H$. El producto ahora está definido mediante:

$$(n_1h_1)(n_2h_2) = (n_1(h_1 \cdot n_2))(h_1h_2).$$

Ejemplos. 27.3.

(1) El grupo S_3 es el producto semidirecto de C_3 y C_2 respecto al único homomorfismo no trivial $\beta : C_2 \longrightarrow C_3$. Si $C_3 = \langle a \rangle$ y $C_2 = \langle b \rangle$, entonces $C_3 \rtimes_\beta C_2$ tiene los elementos

$$(1,1), (a,1), (a^2,1), (1,b), (a,b) \text{ y } (a^2,b),$$

ó equivalentemente 1, a, a^2, b, ab y a^2b, y en esta última representación el producto está definido:

$$ba = (b \cdot a)b = a^2b.$$

(2) Consideramos el único homomorfismo de grupos no trivial $\beta : C_4 \longrightarrow C_3$. Si $C_3 = \langle a \rangle$ y $C_4 = \langle b \rangle$, entonces $C_3 \rtimes_\beta C_4$ tiene 12 elementos. Para encontrar un grupo conocido al que sea isomorfo, llamamos $c = (a, b^2)$ y $d = (1, b)$, entonces:

$$\begin{array}{ll} \mathrm{ord}(c) = 6, & \mathrm{ord}(d) = 4, \\ d^3cdc = 1, & d^2c^3 = 1, \end{array}$$

y tenemos que G es isomorfo al grupo Q_3.

(3) Para cada número natural $n \geq 3$, definimos $\beta : C_2 \longrightarrow C_n$ mediante $\beta(x) = x^{-1}$. Tenemos que el producto semidirecto de C_n por C_2 respecto a β es isomorfo al grupo diédrico D_n.

Caracterización interna del producto semidirecto

Vamos a encontrar una caracterización interna del producto semidirecto de dos grupos.

Teorema. 27.4.
Sean N y H dos grupos y supongamos que H actúa por isomorfismos sobre N mediante el homomorfismo $\beta : H \longrightarrow \mathrm{Aut}(N)$, entonces se verifica:

(1) N y H son (isomorfos a) subgrupos de $G = N \rtimes_\beta H$;

(2) N es un subgrupo normal de G;
(3) $G/N \cong H$;
(4) $G = NH$;
(5) $N \cap H = \{1\}$.

Además la acción de H sobre N coincide con la restricción a H de la acción por conjugación de G sobre N.

DEMOSTRACIÓN. (1). Con las identificaciones anteriores, tenemos $N = \{(n,1) \in G = N \rtimes_\beta H \mid n \in N\}$ y $H = \{(1,h) \in G = N \rtimes_\beta H \mid h \in H\}$, y la operación está definida por:

$$(n_1h_1)(n_2h_2) = (n_1(h_1 \cdot n_2))(h_1h_2),$$

para $n_1, n_2 \in N$ y $h_1, h_2 \in H$. Para $h_1, h_2 \in H$ se tiene $h_1h_2^{-1} \in H$. Para $n_1, n_2 \in N$ se tiene $n_1n_2^{-1} \in N$.
(2). Además para $g = nh \in G$ y $n_1 \in N$, tenemos

$$\begin{aligned} gn_1g^{-1} &= (nh)n_1(nh)^{-1} \\ &= n(h \cdot n_1)h(nh)^{-1} \\ &= n(h \cdot n_1)hh^{-1}n^{-1} \\ &= n(h \cdot n_1)n^{-1} \in N. \end{aligned}$$

(3). Definimos $f : G \longrightarrow H$, mediante $f(nh) = h$, entonces f es un homomorfismo de grupos sobreyectivo y $\mathrm{Ker}(f) = N$. Por el primer teorema de isomorfía tenemos el resultado.
(4). Cada elemento de G es de la forma nh, con $n \in N$ y $h \in H$, luego $G = NH$. Es claro que $N \cap H = \{1\}$.
(5). Si consideramos ahora la conjugación de un elemento n de N por un elemento h de H, tenemos:

$$hnh^{-1} = (hn)h^{-1} = (h \cdot n)hh^{-1} = h \cdot n,$$

luego la acción de H sobre N coincide con la restricción a H de la conjugación en G. □

Este resultado admite un recíproco en la siguiente forma:

Lema. 27.5.
Sea G un grupo con subgrupos N y H verificando:
(1) N es un subgrupo normal de G;
(2) $N \cap H = \{1\}$;
(3) $NH = G$.

Entonces G es isomorfo a un producto semidirecto $N \rtimes_\varphi H$, para algún homomorfismo $\varphi : H \longrightarrow \mathrm{Aut}(N)$.

DEMOSTRACIÓN. Definimos $\varphi : H \longrightarrow \mathrm{Aut}(N)$ mediante $\varphi(h)(n) = hnh^{-1}$, entonces φ es un homomorfismo de grupos. Podemos definir el producto semidirecto de N por H respecto a φ; $N \rtimes_\varphi \mathrm{H}$.
Definimos ahora $\nu : N \rtimes_\varphi H \longrightarrow G$ mediante $\nu(n,h) = nh$. Tenemos que ν es un homomorfismo de grupos

$$\begin{aligned}\nu((n_1,h_1)(n_2,h_2)) &= \nu(n_1(h_1 \cdot n_2), h_1h_2)\\ &= (n_1(h_1 \cdot n_2))(h_1h_2)\\ &= (n_1h_1n_2h_1^{-1})(h_1h_2)\\ &= (n_1h_1)(n_2h_2)\\ &= \nu(n_1,h_1)\nu(n_2,h_2).\end{aligned}$$

Por (3), ν es una aplicación sobreyectiva, y por (2), ν es inyectiva, luego ν es un isomorfismo de grupos. □

Sea $H \subseteq G$ un subgrupo de G. Un subgrupo K de G se llama un **complemento** para H en G si $G = HK$ y $H \cap K = 1$.
Con esta terminología, el Lema 27.5. dice sencillamente que G es un producto semidirecto interno de dos subgrupos propios si, y sólo si, existe un complemento para un subgrupo *normal* propio de G. No todo grupo es el producto semidirecto de dos subgrupos propios (por ejemplo, si G es simple no tiene subgrupos normales propios).
Ejemplos. 27.6.

(1) Dado un grupo G, llamamos **holomorfo** de G al producto semidirecto de G por $\mathrm{Aut}(G)$ respecto al homomorfismo identidad de $\mathrm{Aut}(G)$. Se suele representar por $\mathrm{Hol}(G)$.
(2) Si H es un subgrupo de $\mathrm{Aut}(G)$, y consideramos la acción H sobre G dada por la inclusión $H \subseteq \mathrm{Aut}(G)$, entonces el producto semidirecto de G por H respecto a la inclusión se llama el **holomorfo de** G relativo a H.
(3) Si G es un grupo abeliano que contiene un elemento de orden distinto de 2, entonces el automorfismo de G, $\varphi : G \longrightarrow G$, $\varphi(x) = x^{-1}$, no es la identidad, y tiene orden 2. Existe en este caso un subgrupo $C = \langle\varphi\rangle$ de $\mathrm{Aut}(G)$ de orden 2. Llamamos **grupo diédrico generalizado** de G al holomorfo de G relativo a C, y lo representamos por $\mathrm{Dih}(G)$. Se verifica que G es un subgrupo normal de $\mathrm{Dih}(G)$ de índice 2, y que si G es un grupo cíclico finito de orden n, $n \geq 3$, entonces $\mathrm{Dih}(C_n) \cong D_n$. Si $G \cong \mathbb{Z}$ entonces obtenemos el **grupo diédrico infinito**, al que vamos a representar por D_∞.

28. Aplicaciones. Ejemplos de grupos

Grupos que son producto semidirecto

Ejemplo. 28.1.
Sean $G = S_n$, $H = A_n$ y $K = \langle (1\,2) \rangle \cong \mathbb{Z}_2$. Sabemos que $A_n \triangleleft S_n$, $A_n K = S_n$ y $A_n \cap K = 1$, luego $S_n \cong A_n \rtimes \mathbb{Z}_2$.

Ejemplo. 28.2.
Sean $G = S_4$, $H = V$, $K = S_3 = \mathrm{Stab}_{S_4}(4)$. Sabemos que $V \triangleleft S_4$ y es fácil ver que $V \cap S_3 = 1$ y que $VS_3 = G$. Luego $G \cong V \rtimes S_3$.

Sea G un grupo; existe una acción por automorfismos de $\mathrm{Aut}(G)$ sobre G, definida por la identidad $\mathrm{Aut}(G) \xrightarrow{id} \mathrm{Aut}(G)$. El producto semidirecto $G \rtimes_{id} \mathrm{Aut}(G)$ se llama el **holomorfo** del grupo G y se representa por $\mathrm{Hol}(G)$.

Ejemplo. 28.3.
$\mathrm{Hol}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_4$.

Ejemplo. 28.4.
Si $|G| = n$ y $\pi : G \longrightarrow S_n$ es la representación regular izquierda, entonces $N_{S_n}(\pi(G)) \cong \mathrm{Hol}(G)$.
En particular, como la representación regular izquierda de un generador de $\mathbb{Z}_n$ es un ciclo de longitud n en S_n, deducimos que para cualquier n-ciclo $(1\,2 \ldots n)$,

$$N_{S_n}(\langle (1\,2 \ldots n) \rangle) \cong \mathrm{Hol}(\mathbb{Z}_n) = \mathbb{Z}_n \rtimes \mathrm{Aut}(\mathbb{Z}_n)$$

Se deduce entonces que este grupo tiene orden $n\varphi(n)$.

Definición del **grupo dicíclico** Q_m.

Ejemplo. 28.5.
El ejemplo del grupo diédrico generalizado se puede extender de diversas maneras. Veamos una de ellas: Sea H cualquier grupo abeliano y sea $K = \langle y \mid y^{2n} = 1 \rangle$. Volvemos a definir $\theta : K \longrightarrow \mathrm{Aut}(H)$ como $\theta(y, a) = y * a = a^{-1}$ para todo $a \in H$. Se verifica para cada $a \in H$ que $y^2 a y^{-2} = a$, luego $y^2 \in Z(G)$, siendo $G = H \rtimes_\theta K$. En particular si $n = 2$ y $H = \langle x \mid x^m = 1 \rangle$ con m impar, G es isomorfo al grupo dicíclico Q_m

Ejemplo. 28.6.
Para un número par m el grupo dicíclico no es un producto semidirecto (en particular el grupo cuaternio Q_2 no lo es). En cambio podemos obtener Q_2 como un cociente de un producto semidirecto: Sea m par y sea $H = \langle x \mid ; x^m = 1 \rangle$. Sea $K = \langle y \mid y^4 = 1 \rangle$ y formamos el grupo G del ejemplo anterior. Como en dicho ejemplo, $y^2 \in Z(G)$. Sea $z = x^{\frac{m}{2}}$. Tenemos $z^2 = 1$, $yzy^{-1} = z$ y por tanto $z \in Z(G)$.

3309-02.tex

Formamos el grupo $N = \langle zy^2 \rangle$. Este es un subgrupo de $Z(G)$ y por tanto es normal en G. Sea $\bar{G} = G/N$, y sean $\bar{x} = xN$, $\bar{y} = yN$. Tenemos las presentaciones:

$$G = \langle x, y \mid x^m = 1, y^4 = 1, yxy^{-1} = x^{-1} \rangle$$

$$\bar{G} = \langle \bar{x}, \bar{y} \mid \bar{x}^m = 1, \bar{x}^{\frac{m}{2}}\bar{y}^2 = 1, \bar{y}\bar{x}\bar{y}^{-1} = \bar{x}^{-1} \rangle$$

y este último es precisamente el grupo dicíclico Q_m.

Ejemplo. 28.7.
Sea $H = \mathbb{Q}$ (respecto a la suma), y sea $K = \langle y \rangle \cong \mathbb{Z}$. Definimos $\theta : K \longrightarrow \mathrm{Aut}(\mathbb{Q})$ por $\theta(y)(q) = y * q = 2q$ para todo $q \in \mathbb{Q}$ (nótese que "multiplicación por 2" en $\mathbb{Q}$ es un automorfismo ya que tiene un inverso, "multiplicación por $\frac{1}{2}$"). Identificamos $\mathbb{Q}$ con su imagen en $G = \mathbb{Q} \rtimes_\theta K$. Entonces $\mathbb{Z} \leq G$ y el conjugado $y\mathbb{Z}y^{-1} = 2\mathbb{Z} \lneq \mathbb{Z}$. Luego $y \notin N_G(\mathbb{Z})$ aún cuando $y\mathbb{Z}y^{-1} \leq \mathbb{Z}$ (pero $y^{-1}\mathbb{Z}y \not\leq \mathbb{Z}$). Así que para demostrar que un elemento g normaliza un subgrupo A en un grupo G *infinito* no es suficiente demostrar que $gAg^{-1} \leq A$, lo cual si es suficiente cuando G es un grupo *finito*.

Ejemplo. 28.8.
Sea $C_n = \langle a \mid a^n = 1 \rangle$. Sea $k \in \mathbb{Z}$ tal que $(k, n) = 1$. En este caso a^k también es un generador de C_n, así que la aplicación $a^i \mapsto a^{ki}$ define un automorfismo $\alpha : C_n \longrightarrow C_n$. Sea $m \in \mathbb{Z}$, $k^m \equiv 1 \pmod{n}$. Calculemos: $\alpha^m(a^i) = \alpha^{m-1}(a^{ki}) = \cdots = a^{k^m i} = a^i \Rightarrow \alpha^m = 1$. Sea $C_m = \langle d \mid d^m = 1 \rangle$. Por el teorema de Dyck existe un homomorfismo $\theta : C_m \longrightarrow \mathrm{Aut}(C_n)$ dado por $\theta(d) = \alpha$. Entonces $G = C_n \rtimes_\theta C_m = \{(a^i, d^j) \mid 0 \leq i \leq n, 0 \leq j < m\}$. Identificamos $a = (a, 1), d = (1, d)$. Obtenemos $(a^i, 1)(1, d^j) = (a^i, d^j) = a^i d^j$, y $da = (1, d)(a, 1) = (d * a, d) = (\alpha(a), d) = (a^k, d) = a^k d$. Como G está generado por a y d, obtenemos la presentación:

$$G = \langle a, d \mid a^n = 1, d^m = 1, da = a^k d \rangle$$

que es un **grupo metacíclico**. Depende de tres parámetros: n, m, k sujetos a la relación $k^m \equiv 1$ (mód n). En particular, si $k = n - 1$ y $m = 2$ obtenemos el grupo diédrico D_n. Luego todo grupo diédrico es un producto semidirecto.

Aplicaciones de los teoremas de Sylow

Ejemplo. 28.9. (S_3)
El grupo S_3 tiene tres 2-subgrupos de Sylow: $\langle(12)\rangle$, $\langle(13)\rangle$ y $\langle(23)\rangle$. Tiene un único (por tanto normal) 3-subgrupo de Sylow: $\langle(123)\rangle = A_3$. Nótese que $3 \equiv 1 \pmod 2$.

Ejemplo. 28.10. (A_4)
A_4 tiene un único 2-subgrupo de Sylow: $V = \langle(12)(34),(13)(24)\rangle$. Tiene cuatro 3-subgrupos de Sylow: $\langle(123)\rangle$, $\langle(124)\rangle$, $\langle(134)\rangle$ y $\langle(234)\rangle$. Nótese que $4 \equiv 1 \pmod 3$.

Ejemplo. 28.11. (S_4)
S_4 tiene $n_2 = 3$ y $n_3 = 4$. Ya que S_4 contiene un subgrupo isomorfo a D_4, los tres 2-subgrupos de Sylow de S_4 son isomorfos a D_4.

Ejemplo. 28.12. (S_p)
Sea p un primo. Todo p-subgrupo de S_p tiene orden p, es cíclico y simple; contiene $p-1$ ciclos de longitud p, todos ellos son generadores. El número total de ciclos de longitud p en S_p es exactamente $(p-1)!$, así que tenemos que $n_p = (p-2)!$

El número n_p es también el índice $[S_p : N_{S_p}(P)]$ siendo P un p-subgrupo de Sylow. Entonces, por el teorema de Lagrange, resulta $|N_{S_p}(P)| = p(p-1)$.

Calculamos ahora el centralizador de P en G (luego nos hará falta): $\sigma \in C_{S_p}(P)$ si y sólo si $\sigma \in C_{S_p}((i_1 \dots i_p))$ para cualquier ciclo de longitud p de P. Como todos los ciclos de longitud p son conjugados en S_p, $[S_p : C_{S_p}(P)] = (p-1)!$, (de la igualdad $|\operatorname{Orb}_G(x)| = [G : \operatorname{Stab}_G(x)]$) luego $|C_{S_p}(P)| = p$ y como $|P| = p$ y $P \subseteq C_{S_p}(P)$, entonces $C_{S_p}(P) = P$ y es un subgrupo propio de $N_{S_p}(P)$.

Ejemplo. 28.13. ($\mathrm{GL}_2(\mathbb{Z}_p)$)
Sea p un primo y $G = \mathrm{GL}_2(\mathbb{Z}_p)$.

Recordemos que el orden G es $|G| = (p^2-1)(p^2-p) = p(p-1)^2(p+1)$. La máxima potencia de p que divide a $|G|$ es exactamente p, por lo tanto los p-subgrupos de Sylow de G tienen orden p y son cíclicos.

Resulta que $H = \{\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \mid a \in \mathbb{Z}_p\}$ y $K = \{\left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right) \mid a \in \mathbb{Z}_p\}$ son dos subgrupos *distintos* de G de orden p, luego $n_p \geq p+1$.

Tenemos que $D = \{\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) \mid a, b \in \mathbb{Z}_p^\times\}$ verifica:

(1) D normaliza a H,
(2) $|D| = (p-1)^2$ y
(3) $D \cap H = 1$,

luego DH es un subgrupo de $N_G(H)$ y por tanto $|N_G(H)| \geq |DH| = p(p-1)^2$. De donde $n_p = [G : N_G(H)] = \frac{|G|}{|N_G(H)|} \leq p+1$. En resumen, $n_p = p+1$ y $N_G(H) = DH$.

3309-03.tex

Estudio y clasificación de grupos

Vamos a aplicar el Lema (27.5.) para clasificar los grupos de orden n para algunos valores de n. El argumento básico es el siguiente:

(1) Demostrar que todo grupo de orden n tiene subgrupos propios N y H que satisfacen las hipótesis del Lema (27.5.).
(2) Determinar todos los posibles tipos de isomorfismo para N y H.
(3) Para cada par (N,H), hallado en el paso anterior, hallar todos los homomorfismos que existen $\theta : H \longrightarrow \mathrm{Aut}(N)$.
(4) Para cada terna (N,H,θ) hallada, formar el producto semidirecto $N \rtimes_\theta H$ (así que cualquier grupo de orden n es isomorfo a uno de estos grupos construidos explícitamente) y entre todos estos productos semidirectos determinar qué pares son isomorfos. Eliminadas las repeticiones, nos queda una lista de todos los tipos de isomorfismo distintos de grupos de orden n.

Para valores pequeños de n, hallamos los posibles N y H usando los teoremas de Sylow. Para demostrar la normalidad de N en G podemos usar los teoremas de Sylow o cualquier otro de los criterios conocidos (por ejemplo: *si* $[G:H] = p$ *es el menor primo que divide a* $|G|$ *entonces* $H \triangleleft G$). En muchos de los ejemplos que siguen, $|N|$ y $|H|$ son primos relativos, lo que implica $N \cap H = 1$ por el teorema de Lagrange.

Como N y H son subgrupos propios de G, se determinan inductivamente a partir de subgrupos suyos más sencillos. En los ejemplos que siguen, N y H tienen ordenes suficientemente pequeños como para que conozcamos sus tipos de isomorfismo a partir de resultados previos. Por ejemplo, en muchos casos son de orden primo o cuadrado de primo.

En nuestros ejemplos existen relativamente pocos homomorfismos $\theta : H \longrightarrow \mathrm{Aut}(N)$; en especial después de tomar en cuenta algunas simetrías (como, por ejemplo, reemplazar un generador de H por otro cuando H es cíclico).

Finalmente los productos semidirectos que aparecen en este proceso serán pocos en nuestros ejemplos y en general veremos que no son isomorfos entre sí. Pero en casos mas complejos este puede ser un problema delicado.

Lema. 28.14.
Sean H y K dos grupos y $\rho_1, \rho_2 : K \longrightarrow \mathrm{Aut}(H)$ homomorfismos de grupos.

(1) Si $\theta : K \longrightarrow K$ es un isomorfismo que verifica $\rho_1 = \rho_2\theta$, entonces $\overline{\theta} : H \rtimes_{\rho_1} K \longrightarrow H \rtimes_{\rho_2} K$ definido $\overline{\theta}(h,k) = (h,\theta(k))$ es un isomorfismo de grupos.

$$\begin{array}{ccc} K & \xrightarrow{\rho_1} & \mathrm{Aut}(H) \\ {\scriptstyle\theta}\downarrow & & \| \\ K & \xrightarrow{\rho_2} & \mathrm{Aut}(H) \end{array}$$

3309-04.tex

(2) Si $\nu : H \longrightarrow H$ es un isomorfismo de grupos que verifica $\theta\rho_1(k)\theta^{-1} = \rho_2(k)$ para cada $k \in K$, entonces $\overline{\nu} : H \rtimes_{\rho_1} K \longrightarrow H \rtimes_{\rho_2} K$ definido $\overline{\nu}(h,k) = (\nu(h),k)$ es un isomorfismo de grupos.

$$\begin{array}{ccc} K & \xrightarrow{\rho_1} & \mathrm{Aut}(H) \\ \| & & \downarrow{\scriptstyle \varphi_\nu} \\ K & \xrightarrow{\rho_2} & \mathrm{Aut}(H) \end{array}$$

DEMOSTRACIÓN. (1).

$$\begin{aligned} \overline{\theta}((h_1,k_1)(h_2,k_2)) &= \overline{\theta}(h_1\rho_1(k_1)(h_2),k_1k_2) \\ &= (h_1\rho_1(k_1)(h_2),\theta(k_1k_2)) \\ &= (h_1\rho_2\theta(k_1)(h_2),\theta(k_1)\theta(k_2)) \\ &= (h_1,\theta(k_1))(h_2,\theta(k_2)) \\ &= \overline{\theta}(h_1,k_1)\overline{\theta}(h_2,k_2) \end{aligned}$$

(2).

$$\begin{aligned} \overline{\nu}((h_1,k_1)(h_2,k_2)) &= \overline{\nu}(h_1\rho_1(k_1)(h_2),k_1k_2) \\ &= (\nu(h_1\rho_1(k_1)(h_2)),k_1k_2) \\ &= (\nu(h_1)\nu(\rho_1(k_1)(h_2)),k_1k_2) \\ &= (\nu(h_1)(\nu\rho_1(k_1))(h_2),k_1k_2) \\ &= (\nu(h_1)(\rho_2(k_1)\nu)(h_2),k_1k_2) \\ &= (\nu(h_1)\rho_2(k_1)(\nu(h_2)),k_1k_2) \\ &= (\nu(h_1),k_1)(\nu(h_2),k_2) \\ &= \overline{\nu}(h_1,k_1)\overline{\nu}(h_2,k_2) \end{aligned}$$

□

Esta forma de expresar todo grupo de orden n como un producto semidirecto de subgrupos propios no funciona para n arbitrario. Por ejemplo, Q_2 no es un producto semidirecto porque ningún subgrupo propio tiene un complemento. En general el proceso funciona bien cuando n no es divisible por una potencia alta de un primo p. En el otro extremo, para p un primo y t grande sólo una pequeña parte de los grupos de orden p^t son productos semidirectos no triviales.
En los ejemplos llamamos $\mathrm{Syl}_p(G) = \{P \mid P \text{ es un } p\text{-subgrupo de Sylow de } G\}$ y $n_p = n_p(G) = |\mathrm{Syl}_p(G)|$.

Grupos de orden pq, con p y q primos y $p < q$

Sea $|G| = pq$. Consideramos $P \in \mathrm{Syl}_p(G)$ y $Q \in \mathrm{Syl}_q(G)$. Las condiciones $n_q \mid p$ y $n_q \equiv 1 \pmod q$ fuerzan que $n_q = 1$; así que tenemos un subgrupo normal $Q \triangleleft G$.
Como $n_p \mid q$, las únicas posibilidades son $n_p = 1$ y $n_p = q$, y ésta última sólo se puede dar si $p|(q-1)$.

Los grupos P y Q tienen orden primo y por tanto son cíclicos. Sean $P = \langle y \mid y^p = 1\rangle$ y sea $Q = \langle x \mid x^q = 1\rangle$.
Si $n_p = 1$, entonces $P \triangleleft G$, $PQ = G$, x e y conmutan y tenemos

$$G = \langle x, y \mid x^q = 1, y^p = 1, xy = yx\rangle$$

que es un grupo cíclico de orden pq. En particular, si p no divide a $q-1$, existe un único grupo de orden pq. Esto ocurre por ejemplo para $|G| = 15$.
Si $p \mid (q-1)$. Como $\mathrm{Aut}(Q)$ es cíclico contiene un único subgrupo de orden p, sea éste $\langle\alpha\rangle$. Cualquier homomorfismo $\theta : P \longrightarrow \mathrm{Aut}(Q)$ debe aplicar y en una potencia de α. Por tanto existen p homomorfismos $\theta_i : P \longrightarrow \mathrm{Aut}(Q)$ dados por $\theta_i(y) = \alpha^i$, $0 \le i < p$. Ya que θ_0 es el homomorfismo trivial, $Q \rtimes_{\theta_0} P \cong Q \times P$. Cada uno de los otros θ_i da lugar a un grupo G_i no abeliano de orden pq. Es inmediato comprobar que estos $p-1$ grupos son todos isomorfos ya que para cada θ_i existe un y_i, generador de P, tal que $\theta_i(y_i) = \alpha$. De modo que estos productos semidirectos son todos isomorfos salvo elección del generador arbitrario de P.
Veamos una realización de un grupo no abeliano de orden pq (cuando $p \mid q-1$). Sea Q un q-subgrupo de Sylow de S_q. Por el Ejemplo 28.12. se verifica $|N_{S_q}(Q)| = q(q-1)$. Por el teorema de Cauchy, existe $P < N_{S_q}(Q)$ tal que $|P| = p$. Por el segundo teorema de isomorfía, $PQ < N_{S_q}(Q)$ y $|PQ| = pq$. Como $C_{S_q}(Q) = Q \neq PQ$, y PQ es un grupo no abeliano.

Grupos de orden pqr, $p < q < r$ primos distintos

Sea $|G| = pqr$. En primer lugar veamos que G tiene un subgrupo de Sylow normal: Si no fuera así, tendríamos $n_r = pq$, $n_p \ge q$, $n_q \ge r$. Contamos elementos de orden primo:

número de elementos de orden 1	$=$	1
número de elementos de orden r	$=$	$pq(r-1)$
número de elementos de orden p	$\ge$	$q(p-1)$
número de elementos de orden q	$\ge$	$r(q-1)$
número de elementos de G	$\ge$	$pqr + (r-1)(q-1) \quad > \quad pqr$

Lo cual es imposible. Ahora podemos demostrar: *Para todo grupo de orden pqr con $p < q < r$ primos distintos, $n_r = 1$.* Para verlo, sabemos que uno de los subgrupos de Sylow es normal. Si $n_p = 1$, sea P el p-subgrupo de Sylow. $|G/P| = qr$ luego existe $\bar{K} \triangleleft G/P$ tal que $|\bar{K}| = r$; $\bar{K} = K/P$ con $K \triangleleft G$ y $|K| = pr$. Entonces existe $R < K$ único tal que $|R| = r$. Como R es característico en K y K es normal en G, tenemos $R \triangleleft G$. El mismo razonamiento se aplica si $n_q = 1$. Luego en cualquier caso, $n_r = 1$.
Esta técnica de contar elementos de distintos órdenes se usa con mucha frecuencia, y funciona particularmente bien cuando los p-subgrupos de Sylow tienen orden p (como en este ejemplo), ya que entonces la intersección de dos p-subgrupos distintos es la identidad. Si el orden de los p-subgrupos de Sylow es p^i con $i > 1$, es necesario mayor cuidado al contar, ya que p-subgrupos de Sylow distintos pueden tener intersección no trivial.

Grupos de orden 30

Sea G un grupo de orden 30, sean $P \in \mathrm{Syl}_3(G)$ y $Q \in \mathrm{Syl}_5(G)$ subgrupos de Sylow. Supongamos que ninguno de ellos es normal. Entonces $n_3 = 10$, $n_5 = 6$. Cada elemento de orden 5 está en un

5-subgrupo de Sylow de G y cada 5-subgrupo de Sylow de G contiene cuatro elementos de orden 5, además la intersección de dos 5-subgrupos de Sylow distintos es trivial. Así que G contiene $4\cdot 6 = 24$ elementos de orden 5. Análogamente G contiene $2\cdot 10 = 20$ elementos de orden 3. Luego G contiene por lo menos $24 + 20 = 44$ elementos distintos. Pero G sólo tiene 30 elementos, contradicción.
Se verifica entonces que o $n_3 = 1$ ó $n_5 = 1$. Pero entonces $P \triangleleft G$ ó $Q \triangleleft G$. En cualquier caso, $PQ \subsetneq G$, pues su orden es $|PQ| = 15$, por el segundo teorema de isomorfía, y es normal por ser $[G : PQ] = 2$. Por el apartado anterior solamente existe un grupo de orden 15 y es abeliano; entonces ambos P y Q son subgrupos característicos de PQ (por ser subgrupos de Sylow normales) y por tanto ambos son normales en G.
Tenemos que todo grupo G de orden 30 contiene un subgrupo N de orden 15 y al menos un 2-subgrupo de Sylow H de orden 2. Además N y H verifican las condiciones del Lema 27.5., luego $G \cong N \rtimes_\theta H$.
Tenemos que $N = \langle x \mid x^{15} = 1\rangle$ es el grupo cíclico y

$$\mathrm{Aut}(N) \cong \mathrm{Aut}(\mathbb{Z}_{15}) \cong \mathbb{Z}_{15}^\times \cong \mathbb{Z}_4 \times \mathbb{Z}_2$$

En particular $\mathrm{Aut}(N)$ contiene exactamente tres elementos de orden un divisor de 2:

- $\theta_0(x) = x$, (la identidad);
- $\theta_1(x) = x^4$;
- $\theta_2(x) = x^{-4}$;
- $\theta_3(x) = x^{-1}$.

Sea $H = \langle y \mid y^2 = 1\rangle$. Existen cuatro grupos de orden 30:

- $G_0 = N \rtimes_{\theta_0} H \cong \langle x, y \mid x^{15} = y^2 = 1, yxy^{-1} = x\rangle$;
- $G_1 = N \rtimes_{\theta_1} H \cong \langle x, y \mid x^{15} = y^2 = 1, yxy^{-1} = x^4\rangle$;
- $G_2 = N \rtimes_{\theta_2} H \cong \langle x, y \mid x^{15} = y^2 = 1, yxy^{-1} = x^{-4}\rangle$;
- $G_3 = N \rtimes_{\theta_3} H \cong \langle x, y \mid x^{15} = y^2 = 1, yxy^{-1} = x^{-1}\rangle$.

Para identificar estos grupos con otros conocidos, descomponemos $N = N_1 \times N_2$ donde $N_1 = \langle x^3\rangle \cong \mathbb{Z}_5$ y $N_2 = \langle x^5\rangle \cong \mathbb{Z}_3$. Llamando $u = x^3, v = x^5$ tenemos las presentaciones:

$$\begin{aligned}
G_0 &= \langle u, v, y \mid u^5 = v^3 = y^2 = 1, vuv^{-1} = u, yuy^{-1} = u, yvy^{-1} = v\rangle && \cong \mathbb{Z}_{30}\\
G_1 &= \langle u, v, y \mid u^5 = v^3 = y^2 = 1, vuv^{-1} = u, yuy^{-1} = u^{-1}, yvy^{-1} = v\rangle && \cong \mathbb{Z}_3 \times D_5\\
G_2 &= \langle u, v, y \mid u^5 = v^3 = y^2 = 1, vuv^{-1} = u, yuy^{-1} = u, yvy^{-1} = v^{-1}\rangle && \cong \mathbb{Z}_5 \times D_3\\
G_3 &= \langle u, v, y \mid u^5 = v^3 = y^2 = 1, vuv^{-1} = u, yuy^{-1} = u^{-1}, yvy^{-1} = v^{-1}\rangle && \cong D_{15}
\end{aligned}$$

Nótese que estos grupos son todos no isomorfos entre sí, ya que sus centros respectivos tienen órdenes 15, 5, 3, 1.
Aunque todos los grupos de este ejemplo pueden definirse en función de otros más pequeños usando sólo el producto directo, el argumento que hemos seguido muestra que esta es la lista *completa* de tipos de isomorfismo de grupos de orden 30.

Grupos de orden 12

Sea G un grupo de orden 12. Vamos a ver que o bien G tiene un 3-subgrupo de Sylow normal o bien $G \cong A_4$ (en cuyo caso G tiene un 2-subgrupo de Sylow normal). Más adelante usaremos esta información para clasificar los grupos de orden 12.

Supongamos $n_3 \neq 1$ (por tanto $n_3 = 4$), y sea $P \in \mathrm{Syl}_3(G)$. Consideramos la acción de G sobre G/P por traslación por la izquierda. Obtenemos un homomorfismo $\varphi : G \longrightarrow S_4$ cuyo núcleo está contenido en P. Como P no es normal en G y tiene orden tres, el núcleo de φ es trivial y φ es inyectivo. La imagen de φ es un subgrupo de S_4 de orden 12, necesariamente A_4. Obsérvese que para éste grupo tenemos $n_2 = 1$ y $n_3 = 4$.

Este resultado puede obtenerse también mediante la acción por conjugación: Hacemos actuar a G sobre $\mathrm{Syl}_3(G)$ por conjugación. Obtenemos un homomorfismo $\psi : G \longrightarrow S_4$ cuyo núcleo es la intersección de todos los normalizadores de los subgrupos de orden 3. Para cada uno de éstos tenemos $N_G(P) = P$ (ya que $[G : N_G(P)] = 4$), y como los 3-subgrupos P son distintos y de orden 3, el núcleo de ψ es trivial.

Sea G un grupo arbitrario de orden 12 y sean $N \in \mathrm{Syl}_3(G)$, $K \in \mathrm{Syl}_2(G)$. Sabemos que o $G \cong A_4$ ó $N \triangleleft G$. Nos concentramos en este caso: N y K verifican las condiciones del Lema 27.5., y por tanto $G \cong N \rtimes_\theta K$.

$|N| = 3$ y por tanto $N = \langle x \mid x^3 = 1 \rangle$ y $\mathrm{Aut}(N) \cong \mathbb{Z}_2$. El único automorfismo no trivial viene dado por $\alpha(x) = x^{-1}$. Para K caben dos posibilidades:

(1) $K = \langle y \mid y^4 = 1 \rangle \cong \mathbb{Z}_4$. Existen dos posibles homomorfismos $\theta : K \longrightarrow \mathrm{Aut}(N)$:

- $\theta_0(y) = 1$. Tenemos el grupo:

$$G_0 = \langle x, y \mid x^3 = y^4 = 1, yxy^{-1} = x \rangle \cong \mathbb{Z}_{12}.$$

- $\theta_1(y) = \alpha$. Nos da el grupo:

$$G_1 = \langle x, y \mid x^3 = y^4 = 1, yxy^{-1} = x^{-1} \rangle \cong Q_3.$$

(2) $K = \langle y, z \mid y^2 = z^2 = 1, yzy^{-1} = z \rangle$. Otra vez tenemos dos homomorfismos posibles:

- $\theta_0(y) = \theta_0(z) = 1$ que nos da:

$$G_2 = \langle x, y, z \mid x^3 = y^2 = z^2 = 1, yxy^{-1} = x, zxz^{-1} = x, yzy^{-1} = z \rangle \cong \mathbb{Z}_6 \times \mathbb{Z}_2.$$

- $\theta_1(y) = \alpha, \theta_1(z) = 1$ con lo que queda:

$$G_3 = \langle x, y, z \mid x^3 = y^2 = z^2 = 1, yxy^{-1} = x^{-1}, zxz^{-1} = x, yzy^{-1} = z \rangle \cong D_3 \times \mathbb{Z}_2 \cong D_6$$

En resumen, salvo isomorfismo hay exactamente cinco grupos de orden 12: $\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2$, Q_3, D_6 y A_4. Los dos primeros son abelianos y los tres últimos no lo son.

Grupos de orden p^2q, p y q primos distintos

Sea G un grupo de orden p^2q. Demostraremos que G tiene un subgrupo de Sylow normal. Sean $P \in \mathrm{Syl}_p(G)$ y $Q \in \mathrm{Syl}_q(G)$.

- Sea $p > q$. Ya que $n_p \mid q$ y $n_p = 1 + kp$, debe ser $n_p = 1$, entonces $P \triangleleft G$.
- Sea ahora $p < q$. Si $n_q = 1$, entonces Q es normal en G. Supongamos $n_q > 1$. Como $q > p$, tiene que ser $n_q = p^2$. Además, $q \mid (p^2-1)$ y como q es primo, $q \mid (p-1)$ o bien $q \mid (p+1)$. Lo primero es imposible así que $q \mid (p+1)$ y como $q > p$, $q = p+1$. Esto fuerza a que $p = 2$, $q = 3$ y $|G| = 12$. Pero este caso ya lo hemos tratado antes. En particular todo grupo con $|G| = 20$ tiene $n_5 = 1$.
- Finalmente si $q \nmid (p^2-1)$ y $p \nmid (q-1)$, entonces $n_q = n_p = 1$, el p-subgrupo de Sylow y el q-subgrupo de Sylow de G son abelianos y conmutan elemento a elemento, luego G es abeliano. Para un tal n sólo hay dos grupos salvo isomorfismo. Esto ocurre, por ejemplo, para $|G| = 45$.

Grupos de orden 20

Sea G un grupo arbitrario de orden 20. Por los teoremas de Sylow sabemos que existe un único $H \triangleleft G$ con $|H| = 5$. Sea $H = \langle x \mid x^5 = 1\rangle$. También sabemos que existe $K < G$ con $|K| = 4$. Por el teorema de Lagrange se ve que $H \cap K = 1$, $HK = G$, luego $G \cong H \rtimes_\theta K$. Es fácil ver que $\mathrm{Aut}(H) = \langle \alpha \mid \alpha^4 = 1\rangle$, siendo $\alpha(x) = x^2$. Distinguimos dos casos:
(1) $K = \langle y, z \mid y^2 = z^2 = (yz)^2 = 1\rangle$. Existen dos posibles homomorfismos:

- $\theta_0 = 1$ que nos da el producto directo:

$$G_1 = \langle x, y, z \mid x^5 = y^2 = z^2 = 1, xy = yx, xz = zx, yz = zy\rangle \cong \mathbb{Z}_{10} \times \mathbb{Z}_2$$

- $\theta_1(y) = 1, \theta_1(z) = \alpha^2$ que nos da el grupo diédrico:

$$G_2 = \langle x, y, z \mid x^5 = y^2 = z^2 = 1, xy = yx, xz = zx^{-1}, yz = zy\rangle \cong D_{10}$$

(2) $K = \langle y \mid y^4 = 1\rangle$ Existen tres homomorfismos:

- $\theta_0(y) = 1$ que origina el producto directo:

$$G_3 = \langle x, y \mid x^5 = y^4 = 1,\ yxy^{-1} = x\rangle \cong \mathbb{Z}_{20}$$

- $\theta_1(y) = \alpha^2$ que produce el grupo dicíclico:

$$G_4 = \langle x, y \mid x^5 = y^4 = 1,\ yxy^{-1} = x^{-1}\rangle \cong Q_5$$

- $\theta_2(y) = \alpha$ que da lugar al grupo de Frobenius:

$$G_5 = \langle x, y \mid x^5 = y^4 = 1,\ yxy^{-1} = x^2\rangle \cong F$$

En resumen existen cinco grupos de orden 20 salvo isomorfismos, dos abelianos y tres no abelianos.

Grupos de orden 18

Sea G un grupo arbitrario de orden 18. Por los teoremas de Sylow, existe un único 3–subgrupo de Sylow $H \triangleleft G$ con $|H| = 9$ y $\exists K < G$ tal que $|K| = 2$. Sea $K = \langle y \mid y^2 = 1\rangle$. Para H existen dos posibilidades:

(1) $H = \langle x \mid x^9 = 1\rangle \cong \mathbb{Z}_9$. Entonces $\mathrm{Aut}(H) = \langle \alpha \mid \alpha^6 = 1\rangle \cong \mathbb{Z}_6$, siendo $\alpha(x) = x^2$. Existen dos homomorfismos:

- $\theta_0(y) = 1$ que origina el grupo cíclico:

$$G_0 = \langle x, y \mid x^9 = y^2 = 1,\ yxy^{-1} = x\rangle \cong \mathbb{Z}_{18}$$

- $\theta_1(y) = \alpha^3$ que origina el grupo diédrico:

$$G_1 = \langle x, y \mid x^9 = y^2 = 1,\ yxy^{-1} = x^{-1}\rangle \cong D_9$$

(2) $H = \langle x, z \mid x^3 = z^3 = 1, zx = xz\rangle \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. En este caso, $\mathrm{Aut}(H) \cong \mathrm{GL}_2(\mathbb{Z}_3)$. Por el teorema de Dyck, existe un $\theta_\alpha : K \longrightarrow \mathrm{Aut}(H)$ para cada $\alpha \in \mathrm{Aut}(H)$ tal que $\alpha^2 = 1$. Si α y β son conjugados, los homomorfismos θ_α y θ_β determinan productos semidirectos isomorfos. Luego hay que determinar las clases de conjugación de elementos de orden 1 o 2 en $\mathrm{GL}_2(\mathbb{Z}_3)$. Recordamos de Álgebra Lineal que dos matrices son conjugadas en el grupo lineal general si y sólo si son semejantes, lo cual ocurre si y sólo si tienen los mismos factores invariantes. Las matrices A que nos interesan verifican $A^2 = I$, luego son aquellas cuyo polinomio mínimo divide a $X^2 - 1$. Como son matrices dos por dos, obtenemos las siguientes posibilidades:

- Polinomio mínimo $= X - 1$. Entonces los factores invariantes son $X - 1$, $X - 1$: $A = I$, $\alpha(x) = x$, $\alpha(z) = z$ y obtenemos el producto directo:

$$G_2 = \langle x, y, x \mid x^3 = y^2 = z^3 = 1, zx = xz, yxy^{-1} = x, yzy^{-1} = z\rangle \cong \mathbb{Z}_6 \times \mathbb{Z}_3$$

- Polinomio mínimo $= X + 1$. Entonces los factores invariantes son $X + 1$, $X + 1$: $A = -I$, $\alpha(x) = x^{-1}$, $\alpha(z) = z^{-1}$ y obtenemos el grupo diédrico generalizado:

$$G_3 = \langle x, y, x \mid x^3 = y^2 = z^3 = 1, zx = xz, yxy^{-1} = x^{-1}, yzy^{-1} = z^{-1}\rangle$$

- Polinomio mínimo $= X^2 - 1$. Los divisores elementales son $X + 1, X - 1$: $A = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\alpha(x) = x^{-1}$, $\alpha(z) = z$ y obtenemos el producto directo:

$$G_4 = \langle x, y, x \mid x^3 = y^2 = z^3 = 1,\ zx = xz,\ yxy^{-1} = x^{-1},\ yzy^{-1} = z\rangle \cong D_3 \times \mathbb{Z}_3$$

En total tenemos, salvo isomorfismo, cinco grupos de orden 18, dos abelianos y tres no abelianos.

Exactamente el mismo razonamiento se aplica para determinar todos los grupos de orden $2p^2$ con p primo impar, y siempre nos quedan los cinco grupos análogos.

Grupos de orden 24

El razonamiento del párrafo sobre grupos de orden 12 puede generalizarse para obtener el siguiente resultado: Sea G un grupo de orden 24. Entonces o $n_3 = 1$ ó $n_2 = 1$ ó $G \cong S_4$.
Supongamos $n_3 \neq 1$ (por tanto $n_3 = 4$), y sea $P \in \mathrm{Syl}_3(G)$. Tomamos la acción de G sobre $\mathrm{Syl}_3(G)$ por conjugación. Obtenemos un homomorfismo $\varphi : G \longrightarrow S_4$ cuya imagen es un subgrupo transitivo de S_4 y por tanto $4 \mid |\mathrm{Im}(\varphi)|$. Por el primer teorema de isomorfía, $|\mathrm{Ker}(\varphi)| \mid 6$. Si $|\mathrm{Ker}(\varphi)| = 3$ ó 6, G tendría un 3-subgrupo de Sylow normal en contra de la hipótesis. Así que quedan dos posibilidades:

- $|\mathrm{Ker}(\varphi)| = 2$. Entonces $|\mathrm{Im}(\varphi)| = 12$, $\mathrm{Im}(\varphi) = A_4$ que tiene un único subgrupo de orden 4 (que es normal). Su imagen inversa bajo φ es un subgrupo normal de G de orden 8, así que $n_2 = 1$.
- $|\mathrm{Ker}(\varphi)| = 1$. Entonces $\mathrm{Im}(\varphi) = S_4$, y $G \cong S_4$.

Grupos de orden 36

En los ejemplos considerados hasta ahora hemos deducido la existencia de un subgrupo de Sylow normal. Vamos a ver que a veces, como en este caso, podemos deducir la existencia de un subgrupo normal propio, aunque no necesariamente de Sylow: *Si G es un grupo de orden 36, entonces ó $n_3 = 1$ ó $\exists H \triangleleft G$ tal que $|H| = 3$.* Para verlo, supongamos $n_3 = 4$ (el único valor posible distinto de 1, según el segundo teorema de Sylow). La acción por conjugación de G sobre $S = \mathrm{Syl}_3(G)$ nos da un homomorfismo no trivial $\varphi : G \longrightarrow S_4$. Considerando el posible orden de la imagen y usando el primer teorema de isomorfía, obtenemos $|\mathrm{Ker}(\varphi)| = 3$ ó 9. En el último caso $n_3 = 1$ contra la hipótesis, así que $|\mathrm{Ker}(\varphi)| = 3$, y $H = \mathrm{Ker}(\varphi)$ es normal en G.
Si $n_3 = 4$, el homomorfismo φ nos permite estudiar con mas detalle la estructura de G: Obsérvese que $\mathrm{Im}(\varphi) \cong A_4$ y que A_4 contiene un único subgrupo normal V de orden 4, isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$. $K = \varphi^{-1}(V)$ es un subgrupo normal de G de orden 12. Además K contiene un subgrupo normal H de orden 3 y todos los 2-subgrupos de Sylow de G, que son isomorfos a V. Esto nos deja como únicas posibilidades $K \cong D_6$ ó $K \cong \mathbb{Z}_6 \times \mathbb{Z}_2$. Pero en el primer caso D_6 (y por tanto K) contiene un subgrupo característico de orden 6, que será normal en G (ya que K es normal en G), y su imagen bajo φ será un subgrupo normal de A_4 de orden 2. Pero A_4 no tiene subgrupos normales de orden 2, contradicción. Luego K es abeliano y tiene un único subgrupo de orden 4 que es el único 2-subgrupo de Sylow de G. En resumen: *Para todo grupo G de orden 36, ó $n_3 = 1$ ó $n_2 = 1$.*

Grupos de orden p^2q^2, p y q primos con $p < q$

Vamos a demostrar: *Todo grupo de orden p^2q^2 tiene un subgrupo de Sylow normal.* Si $n_q = 1$ ya está. En otro caso, $n_q \mid p^2$ y $n_q \equiv 1$ (mód q). Luego $q \mid (p-1)$ ó $q \mid (p+1)$. Lo primero es imposible porque $(p-1) < p < q$ y lo segundo sólo es posible si $q = p+1$. Como p y q son primos, es forzoso que $p = 2$ y $q = 3$. Pero este caso ya lo hemos tratado. Obsérvese que como en casos anteriores, si

3309-05.tex

$p \nmid (q^2-1)$ y $q \nmid (p^2-1)$, G es abeliano. Para este último caso existen exactamente cuatro grupos salvo isomorfismos con orden p^2q^2.

Grupos de orden 60

Vamos a ver cómo podemos utilizar los teoremas de Sylow para investigar la estructura de los grupos de un orden dado aunque para ese orden existan grupos simples. Obsérvense dos técnicas: Iremos cambiando de un primo a otro y usaremos inductivamente los resultados que hemos obtenido para grupos de orden menor que 60.

Teorema. 28.15.
Si $|G| = 60$ y G tiene mas de un 5-subgrupo de Sylow, entonces G es simple

DEMOSTRACIÓN. Supongamos que $|G| = 60$ y G tiene mas de un 5-subgrupo de Sylow, pero que existe $H \triangleleft G$ no trivial. Por el segundo teorema de Sylow, $n_5 = 6$. Sea $P \in \mathrm{Syl}_5(G)$. Entonces $|P| = 5$ y $|N_G(P)| = 10$.
Si $5 \mid |H|$ entonces H contiene un 5-subgrupo de Sylow y como es normal, los contiene a todos. En particular, $|H| \geq 1+6\cdot 4 = 25$ y la única posibilidad es $|H| = 30$. Pero antes hemos visto que cualquier grupo de orden 30 tiene un único 5-subgrupo de Sylow. Luego $5 \nmid |H|$ para todo subgrupo normal propio de G.
Si $|H| = 6$ ó 12, H tiene un subgrupo de Sylow normal (por tanto característico) que es también normal en G. Reemplazando H por este grupo nos hemos reducido al caso $|H| = 2$, 3 ó 4. Sea $\bar{G} = G/H$, así que $|\bar{G}| = 30$, 20 ó 15. En todos los casos, $\bar{G}$ tiene un subgrupo normal $\bar{P}$ de orden 5 por los resultados previos. Llamemos K a la preimagen de $\bar{P}$ en G, de forma que $K \triangleleft G$, $K \neq G$ y $5 \mid |K|$. Esto contradice el párrafo precedente. □

Corolario. 28.16.
A_5 es simple

DEMOSTRACIÓN. Los subgrupos $< (1\ 2\ 3\ 4\ 5\ ) >$ y $< (1\ 3\ 2\ 4\ 5) >$ son 5-subgrupos de Sylow distintos de A_5. □

Teorema. 28.17.
Si G es un grupo simple de orden 60, entonces $GcongA_5$

DEMOSTRACIÓN. Sea G un grupo simple de orden 60, sea $P \in \mathrm{Syl}_2(G)$ y sea $N = N_G(P)$, así que $[G:N] = n_2 = 3$, 5 ó 15.
En primer lugar, G no tiene ningún subgrupo propio H de índice menor que 5: Si H fuera un subgrupo de índice 4, 3 ó 2, considerando la acción por la izquierda de G sobre G/H obtendríamos un homomorfismo no trivial de G en S_n, $n = 4$, 3 ó 2, con núcleo K normal en G y distinto de G, así que $K = 1$. Pero 60 ($= |G|$) no divide a 4!. En particular, este argumento muestra que $n_2 \neq 3$.
Si $n_2 = 5$, entonces N tiene índice 5 en G, y la acción de G mediante multiplicación por la izquierda sobre G/N nos da un homomorfismo $G \longrightarrow S_5$. Como G es simple, el núcleo es 1 y G es isomorfo a un subgrupo de S_5. Identificamos G con éste subgrupo. Si $G \not\subset A_5$, entonces $GA_5 = S_5$ y por el segundo teorema de isomorfismo, $[G : G \cap A_5] = 2$ en contradicción con el párrafo anterior. Luego $G \subset A_5$ y contando órdenes, $G = A_5$ como queremos.
Finalmente sea $n_2 = 15$. Si para todo par $P, Q \in \mathrm{Syl}_2(G)$, $P \cap Q = 1$, entonces el número de elementos no identidad en todos ellos sería $(4-1)\cdot 15 = 45$. Pero $n_5 = 6$ y el número de elementos de G de orden 5 es $(5-1)\cdot 6 = 24$ y en total $|G| \geq 24+45 = 69$. Esta contradicción prueba que $\exists P, Q \in \mathrm{Syl}_2(G)$ con $|P \cap Q| = 2$. Sea $M = N_G(P \cap Q)$. Ya que P y Q son abelianos (tienen orden 4), $P \cap Q$ es normal en ambos y ambos son subgrupos de M. Por lo tanto $4 \mid |M|$. Aplicando el segundo teorema de Sylow a M, $n_2(M)$ es impar, es estrictamente mayor que 1 y divide a $|M|$. La única posibilidad es $|M| = 12$, $[G : M] = 5$ y el argumento del párrafo anterior con M en lugar de N nos da $G \cong A_5$. Esto nos lleva a una contradicción ya que $n_2(A_5) = 5$. □

Simplicidad de A_n

Teorema. 28.18. (Teorema de Abel)
A_n es simple para todo $n \geq 5$.

DEMOSTRACIÓN. Por inducción sobre n. Si $n = 5$, es el corolario demostrado en el último ejemplo de la sección anterior. Sea ahora $n > 5$ y supongamos el teorema cierto para $n-1$. Para $i = 1, \ldots, n$ sea $G_i = \{\sigma \in A_n \mid \sigma(i) = i\}$. Todos los G_i son conjugados entre sí e isomorfos a A_{n-1}, luego son simples. Sea H un subgrupo normal de A_n y consideramos $H \cap G_i triangleleft G_i$. Luego $H \cap G_i = 1$ ó $H \cap G_i = G_i$. En este último caso, $\forall j, \exists \sigma \in A_n$ tal que $H = \sigma H \sigma^{-1} \supset \sigma G_i \sigma^{-1} = G_j$, y $H \supseteq G_1 \vee \cdots \vee G_n = A_n$. Así que si $H \neq A_n$ ha de ser $\forall i, H \cap G_i = 1$. Supongamos que $H \neq 1$, y sea $\sigma \in H$, $\sigma \neq 1$. Descomponemos en ciclos disjuntos:

$$\sigma = (i_1\, i_2 \ldots)(\ldots)\ldots$$

Supongamos que algún ciclo (p.e. el primero) tiene una longitud mayor que dos, es decir que $\sigma(i_2) = i_3 \neq i_1$. Como $n > 5$, sean $i_4, i_5 \neq i_1, i_2, i_3$ y sea $\tau = (i_3\, i_4\, i_5) \in A_n$. Entonces $\tau\sigma\tau^{-1} \in H$ y $\tau\sigma\tau^{-1}(i_1) = i_2 = \sigma(i_1)$, $\tau\sigma\tau^{-1}(i_2) = i_4 \neq i_3 = \sigma(i_2)$ luego $1 \neq \sigma^{-1}\tau\sigma\tau^{-1} \in H$, $H \cap G_{i_1} \neq 1$, contradicción.
Así que en la descomposición anterior todos los ciclos tienen longitud 2, son disjuntos y mueven todo i. Como $n > 5$ será $\sigma = (i_1\, i_2)(i_3\, i_4)(i_5\, i_6)\ldots$. Sea ahora $\tau = (i_1\, i_2)(i_3\, i_5)$. Entonces $\tau\sigma\tau^{-1}\sigma^{-1} \neq 1$, $\tau\sigma\tau^{-1}\sigma^{-1}(i_1) = i_1$, otra vez contradicción. Luego $H = 1$ y A_n es simple. □

Resumen de técnicas

Como ya dijimos antes, la aplicación principal de los teoremas de Sylow es demostrar que para un n dado, todo grupo de orden n posee un subgrupo normal. Para los n pequeños muchas veces son suficientes las condiciones sobre n_p dadas por el segundo teorema de Sylow. Pero a veces es necesario un estudio mas fino. En esta sección resumimos algunas de las técnicas mas sencillas para mostrar la existencia de subgrupos normales de un grupo de orden dado.

Contar elementos

Sea G un grupo de orden n, sea p un primo divisor de n y sea $P \in \mathrm{Syl}_p(G)$. Si $|P| = p$, todo elemento no identidad de P tiene orden p y todo elemento de orden p está en algún conjugado de P. Por el teorema de Lagrange, conjugados distintos de P intersecan en la identidad, luego el número de elementos de orden p es $n_p(p-1)$.

Si los p-subgrupos de Sylow de G para diferentes primos p tienen orden primo y suponemos que ninguno de ellos es normal, puede ocurrir que el número total de elementos de orden primo sea mayor que $|G|$. Esta contradicción muestra que al menos uno de los n_p debe ser 1. Este es el argumento que hemos usado para mostrar que no hay grupos simples de orden 30.

A veces la cuenta de elementos de orden primo no produce demasiados elementos, pero quedan tan pocos elementos restantes que debe existir un subgrupo normal formado por ellos. Así se puede demostrar que en un grupo de orden 12, ó $n_2 = 1$ ó $n_3 = 1$. Esta técnica funciona especialmente bien cuando G tiene un p-subgrupo de Sylow P de orden p tal que $n_p = \frac{|G|}{p}$, por ejemplo $|G| = 56$ u 80.

Considerar subgrupos de índice pequeño

Recuérdese que si G tiene un subgrupo H de índice k, la acción por traslación sobre las clases por la izquierda G/H origina un homomorfismo $G \longrightarrow S_k$ cuyo núcleo está contenido en H. Si $k > 1$, este núcleo es un subgrupo normal de G distinto de G, y si G es simple debe ser la identidad. Entonces por el primer teorema de isomorfismo, $G \cong L < S_k$ y en particular, $|G| \mid k!$. Este argumento muestra que si k es el mínimo entero tal que $|G| \mid k!$ y G es un grupo finito simple, entonces G no contiene subgrupos de índice menor que k. En los ejemplos ese k es usualmente muy fácil de calcular: El mayor primo p que divide a $|G|$ aparece con exponente 1 ó 2, y $k = p$ ó $2p$, respectivamente. Hemos usado esta técnica en el segundo párrafo de la demostración del teorema 4 (G era un grupo simple de orden 60).

Representación por permutaciones

Este método es un refinamiento del anterior. Si G contiene un subgrupo H de orden k, obtenemos un homomorfismo $\varphi : G \longrightarrow S_k$ cuya imagen es un subgrupo transitivo y de las propiedades de $\mathrm{Im}(\varphi)$ deducimos propiedades de los elementos y los subgrupos de G. Por ejemplo, si G es simple y contiene un elemento o subgrupo de un orden particular, también debe contenerlo S_k. O bien: Si $P \in \mathrm{Syl}_p(G)$ y P es también un p-subgrupo de Sylow de S_k, entonces $|N_G(P)|$ divide a $|N_{S_k}(P)|$. Esta

condición es muy útil cuando p es un primo y $k = p$ ó $p+1$. Nosotros hemos utilizado este método en el estudio de los grupos de orden 60.

Una variante consiste en tomar un primo p tal que $n_p \neq 1$ y considerar la acción por conjugación sobre $S = \mathrm{Syl}_p(G)$. Obtenemos ahora un homomorfismo $\varphi : G \longrightarrow S_{n_p}$ y estudiamos la existencia de un subgrupo normal ($\mathrm{Ker}(\varphi)$) y las propiedades de $\mathrm{Im}(\varphi)$. Hemos utilizado esta técnica con los grupos de orden 12, 24 y 36. También es aplicable a las grupos de orden 48, 72 y 96.

A veces se puede mejorar un poquito este método trabajando en A_k en lugar de S_k.

Considerar p-subgrupos para primos p distintos

Sean p y q dos primos distintos tales que todo grupo de orden pq es cíclico. Esto es equivalente a $p < q$ y $p \nmid (q-1)$. Si G tiene un q-subgrupo de Sylow Q de orden q y $p \mid |N_G(Q)|$, por el teorema de Cauchy obtenemos $P < N_G(Q)$, $|P| = p$ (nótese que P no tiene que ser un p-subgrupo de Sylow de G). Así PQ es un subgrupo, es abeliano, está contenido en $N_G(P)$ y por tanto $q \mid |N_G(P)|$. Esta información numérica puede ser suficiente para mostrar que $N_G(P) = G$, es decir, $P \triangleleft G$, o al menos para forzar que $[G : N_G(P)]$ sea menor que el índice mínimo permitido por la representación por permutaciones.

Se puede refinar este método no requiriendo que P y Q sean de orden primo: Si p y q son primos distintos que dividen a $|G|$ y tales que $Q \in \mathrm{Syl}_q(G)$ y $p \mid |N_G(Q)|$, sea $P \in \mathrm{Syl}_p(N_G(Q))$. Podemos aplicar los teoremas de Sylow en $N_G(Q)$ para ver que $P \triangleleft N_G(Q)$ y forzar que $N_G(P)$ tenga índice pequeño. Si además P es un p-subgrupo de Sylow de G, podemos usar el segundo teorema de Sylow para restringir mas los posibles valores de $|N_G(P)|$. Por otra parte, si P no es un p-subgrupo de Sylow de G, $P < P_1 \in \mathrm{Syl}_p(G)$ y en este caso, $P \lneq N_{P_1}(P)$. Luego $N_G(P)$ (que contiene a $N_{P_1}(P)$) tiene orden divisible por una potencia de p estrictamente mayor que $|P|$, y además es divisible por $|Q|$.

Normalizadores de intersecciones de p-subgrupos de Sylow

Si $P \in \mathrm{Syl}_p(G)$ y $|P| = p^i$, $i \geq 2$, entonces los conjugados distintos de P puede que intersecten en subgrupos no triviales y no podemos usar el argumento de contar elementos. Sea $R \in \mathrm{Syl}_p(G)$ con $R \neq P$ y $P_0 = P \cap R \neq 1$. Entonces $P_0 \lneq P$, $P_0 \lneq R$ luego $P_0 \lneq N_P(P_0)$ y $P_0 \lneq N_R(P_0)$. Se puede usar esto para demostrar que el normalizador de P_0 en G es suficientemente grande.

Este método funciona especialmente bien cuando $|P| = p^a$ y $|P_0| = p^{a-1}$. En este caso $P_0 \triangleleft P$, $P_0 \triangleleft R$, luego $P,R < N_G(P_0) = N$, y N tiene dos p-subgrupos de Sylow distintos. Por el segundo teorema de Sylow, $|N| = p^a k$ donde $k > p+1$. Hemos usado esta forma de encontrar subgrupos en el último párrafo de la demostración del teorema 4 (en los grupos de orden 60).

Recapitulando: Si para cada P, $R \in \mathrm{Syl}_p(G)$ se tiene $P \cap R = 1$, aplicamos el argumento de contar elementos de orden potencia de p. En otro caso, existe una intersección de p-subgrupos de Sylow cuyo normalizador es "grande". Para algunos ordenes de grupo no podemos decidir cual de las dos situaciones se produce, pero podemos dividir el argumento en dos casos y deducir la existencia de un subgrupo normal en cada uno de ellos. Vamos a establecer ahora una condición suficiente para tener una intersección grande:

Lema. 28.19.
Sea G un grupo finito y p un primo tales que $n_p \not\equiv 1 \pmod{p^2}$. Entonces existen $P,R \in \mathrm{Syl}_p(G)$ tales que $[P : P \cap R] = p$, y por tanto $P \cap R \triangleleft P$.

DEMOSTRACIÓN. El argumento es un refinamiento de la demostración de la congruencia en el segundo teorema de Sylow: Hagamos actuar a P sobre $S = \mathrm{Syl}_p(G)$ por conjugación. Consideramos la fórmula de descomposición en órbitas:

$$|S| = \sum [P : \mathrm{Stab}_P(Q)] = \sum [P : P \cap Q]$$

Como en la demostración del segundo teorema de Sylow,

$$[P : \mathrm{Stab}_P(Q)] = [P : P \cap Q] = 1 \Leftrightarrow P = Q$$

y todos los demás índices son potencias positivas de p. Si todos ellos fuesen divisibles por p^2, sería $n_p = |S| \equiv 1 \pmod{p^2}$, en contradicción con la hipótesis. Luego existe un R tal que $[P : P \cap R] = p = [R : P \cap R]$ lo que implica $P \cap R \triangleleft P$ y $P \cap R \triangleleft R$. □

Grupos: Clases conjugadas

Automorfismos internos

Dado un grupo G y un elemento $a \in G$, "conjugación por a" es la aplicación $\gamma_a : G \to G$ definida por $\gamma_a(x) = axa^{-1}$

Lema. 28.20.
(1) γ_a *es un automorfismo de* G.
(2) $\gamma_{ab} = \gamma_a\gamma_b$; $\gamma_1 = 1_G$.

DEMOSTRACIÓN.
(1) $\gamma_a(xy) = a(xy)a^{-1} = axa^{-1}axa^{-1} = \gamma_a(x)\gamma_a(y)$ luego γ_a es un homomorfismo. Por otra parte $\gamma_a(x) = axa^{-1} = 1$ si y sólo si $x = a^{-1}a = 1$. Luego γ_a es inyectiva. Para todo $y \in G$ sea $x = a^{-1}ya$. Entonces $\gamma_a(x) = y$ y γ_a es sobre.
(2) $\gamma_a\gamma_b(x) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = \gamma_{ab}(x)$

□

El automorfismo $\gamma_a : G \to G$ se llama **automorfismo interno** definido por a.
Definimos una aplicación $\gamma : G \longrightarrow \mathrm{Aut}(G)$ por $\gamma(a) = \gamma_a$. Entonces $\gamma(ab) = \gamma_a\gamma_b$ y por tanto γ es un homomorfismo. El núcleo de γ consta de los elementos $a \in G$ tales que axa^{-1} para todo $x \in G$. Es decir que $\ker(\gamma) = Z(G)$. La imagen es un subgrupo de $\mathrm{Aut}(G)$ que denotamos $\mathrm{Int}(G)$ y llamamos **grupo de automorfismos internos** de G. Por el primer teorema de isomorfismo $\mathrm{Int}(G) \cong G/Z(G)$.

Lema. 28.21.
Para cualquier grupo G, $\mathrm{Int}(G)$ *es un subgrupo normal de* $\mathrm{Aut}(G)$.

DEMOSTRACIÓN. Para todo $f \in \mathrm{Aut}(G)$, para todo $\gamma_a \in \mathrm{Int}(G)$ y para todo $g \in G$ calculamos:

$$(f\gamma_a f^{-1})(g) = f(\gamma_a(f^{-1}(g))) = f(af^{-1}(g)a^{-1}) = f(a)gf(a)^{-1} = \gamma_{f(a)}(g)$$

luego $f\gamma_a f^{-1} = \gamma_{f(a)}$. □

El grupo cociente $\mathrm{Aut}(G)/\mathrm{Int}(G)$ se llama **grupo de clases de automorfismos** de G o también **grupo de los automorfismos externos** de G.
Podemos formar la sucesión exacta de grupos y homomorfismos:

$$1 \longrightarrow Z(G) \longrightarrow G \longrightarrow \mathrm{Aut}(G) \longrightarrow \frac{\mathrm{Aut}(G)}{\mathrm{Int}(G)} \longrightarrow 1$$

3309-06.tex

Holomorfismos de un grupo

El grupo $A = \mathrm{Aut}(G)$ es un subgrupo del grupo $P(G)$ de permutaciones del conjunto G. Ahora bien, $P(G)$ contiene otros dos subgrupos interesantes: El grupo $R = R(G)$ de **traslaciones por la derecha** y el grupo $L = L(G)$ de **traslaciones por la izquierda** (ver ejemplos de "Grupos de operadores"). Consideremos el primero. Por el Lema (28.21.), $\sigma\rho_a\sigma^{-1} = \rho_{sigma_a}$ para todo $\sigma \in \mathrm{Aut}(G)$ y por tanto $RA = AR$ es un subgrupo de $P(G)$ generado por R y A.
Denotamos para cualquier $a \in G$:

- La traslación por la derecha por a como $\rho_a : G \to G$ dada por $\rho_a(x) = xa$.
- La traslación por la izquierda por a como $\lambda_a : G \to G$ dada por $\lambda_a(x) = ax$.
- La conjugación por a como $\gamma_a : G \to G$ dada por $\gamma_a(x) = axa^{-1}$.

El grupo $RA = AR$ se llama **holomorfo** del grupo G y se denota por $H = \mathrm{Hol}(G)$. Sus elementos se llaman **holomorfismos** del grupo G.
Para todo $a \in G$ se verifica que $\lambda_a = \gamma_a\rho_a$, toda traslación por la izquierda pertenece a H, y por tanto el grupo L está contenido en H. La relación precisa entre H, L, R y A viene dada por el siguiente teorema:

Teorema. 28.22.
Sea G un grupo arbitrario. Entonces:
(1) R y L son cada uno el centralizador del otro en $P(G)$.
(2) $H = AR$ es el normalizador de R en $P(G)$
(3) A es el estabilizador de $1 \in G$ en la acción de H sobre G.

DEMOSTRACIÓN. Supongamos que $\tau \in P(G)$ conmuta con todo elemento de R, o sea $\tau\rho_a = \rho_a\tau$. Así que para cualesquiera $x, a \in G$ se verifica $\tau(xa) = \tau(x)a$. Tomando $x = 1$ y $b = \tau(1)$ obtenemos $\tau(a) = ba$ para todo $a \in G$, y $\tau = \lambda_b \in L$. A la inversa, es inmediato que para cualesquiera $a, b \in G$ se verifica $\rho_a\lambda_b = \lambda_b\rho_a$. Por tanto L es el centralizador de R en $P(G)$. la otra mitad se demuestra simétricamente. Llamemos N al normalizador de R en $P(G)$. Ya que para todo $\sigma \in \mathrm{Aut}(G)$ se verifica $\sigma\rho_a\sigma^{-1} = \rho_{\sigma(a)}$ obtenemos que $H \subset N$. □

Vamos a caracterizar directamente los elementos de $\mathrm{Hol}(G)$:

Teorema. 28.23.
Sea $f \in P(G)$ una biyección. Entonces $f \in \mathrm{Hol}(G)$ si, y sólo si, tiene la siguiente propiedad: Para cualesquiera $x, y, z \in G$ se verifica $f(xy^{-1}z) = f(x)f(y)^{-1}f(z)$.

DEMOSTRACIÓN. Sea $f \in \mathrm{Hol}(G)$. Entonces $f = \rho_a\sigma$ con $\rho_a \in R(G)$ y $\sigma \in \mathrm{Aut}(G)$. Calculamos: $f(xy^{-1}z) = \rho_a\sigma(xy^{-1}z) = \rho_a(\sigma(x))(\rho_a\sigma(y))^{-1}\rho_a\sigma(z)$.

A la inversa supongamos que $f(xyz) = f(x)f(y)^{-1}f(z)$. Sea $a = f(1)$. Un sencillo cálculo muestra que $\sigma = \rho_a^{-1}f$ es un automorfismo de G y por tanto $f = \rho_a\sigma \in H$. □

Diagrama de inclusiones

En todo grupo G existe otra aplicación interesante: $\sigma_{-1} : G \to G$ definida por $\sigma_{-1}(x) = x^{-1}$. Esta σ_{-1} es un automorfismo si y sólo si G es abeliano. Pero en el caso general tiene algunas propiedades interesantes:

Lema. 28.24.
(1) $\sigma_{-1}^2 = 1_G$. *En particular,* σ_{-1} *es una biyección.*
(2) Para todo automorfismo $\sigma \in \mathrm{Aut}(G)$ *se verifica* $\sigma_{-1}\sigma\sigma_{-1} = \sigma$, *así que* σ_{-1} *pertenece al centralizador de* $\mathrm{Aut}(G)$ *en* $P(G)$.
(3) Para toda traslación por la izquierda $\lambda_a \in L$ *se verifica* $\sigma_{-1}\lambda_a\sigma_{-1} = \rho_{a^{-1}}$, *así que* σ_{-1} *intercambia las traslaciones a la izquierda y a la derecha. Luego pertenece al normalizador de* $\mathrm{Hol}(G)$ *en* $P(G)$.

Vamos a considerar cómo es el subretículo de los subgrupos de $P(G)$ descritos en los párrafos anteriores: L es el grupo de traslaciones por la izquierda, R las traslaciones por la derecha y $Z = L \cap R \cong Z(G)$ es el grupo de las traslaciones por elementos del centro de G. LR es el compuesto de ambos. Obsérvese que L, R y $LR = RL$ son normales en $\mathrm{Hol}(G)$ y que

$$\frac{\mathrm{Hol}(G)}{LR} \cong \frac{\mathrm{Aut}(G)}{\mathrm{Int}(G)}$$

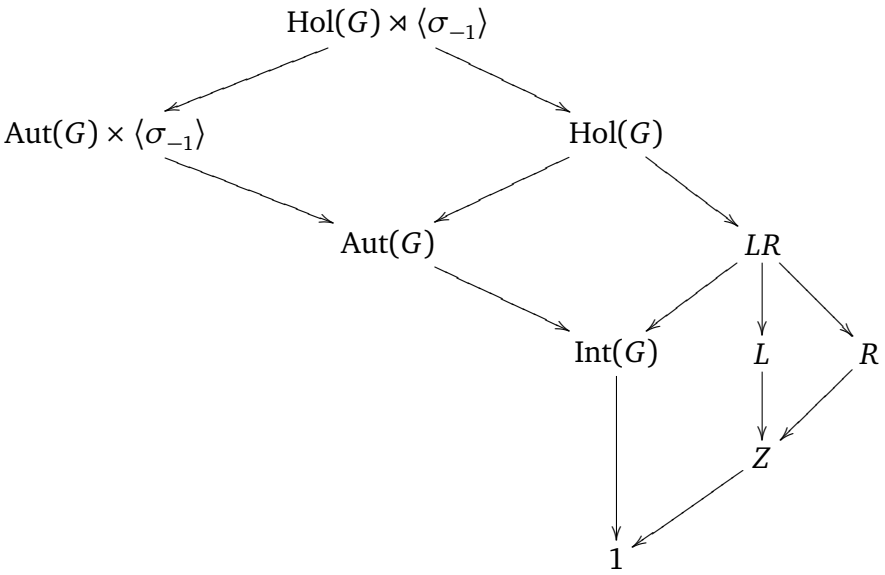
Por otra parte, L y R son conjugados en $\mathrm{Hol}(G) \rtimes \langle\sigma_{-1}\rangle$.

Otro grupo interesante no reflejado en el diagrama es

$$T = \{\sigma \in \mathrm{Aut}(G) \mid \ \forall x \in G\, x \sim \sigma(x)\}$$

Se verifica $\mathrm{Int}(G) \subset T \lhd \mathrm{Aut}(G)$. Ya sabemos que $\mathrm{Hol}(G) = L \rtimes \mathrm{Aut}(G) = R \rtimes \mathrm{Aut}(G)$

El diagrama de inclusiones es el siguiente:



Sea $\sigma \in \mathrm{Aut}(G)$ de orden finito n y sea $m = |G|$

Lema. 28.25.
El grupo $L \rtimes \langle \sigma \rangle$ tiene orden nm.

Ejercicios propuestos

Ejercicio. 28.26.
Determinar, salvo isomorfismo, todos los grupos de orden 12.
Ref.: 3309e_001 *SOLUCIÓN*

Ejercicio. 28.27.
Prueba que Q_2 no es un producto semidirecto de dos subgrupos no triviales.
Ref.: 3309e_000 *SOLUCIÓN*

3309-09.tex

Bibliografía

[1] R. B. J. T. Allenby, *Rings, fields and groups. An introduction to abstract algebra*, Arnold, 1983.

[2] E. Artin, *Geometric algebra*, Wiley, 1957. 10

[3] M. Artin, *Algebra*, Prentice Hall, 1991.

[4] J. A. Beachy and W. D. Blair, *Abstract algebra, 2nd ed.*, Waveland Press, 1996.

[5] P. M. Cohn, *Algebra I*, John Wiley, 1974. 10

[6] _____, *Algebra II*, John Wiley, 1977.

[7] _____, *Basic algebra*, Springer, 2003.

[8] D. S. Dummit and R. M. Foote, *Abstract algebra*, Prentice Hall, 1991.

[9] _____, *Abstract algebra. 3rd ed.*, Wiley, 2004.

[10] J. D. Fraleigh, *A first course in abstract algebra*, Addison–Wesley, 1967.

[11] T. W. Hungerford, *Algebra*, Springer–Verlag, 1974.

[12] N. Jacobson, *Lectures in abstract algebra. III. Theory of fields and Galois theory*, Springer Verlag, 1964.

[13] _____, *Basic algebra I*, Freeman, 1974.

[14] _____, *Basic algebra i. 2nd. ed.*, Freeman, 1985.

[15] _____, *Basic algebra II. 2nd ed.*, Freeman, 1989.

[16] I. Kaplansky, *Fields and rings*, Chicago Univ. Press, 1972.

[17] J. P. Lafon, *Algèbre commutative: Languages géometrique et algébrique*, Collection enseignement des sciences, 24, Hermann, Paris, 1977.

[18] S. Lang, *Algebra*, Aguilar, 1971.

[19] _____, *Algebra 3rd. ed.*, Springer, 2002.

[20] S. MacLane and G. Birkhoff, *Algèbre I. Structures fondamentales. II. Les grands théorèmes*, Gauthier–Villar, 1971.

[21] S. MacLane and G. Birkhoff, *Algebra*, Macmillan, 1979.

[22] P. J. McCarthy, *Algebraic extensions of fields*, Chelsea, 1976.

[23] J. J. Rotman, *The theory of groups. An introduction*, Allyn and Bacon, 1973.

[24] L. Rowen, *Graduate Algebra: Commutative view*, Graduate Studies in Mathematics, 73, Graduate Studies in Math., 73. Amer. Math. Soc., 2006.

[25] J. Scherk, *Algebra. A computational introduction*, Chapman–Hall, 2000.

[26] L. E. Sigler, *Algebra*, Reverté, 1981.

[27] I. Stewart, *Galois theory*, Chapman and Hall, 1973.

[28] B. L. van der Waerden, *Algebra i*, Frederick Ungar Publ. Co., 1970.

Índice alfabético

G–conjunto, 176
G–conjunto a izquierda, 174
G–conjunto pprimitivo, 178
G–conjuntos equivalentes, 176
G–conjuntos isomorfos, 176
G–subconjunto, 176
H_G, 176
i-ésimo centro de un grupo, 49
i-ésimo subgrupo conmutador, 53
i-ésimo subgrupo derivado, 53
p–grupo, 187
p-subgrupo, 187
p-subgrupo de Sylow, 191
órbita de una acción, 177

acción, 174
    primitiva, 178
    transitiva, 177
acción k–mente transitiva, 206
acción a la izquierda, 174
acción efectiva, 176
acción fiel, 176
acción por automorfismos, 218
acción por conjugación, 175, 180
acción por traslaciones a la izquierda, 175, 180
acción sobre por conjugación sobre subgrupos, 175
acción transitiva, 177
acción trivial, 174
automorfismo
    interno, 65, 238
automorfismo interior, 176

bloque, 178
bloque de imprimitividad, 178
bloque impropio, 178

centralizador, 195
centralizador de un elemento, 180
centralizador de un subconjunto, 50
centro de un grupo, 49, 176, 180
ciclo, 13
clase a la izquierda, 19
clase conjugada, 195
clase de conjugación, 180
componente p–primaria, 194
composición, 44
congruencia, 178
conjunto de generadores, 18, 89
conjunto de relaciones de definición, 136
conmutador de dos elementos, 52, 154

diedros regulares, 95
dominio de operadores, 174

elemento
    cero, 8
    inverso, 8
    neutro, 5, 6
    neutro a la derecha, 7
    opuesto, 8
    orden de un —, 18
    simétrico, 6
    simétrico a la derecha, 7
    uno, 8
epimorfismo, 39
estabilizador de un elemento, 179

factores de composición, 148
finitamente presentado, 136
función tociente de Euler, 57

grupo, 6
    cíclico, 18

abelianizado, 154
abeliano, 6
automorfismos externos, 238
automorfismos internos, 238
centro de un —, 30
clases de automorfismos, 238
cociente, 42
conmutativo, 6
cuaternio, 28
de los cuaternios, 28
exponente de un —, 28
factor, 165
factores de composición de un —, 151
finitamente generado, 18
finito, 11
infinito, 11
longitud derivada de un —, 155
orden de un —, 11
simétrico, 13
simple, 148
soluble, 152
grupo abelianizado, 52
grupo cuasidiédrico, 107
grupo cuaternio, 97
grupo de isotropía, 179
grupo de Klein abstracto, 89
grupo de los cuaternios, 97
grupo de transformaciones, 175
grupo diédrico generalizado, 221
grupo diédrico infinito, 221
grupo dicíclico, 108, 222
grupo libre, 130, 131
grupo lineal especial, 97
grupo lineal general, 96
grupo metacíclico, 223
grupo modular, 108
grupo producto directo, 165
grupo semidiédrico, 107
grupo unimodular, 97
grupos dicíclicos, 106

hipercentro de un grupo, 50
hiperconmutador de un grupo, 53
holomorfismo, 239
holomorfo de un grupo, 221, 222, 239
holomorfo de un grupo relativo a un subgrupo, 221
homomorfismo de G-conjuntos, 176
homomorfismo de grupos, 37

imagen de un homomorfismo, 38
imagen de un subconjunto, 38
imagen inversa de un subconjunto, 38
isometría, 87
isomorfismo, 39

Lema de la mariposa, 48
Lema de Zassenhaus, 48
Ley modular, 48

matriz
ortogonal, 64
matriz triangular superior estricta, 210
monoide, 5
monomorfismo, 39

núcleo de la acción, 175
núcleo de un homomorfismo, 38
núcleo definidor, 135
normalizador de un subconjunto, 50

operación
binaria, 5

partición en bloques, 178
permutación, 13
cíclica, 13
longitud de una —, 14
permutación par, 60
permutaciones
disjuntas, 14
permutaciones del mismo tipo, 203
presentación de un grupo, 89
producto, 8
producto directo, 162, 163, 165
producto directo interno, 47, 166, 167
producto semidirecto, 218
propiedad

asociativa, 5, 6
cancelativa, 8
conmutativa, 6
proyecciones canónicas
del producto directo, 165

rango, 134
Regla de Dedekind, 47
relación compatible, 178
relación de equivalencia
compatible, 41
relaciones de un grupo, 89
representación por permutaciones, 175
representación regular por la izquierda, 195
representaciones lineales, 97
restricción de la acción, 174

sólidos platónicos, 94
serie de composición, 148
serie derivada de un grupo, 155
serie normal, 147
abeliana, 152
factores, 147
longitud, 147
propia, 147
refinamiento, 147
refinamiento propio, 148
soluble, 152
términos, 147
series normales
equivalentes, 150
sistema de generadores, 18
sistema de generadores libre, 130
sistemas de generadores, 136
subgrupo, 16
índice de un —, 19
conjugado, 41
conmutador, 154
derivado, 154
generado, 18
impropio, 16
propio, 16
puntos fijos, 64
total, 16
trivial, 16
subgrupo alternado, 60
subgrupo característico, 49
subgrupo complemento, 221
subgrupo conmutador, 52, 53
subgrupo de torsión, 113
subgrupo derivado, 52
subgrupo normal, 41
subgrupo totalmente invariante, 49, 211
subgrupo transitivo, 204
suma, 8

Teorema
Lagrange, 19
Teorema de Dyck, 90
teorema de Nielsen-Schreier, 135
Teorema del doble cociente, 46
Teorema del paralelogramo, 46
transversal, 195
traslaciones
por la derecha, 239
por la izquierda, 239
trasposición, 15