UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA
ESCUELA DE MATEMÁTICA

Tesis:

"Clasificación y estructura de grupos finitos con apoyo del recurso computacional *GAP* (Groups, Algorithms, Programming)"

Presentado por:
Mario Alexis Ruiz Mejia

Para optar al grado de:
Licenciado en Matemática

Ciudad Universitaria, Septiembre de 2013

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA
ESCUELA DE MATEMÁTICA

Tesis:

"Clasificación y estructura de grupos finitos con apoyo del recurso computacional *GAP* (Groups, Algorithms, Programming)"

Presentado por:
Mario Alexis Ruiz Mejia

Para optar al grado de:
Licenciado en Matemática

Ciudad Universitaria, Septiembre de 2013

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA
ESCUELA DE MATEMÁTICA

Tesis:

"Clasificación y estructura de grupos finitos con apoyo del recurso computacional *GAP* (Groups, Algorithms, Programming)"

Presentado por:
Mario Alexis Ruiz Mejia

Asesor:
M.Sc. Ingrid Carolina Martínez Barahona

Ciudad Universitaria, Septiembre de 2013

AUTORIDADES

Rector Universitario:
Ing. Mario Roberto Nieto Lovo

Secretaria General:
Dra. Ana Leticia Zavaleta de Amaya

Fiscal General:
Lic. Francisco Cruz Letona

FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA

Decano:
M.Sc. Martín Enrique Guerra Cáceres

Secretario:
Lic. Carlos Quintanilla

ESCUELA DE MATEMÁTICA

Director:
Dr. José Nerys Funes Torres

Secretaria:
M.Sc. Alba Idalia Córdova Cuéllar

Ciudad Universitaria, Septiembre de 2013

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA
ESCUELA DE MATEMÁTICA

Asesor:
M.Sc. Ingrid Carolina Martínez Barahona

Ciudad Universitaria, Septiembre de 2013

Índice general

Introducción

La presente memoria se desarrolla dentro del marco de la Teoría de Grupos Finitos; concretamente se estudia la relación existente entre la estructura de un grupo y los tamaños de las órbitas de conjugación de sus elementos. Estudiar el orden de un grupo es una forma clásica para obtener información sobre las propiedades estructurales de él. En los últimos años se han abierto nuevas líneas de investigación que dan cabida al estudio estructural del grupo a partir de los tamaños de ciertos tipos subconjuntos: subgrupos, subgrupos cíclicos, subgrupos normales, órbitas, p-subgrupos de Sylow, normalizadores, estabilizadores, centralizadores, entre otros. Un área poco investigada, con aplicaciones en el propio campo, otras áreas de la matemática y ciencias.

La teoría de grupos tiene su origen en el trabajo de E. Galois [1] sobre solubilidad por radicales de la ecuación $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$. Sin embargo, algunos de los resultados de la teoría de grupos habían aparecido con anterioridad en trabajos de otros matemáticos, entre los que entra Cauchy [2]. Hoy en día, la teoría de grupos es una de las áreas de la matemática que más aplicaciones tiene. Éstas van desde las ciencias exactas hasta la música. En las ciencias exactas, las aplicaciones incluyen áreas tales como geometría algebraica, teoría de números, teoría de grafos y topología algebraica; además el estudio de los grupos especialmente finitos aparece en diversas áreas de las ciencias como: en física y química, su aplicación tiene lugar en el estudio de simetrías de las estructuras moleculares, una interesante aplicación de esta teoría puede encontrarse en [3].

Enmarcando este estudio, la teoría de grupos de orden finito es un área de la matemática con una rica historia, la cual se fundamenta en el trabajo de muchos grandes matemáticos. De acuerdo con William Burnside, la teoría de grupos finitos tuvo sus orígenes en los intentos del matemático francés A. I. Cauchy (1789-1857), quien en 1815 empezó en forma consistente la teoría de permutaciones, la cual desarrolló después de 1846 en la teoría de grupos de permutaciones, como matemático finalmente empezó a resumir los conceptos originales de grupos teóricos el cual fue legado de Cauchy y el joven matemático E. Galois (1811-1832). Sobre las bases de Cauchy y Galois podemos empezar a estudiar los grupos finitos, este campo de estudio que fue rápidamente estructurado, con importantes contribuciones al matemático Noruego L. Sylow (1832-1918), y del matemático Alemán L. Kronecker (1823-1891). Con una publicación en 1878 de los escritos sobre la teoría de grupos del matemático inglés A. Cayley (1821-1895), la teoría de grupos fue considerada un campo de las matemáticas independiente y auto sostenido. En las décadas pasadas, la clasificación de todos los grupos finitos llevó a muy grandes investigaciones. En la actualidad, ésta es la meta de esta teoría.

Para clasificar todos los grupos finitos de orden n, es necesario producir una lista de todos los grupos no isomorfos de orden n, posteriormente hacer un poco de trabajo extra y determinar sus tablas de grupo. Sin embargo, los grupos teóricos han sido determinados como estructuras de grupos

en el mayor de los casos probando que el grupo es isomorfo a otro grupo o clase de grupos, la cual es más común o conocida.

En esta investigación se pretenden estudiar la mayoría de los grupos abstractos de orden menor que cien.Se parte del orden del grupo para estudiar las propiedades estructurales y la descomposición en productos directos o semidirectos, con el objetivo de clasificar y listar los grupos esencialmente diferentes (salvo isomorfismos). Este esfuerzo se hace desde dos perspectivas: teórica y computacional.

Los primeros tres capítulos de este trabajo están dedicados a la clasificación teórica de los grupos de orden finito, específicamente en los casos que el orden sea un número primo, el producto de dos números primos diferentes o iguales.

Específicamente: en el Capítulo 1, se definen los conceptos básicos, se enuncian y demuestran sólo algunos teoremas clásicos de la teoría de grupos que serán referidos en el desarrollo de los capítulos posteriores.

El Capítulo 2, expone la descomposición de un grupo como producto directo o semidirecto de subgrupos y la ecuación de clase, con el propósito de dar una demostración combinatoria de los teoremas de Sylow, que son herramientas fundamentales para el propósito de este estudio.

En el Capítulo 3, se clasifican algunos grupos finitos de forma general, el estudio de las órbitas de conjugación se simplifica significativamente cuando se aplican los teoremas de Sylow, esta técnica se expone detalladamente en la clasificación de grupos de orden pq, con p y q números primos distintos.

El Capítulo 4, describe el uso del programa GAP (Groups, Algorithms, Programming) para trabajar con la estructura abstracta de grupo, y lograr clasificar a los grupos finitos mediante el método computacional. Ahí se evidencia la ventaja de contar con esta herramienta al momento de trabajar con grupos, subgrupos, acciones de grupo, homomorfismos, clases laterales, etc. El capítulo finaliza resolviendo el cubo de Rubik de dimensiones $2 \times 2 \times 2$, como aplicación concreta en GAP de los conceptos y teoría desarrollados en los capítulos previos.

El estudio se completa con los dos apéndices: en el Apéndice A, se ha programado un algoritmo en GAP que al ejecutarlo genera una lista con la estructura de todos los grupos de orden menor o igual a cien que no son isomorfos entre sí. Tener esta lista es de mucha utilidad pues permite acceder rápidamente a esta información, y así, omitir el largo tiempo de espera al momento de ejecutarlo. El propósito del Apéndice B es auxiliar al lector la comprensión de las notaciones y conceptos teóricos utilizados en la lista construida en el Apéndice A, para lograr una lectura más cómoda y fluída de la información provista.

Finalmente, esta obra puede ser leída por estudiantes de un primer curso de Álgebra Abstracta, pues su contenido es fácilmente comprendido por estudiantes de matemática de los primeros semestres de licenciatura. Por esta razón se espera sea un recurso bibliográfico de apoyo y consulta para los estudiantes que quieran profundizar e involucrarse en estos tópicos.

Capítulo 1

Teoría elemental de grupos: definiciones y resultados

1.1. Introducción

La estructura de grupo es una de las más comunes en toda la matemática pues aparece en forma natural en muchas situaciones, donde se puede definir una operación sobre un conjunto. Por ser tan simple en su definición, el concepto de grupo se puede considerar como punto de partida para el estudio de otras estructuras algebraicas más complicadas.

Muchos objetos matemáticos provenientes de áreas tan disímiles como Geometría Analítica, Combinatoria, Análisis Complejo, Topología, etc, tienen incorporados la estructura de grupo, aunque esto pase desapercibido para muchos de nosotros. Existen grupos finitos de cualquier tamaño, grandes o pequeños; de estructura muy simple, como los grupos cíclicos o bastantes complicados, como los grupos de simetrías; grupos infinitos con uno o varios generadores, o bien infinitos sin una base finita.

También se pueden crear nuevos grupos, usando los anteriores, por medio de ciertas operaciones entre ellos. Esto, por supuesto, puede hacer pensar al lector que el estudio de la teoría de grupos es una tarea abrumadora, dada la gran cantidad de grupos que intervienen.

Sin embargo existe una relación muy útil que podemos construir entre dos grupos, lo cual permite comparar la estructura de ambos sin hacer consideraciones acerca de la naturaleza misma de los elementos. Este concepto, que juega un papel central dentro de toda esta teoría, es el de isomorfismo de grupos. Si dos grupos son isomorficos, entonces desde el punto de vista del álgebra son casi iguales: esto es, poseen la misma estructura.

Los grupos aparecieron un poco tarde en la historia de las matemáticas, aproximadamente a mediados del siglo XIX.

El concepto de operación binaria o ley de composición interna aparece por vez primera en la obra del matemático alemán C. F. Gauss en relación a un trabajo sobre composición de formas cuadráticas del tipo:

$$f(x, y) = ax^2 + bxy + cy^2$$

con coeficientes enteros.

Gauss da una definición de equivalencia de formas cuadráticas, y luego define una operación de multiplicación de formas, y posteriormente demuestra que esta multiplicación es compatible con la relación de equivalencia.

También Gauss y algunos de sus predecesores en el campo de Teoría de Números, como Euler y Lagrange habían estudiado las propiedades de suma y multiplicación de los enteros módulo p, con p primo.

Pero fue el genio de Evariste Galois quien dio inicio a la moderna teoría de grupos, al exponer en sus brillantes trabajos la relación entre las ecuaciones algebraicas y el grupo de permutaciones de las raíces. Galois fue el primero que destacó la importancia de los subgrupos normales y estudió en detalle las propiedades abstractas de los grupos.

La definición general de grupo, fue dada por Cayley en 1854. Pero es a partir de 1880 cuando comienza a desarrollarse la teoría general de los grupos finitos con los trabajos de S. Lie, Felix Klein y Henry Poincaré.

1.2. Grupos

Definición 1.1 Un **grupo** es un conjunto no vacío G en donde hay definida una operación binaria $\cdot$, llamada producto, la cual satisface:

1. $a \cdot b \in G$ para todo $a, b \in G$.
2. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para todo $a, b, c \in G$ (Ley Asociativa).
3. Existe un elemento $e \in G$, llamado elemento neutro o identidad de la operación, el cual satisface: $a \cdot e = e \cdot a = a$, para todo $a \in G$.
4. Para todo a en G, existe un elemento $a^{-1} \in G$, llamado el inverso de a, el cual satisface: $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Definición 1.2 Si el conjunto G es finito, entonces G se dice **grupo finito**. Caso contrario, diremos que G es infinito.

Definición 1.3 El orden de grupo es el cardinal del conjunto G.

Notación: Usamos la notación de potencias en G.

$$\begin{aligned} e &= a^0 \\ a &= a^1 \\ a^2 &= a \cdot a \\ &\vdots \\ a^{n+1} &= a^n \cdot a \end{aligned}$$

Definición 1.4 Un grupo G se dice **abeliano** o **conmutativo**, si $a \cdot b = b \cdot a$ para todo $a, b \in G$.

1.3. Teorema de Lagrange

Introducción

En este capítulo estudiaremos uno de los teoremas más importantes de toda la teoría de grupos: el Teorema de Lagrange. Daremos en primer lugar una serie de resultados básicos que se derivan de la definición de grupo, para posteriormente introducir el concepto de subgrupo y en especial se estudiar las propiedades de los grupos ciclícos.

Si H es un subgrupo de un grupo finito G, entonces el Teorema de Lagrange establece que el orden de H es un divisor del orden de G. Este resultado genera una serie de propiedades interesantes en los grupos finitos de tipo estructural. Finalizamos el capítulo con el estudio de las clases laterales de un subgrupo H de G.

Resultados preliminares

En esta sección demostramos algunos hechos básicos sobre grupos, que se deducen a partir de la definición.

Lema 1.5 Si G es un grupo entonces

1. El elemento identidad es único.
2. Todo $a \in G$ tiene un inverso único en G.
3. Para todo $a \in G$, $(a^{-1})^{-1} = a$.
4. Para todo $a, b \in G$, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Demostración.

1. Sean e y f dos elementos identidad en G. Entonces se tiene la ecuación $e = e \cdot f = f$, de donde $e = f$.
2. Supongamos que un elemento $a \in G$ posee dos inversos x e y. Luego

$$x \cdot a = a \cdot x = e$$
$$y \cdot a = a \cdot y = e$$

Luego

$$\begin{aligned} y(a \cdot x) &= y \cdot e = y \\ (y \cdot a) \cdot x &= y \\ e \cdot x &= y \\ x &= y \end{aligned}$$

3. Para $a \in G$, se tiene

$$a^{-1} \cdot a = e$$
$$a \cdot a^{-1} = e$$

Luego a es el inverso de a^{-1}, único, y por lo tanto $(a^{-1})^{-1} = a$.

4. Sean $a, b \in G$. Luego

$$\begin{aligned}(a \cdot b)(b^{-1}a^{-1}) &= a \cdot (b \cdot b^{-1}) \cdot a^{-1} \\ &= (a \cdot e) \cdot a^{-1} \\ &= a \cdot a^{-1} \\ &= e\end{aligned}$$

Similarmente

$$\begin{aligned}(b^{-1}a^{-1})(a \cdot b) &= b^{-1} \cdot (a^{-1} \cdot a) \cdot b \\ &= b^{-1} \cdot e \cdot b \\ &= b^{-1} \cdot b \\ &= e\end{aligned}$$

Por lo tanto

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

□

Definición 1.6 Sea G un grupo y $H \subseteq G$. Si H es un grupo con la operación definida en G, entonces H se dice **subgrupo de** G. Y usaremos la notación $H < G$, además si $H < G$ y $H \neq \{e\}$ y $H \neq G$, se dirá que H es un **subgrupo propio** de G.

A los subgrupos $\{e\}$ y G de un grupo G se llamarán **subgrupos triviales de** G.

El siguiente teorema establece un criterio muy útil para determinar cuando un subconjunto H de un grupo G es un subgrupo.

Teorema 1.7 Un subconjunto H de un grupo G es un subgrupo, si y sólo si

1. $a \cdot b \in H$ para todo $a, b \in H$
2. $a^{-1} \in H$ para todo $a \in H$.

Demostración. Puesto que la operación binaria en G es asociativa, sólo falta verificar que $e \in G$. En efecto, sea $a \in H$, luego $a^{-1} \in H$ (por 2.) y además $a \cdot a^{-1} = e \in H$ (por 1). Luego H es un grupo, y por lo tanto un subgrupo de G. □

Teorema 1.8 Sea G un grupo y $a \in G$. Entonces el conjunto $H = \{a^n : n \in \mathbb{Z}\}$ es un subgrupo de G. Además H es el subgrupo de G más pequeño que contiene a.

Demostración. De acuerdo al teorema anterior, será suficiente probar:

- $a^n \cdot a^m \in H$, para $a^n, a^m \in H$
- $(a^n)^{-1} \in H$. para $a^n \in H$.

Claramente $a^n \cdot a^m = a^{n+m} = a^z$ con $z = n + m \in \mathbb{Z}$, por lo tanto $a^n \cdot a^m \in H$. También $(a^n)^{-1} = a^{-n} \in H$. Luego $H < G$.

Para probar la segunda afirmación, sea K un subgrupo de G y $a \in K$. Luego $a^0 = e \in K$ por ser K un grupo. También $a^2 \in K$, pues $a \in K$ y K es cerrado bajo la operación en G. De esta forma se concluye $a^n \in K$ para todo $n \geq 0$.

También $a^{-1} \in K$, pues $a \in K$ y su inverso se halla en K. Similarmente $a^{-2} = a^{-1} \cdot a^{-1} \in K$, pues $a^{-1} \in K$ y K es cerrado. Luego $a^{-n} \in K$ para todo $n \geq 0$. Hemos probado entonces que $H \subseteq K$ □

Definición 1.9 Un grupo G se dice **cíclico** si $G = \langle a \rangle$ para algún $a \in G$. Al grupo H definido anteriormente se llama **subgrupo cíclico** generado por a y al elemento a se llama **generador de** H. Usaremos la notación: $H = \langle a \rangle$.

El estudio de grupos cíclicos motiva la siguiente definición:

Definición 1.10 Si G es un grupo y $a \in G$, el **orden de** a es el menor entero positivo n tal que $a^n = e$.

Ahora pasaremos a estudiar una condición necesaria para que un subconjunto de un grupo finito, sea un subgrupo de este.

Teorema 1.11 (Lagrange). Sea G un grupo finito y H un subgrupo de G. Entonces el orden de H divide al orden de G.

Demostración. Si $H = \{e\}$ ó $H = G$ no hay nada que probar. Supongamos entonces que $H \neq \{e\}$ y $H \neq G$. Sea $H = \{h_1, \ldots, h_r\}$ donde $r = \texttt{Ord}(H)$.

Luego existe un elemento $a \in G$, tal que $a \notin H$. Entonces tenemos los siguientes elementos en G.

$$h_1, h_2, \ldots, h_r, ah_1, \ldots, ah_r.$$

Afirmamos que hay $2r$ elementos distintos. En efecto:

- Si $ah_i = h_j$, entonces multiplicando por h_i^{-1} a la derecha nos da $a = h_j h_i^{-1} \in H$. Luego $a \in H$, lo cual es una contradicción.

- Si $ah_i = ah_j$, cancelación por a nos da $h_i = h_j$, lo cual es una contradicción. Si esos $2r$ elementos son todos elementos de G, entonces $\texttt{Ord}(G) = 2r = 2\,\texttt{Ord}(H)$ y entonces $\texttt{Ord}(H)$ divide al orden de G.

  Si por el contrario, hay más de $2r$ elementos en G, continuamos el proceso y tendremos que existe un elemento $b \in G$, distinto de los anteriores. Luego tenemos los siguientes elementos en G

$$\begin{array}{lll} a_0h_1, & \ldots, & a_0h_r \\ a_1h_1, & \ldots, & a_1h_r \\ a_2h_1, & \ldots, & a_2h_r \\ & \vdots & \end{array}$$

  donde $a_0 = e$, $a_1 = a$, $a_2 = b$, etc, y a_i no es ninguno de los elementos que están en as filas anteriores a la i-ésima. Se puede probar que todos estos elementos que se generan son distintos. En efecto:

  - Si $a_ih_j = a_ih_k$, entonces cancelando se tiene que $h_j = h_k$, lo cual es una contradicción.
  - Si para $i > l$ se tiene $a_ih_j = a_lh_k$, entonces multiplicando por h_j^{-1} a la derecha se tiene $a_i = a_lh_kh_j^{-1}$. Como H es un grupo , tendremos que $h_kh_j^{-1} \in H$, luego $h_kh_j^{-1} = h_s$, para algún s y por lo tanto $a_i = a_lh_s$. Entonces el elemento a_i pertenece a la l-ésima fila, lo cual es una contradicción.

    Puesto que G es un grupo finito, este proceso de formación de filas se detiene despúes de un número finito de pasos, digamos k pasos. Se tendrá entonces que hay $k\,\texttt{Ord}(H)$ elementos en G. Con esto termina la demostración.

□

Usamos la notación $\texttt{Ord}(a)$ para indicar el orden de a. Si ese entero no existe, diremos que a tiene **orden infinito**.

Corolario 1.12 Si G es un grupo finito y $a \in G$, entonces $\texttt{Ord}(a)$ es un divisor de $\texttt{Ord}(G)$.

Demostración. Sea $a \in G$ y consideremos el subgrupo cíclico generado por a, $H = \langle a \rangle$ el cual consiste en los elementos

$$a^0 = e, a, a^2, \ldots, a^{n-1}$$

donde $a^n = e$.

Es claro entonces que $n = \texttt{Ord}(H)$ y además $n = \texttt{Ord}(a)$. De acuerdo con el teorema de Lagrange, tendremos que $\texttt{Ord}(H)|\texttt{Ord}(G)$. Luego $\texttt{Ord}(a)|\texttt{Ord}(G)$. □

Corolario 1.13 Si G es un grupo finito y $a \in G$, entonces $a^{\texttt{Ord}(G)} = e$.

Demostración. Sabemos que $a^{\texttt{Ord}(a)} = e$, y por el corolario anterior $\texttt{Ord}(G) = k{\cdot}\texttt{Ord}(a)$ para algún k. Luego $a^{\texttt{Ord}(G)} = a^{\texttt{Ord}(a)\cdot k} = \left(a^{\texttt{Ord}(a)}\right)^k = e^k = e$. □

Corolario 1.14 Si G es un grupo finito de orden primo p, entonces G es cíclico.

Demostración. Sea $a \in G$, $a \neq e$. Entonces $H = \langle a \rangle$ el subgrupo cíclico generado por a tiene orden un divisor de p. Luego hay dos posibilidades:

- $\texttt{Ord}(H) = p$, lo cual implica $H = G$ y G es cíclico generado por a
- $\texttt{Ord}(H) = 1$, y por lo tanto se tendría $a = e$, lo cual es imposible. Luego G es un grupo cíclico.

□

Operaciones con los subgrupos

Cuando se tiene un grupo G, es posible conocer parte del mismo si se conoce un subgrupo H de G. Si G tiene varios subgrupos diferentes, entonces cada uno de ellos es una pieza dentro de una gran maquinaria: cada una cumple una función específica en G. Cuando se conocen todos los subgrupos de G entonces se tiene un conocimiento total del grupo G, en cierto sentido.

Si queremos mirar como se multiplican dos elementos dentro de G, y estos dos elementos están dentro de un subgrupo H, el cual ha sido determinado de antemano, entonces el problema estará resuelto porque sabemos como se ejecuta la multiplicación dentro de H.

Si por el contrario un elementos está en un subgrupo H, y otro elemento esta fuera de H y dentro otro subgrupo K, entonces el producto de ambos elementos estará en un conjunto L contenido en G. Nos preguntamos: ¿Cómo podríamos garantizar que L sea un subgrupo de G? ¿Cuál es el orden de L?

Definición 1.15 Sea G un grupo y H, K dos subgrupos de G. Entonces la **intersección** de H y K, es el conjunto

$$H \cap K = \{x \in G : x \in H, \text{ y } x \in K\}$$

Proposición 1.16 La intersección de dos subgrupos de G es un subgrupo de G.

Demostración. Sean $x,\ y \in H \cap K$. Entonces $xy \in H$, y además $xy \in K$, pues H y K son grupos. Luego $xy \in H \cap K$.

Por otro lado, si $x \in H \cap K$, entonces $x^{-1} \in H$, y $x^{-1} \in K$, pues H y K son grupos. Luego $x^{-1} \in H \cap K$. □

Clases laterales

En esta sección se expone la ventajas de tener una partición del grupo en clases de equivalencias, además se mostrará que bajo ciertas condiciones sobre H, este conjunto de clases de equivalencias módulo H se le podrá dotar de una estructura de grupo.

Definición 1.17 Sea G un grupo y H un subgrupo de G. Si $a \in G$, entonces la **clase lateral derecha de a en H** es el conjunto

$$Ha = \{ha : h \in H\}.$$

Definición 1.18 Sea $a \in G$, entonces la **clase lateral izquierda de a** es el conjunto

$$aH = \{ah : h \in H\}.$$

Definición 1.19 Sea G un grupo y H un subgrupo de G. Sean a y b dos elementos de G. Diremos que a **es congruente a** b módulo H y lo denotamos $a \equiv b \mod H$ si y sólo si $ab^{-1} \in H$.

Teorema 1.20 Sea G un grupo y $H < G$, entonces la relación de congruencia módulo H, determina una relación de equivalencia en G.

Demostración.

1. **Reflexiva:** Sea $a \in G$, entonces $aa^{-1} = e \in H$, luego $a \equiv a \mod H$.
2. **Simétrica:** Supongamos que $a \equiv b \mod H$, entonces $ab^{-1} \in H$. Ahora bien, como H es un grupo, se tiene $(ab^{-1})^{-1} = ba^{-1} \in H$, luego $b \equiv a \mod H$
3. **Transitiva:** Supongamos que $a \equiv b \mod H$ y $b \equiv c \mod H$. Luego

   $$ab^{-1} \in H \quad \text{y} \quad bc^{-1} \in H.$$

   Como H es un subgrupo de G, se debe tener $ac^{-1} = (ab^{-1})(bc^{-1}) \in H$. Luego $a \equiv c \mod H$.

□

Teorema 1.21 Para todo $a \in G$, sea $[a] = \{x \in G : x \equiv a \mod H\}$. Entonces $[a] = Ha$.

Demostración. Sea $x \in [a]$, entonces $x \equiv a \mod H$, luego $xa^{-1} \in H$, por lo tanto existe $h \in H$ tal que $xa^{-1} = h$, lo cual implica $x = ha$. Y así $x \in Ha$.

Recíprocamente, supongamos que $x \in Ha$. Luego existe $h \in H$, tal que $x = ha$. Luego $xa^{-1} = h$ y por ende $x \equiv a \mod H$. Con esto se prueba que $x \in [a]$, lo cual da fin a la demostración. □

Observación Si a es un elemento de G, el conjunto $[a]$ se llama **la clase de equivalencia módulo H**. El teorema anterior nos dice entonces, que toda clase lateral es igual a una clase de equivalencia.

A continuación, probaremos que todas las clases laterales tienen el mismo número de elementos.

Teorema 1.22 Sean a y $b \in G$. Entonces $\texttt{Ord}(Ha) = \texttt{Ord}(Hb)$.

Demostración. Consideremos la función

$$\begin{array}{rcl} \phi & : & Ha \longrightarrow hb \\ & & ha \longrightarrow hb \end{array}$$

Entonces probaremos que ϕ es inyectiva. En efecto, sean $h_1, h_2 \in H$. Si suponemos $\phi(h_1 a) = \phi(h_2 a)$, se tiene que $h_1 b = h_2 b$, y luego $h_1 = h_2$. Claramente ϕ es sobreyectiva y por lo tanto ϕ es biyectiva.

□

Definición 1.23 Sea G y H un subgrupo de G, entonces el número de clases laterales de H en G se llama el **índice de H en G** y lo denotamos por $[G : H]$.

Corolario 1.24 Sea G un grupo, H un subgrupo de G. Entonces

$$\texttt{Ord}(G) = [G : H] \cdot \texttt{Ord}(H) \tag{1.1}$$

Demostración. Notar que todas las clases laterales derechas de G tiene el mismo número de elementos, en particular H mismo es una clase lateral derecha pues $H = He$, de aquí se deduce

$\texttt{Ord}(G)$ = número de clases laterales · número de elementos en $H = [G : H] \cdot \texttt{Ord}(H)$ □

Nota: Si G es finito, entonces se tiene

$$[G : H] = \frac{\texttt{Ord}(G)}{\texttt{Ord}(H)} \tag{1.2}$$

Observación: La fórmula (1.2) nos proporciona otra demostración del teorema de Lagrange.

1.4. Isomorfismos

Cuando se estudian los grupos en abstracto, considerando únicamente la forma como se multiplican los elementos, es necesario construir la tabla de multiplicación de un grupo finito, en ésta se recoge toda la mayor cantidad de información posible sobre la operación en el grupo, sin prestar atención a la naturaleza misma de los elementos.

Es posible que dos grupos finitos del mismo orden tengan tablas de multiplicación diferentes, en este caso diremos que los grupos no tienen la misma forma, o bien que ellos no son *isomorfos*.

El concepto de isomorfismo es fundamental en toda la teoría de grupos, pues permite unificar una gran cantidad de grupos bajo una misma estructura abstracta.

Grupos normales

Definición 1.25 Sea G un grupo. Un subgrupo N de G se dice **subgrupo normal** de G si y sólo si $gng^{-1} \in N$, para todo $g \in G$, $n \in N$. Escribiremos $N \triangleleft G$ para indicar que N es un subgrupo normal de G

Lema 1.26 Sea N subgrupo de G. Entonces $N \triangleleft G$ y sólo si

$$gNg^{-1} = N, \text{ para todo } g \in G. \tag{1.3}$$

Demostración. Sea N normal. Entonces $gng^{-1} \in N$ para todo n. Luego $gNg^{-1} \subset N$. En particular, $g^{-1}Ng \subset N$, luego $N = g(g^{-1}Ng)g^{-1} \subset gNg^{-1} \subset N$, y por lo tanto $gNg^{-1} = N$.

Recíprocamente, si (1.3) es cierto, entonces N es normal en G. □

Observación 1 Si G es un grupo abeliano entonces todo subgrupo N de G es normal. Por lo tanto la noción de normalidad carece de interés cuando trabajamos con grupos abelianos.

Lema 1.27 Sea G un grupo y $N < G$. Entonces N es subgrupo normal de G, si y sólo si toda clase lateral derecha de G es una clase lateral izquierda.

Demostración. Sea N normal en G. Consideremos la clase lateral derecha Na. Entonces de acuerdo al lema 1.26

$$a^{-1}Na = N$$

de donde $Na = aN$. Luego Na es una clase lateral izquierda. Por otra parte, si $g \in G$, afirmamos que

$$gNg^{-1} = N$$

En efecto, gN es una clase lateral derecha y de acuerdo a la hipótesis debe ser una clase lateral izquierda. Pero

$$g = ge \in gN$$

y además

$$g = eg \in Ng.$$

Luego la única clase lateral izquierda que contienen a g es Ng, y por lo tanto

$$gN = Ng,$$

y de aquí se obtiene

$$gNg^{-1} = N.$$

□

1.5. Grupo cociente

Sea G un grupo y N un subgrupo normal de G. Entonces el conjunto de las clases laterales derechas de N en G, el cual denotamos por G/N, se puede dotar de estructura de grupo.

En primer lugar, definimos una multiplicación en G/N de la forma siguiente:

$$\begin{array}{rcl} G/N \times G/N & \longrightarrow & G/N \\ (Na, Nb) & \longrightarrow & Na \cdot Nb = Nab \end{array} \tag{1.4}$$

Nótese que por ser N normal se tiene que el producto de dos clases laterales derechas es de nuevo una clase lateral derecha, pues

$$Na \cdot Nb = N(aN)b = N \cdot Nab = Nab$$

Se pueden verificar los 4 axiomas de grupo para el conjunto cociente G/N con la operación así definida:

1) Si Na y Nb son dos clases laterales, entonces

$$NaNb = Nab \in G/N.$$

2) Si Na, Nb y Nc están en G/N se tiene

$$\begin{array}{rcl} Na(NbNc) & = & Na(Nbc) \\ & = & Na(bc) \\ & = & N(ab)c \\ & = & (NaNb)Nc \end{array}$$

3) Si $Na \in G/N$, entonces

$$Na \cdot N = Na = N \cdot Na$$

Luego N es el elemento neutro, para la multiplicación de clases laterales.

4) Si $Na \in G/N$, $Na^{-1} \in G/N$ y

$$\begin{array}{c} Na \cdot Na^{-1} = N(aa^{-1}) = Ne = N \\ Na^{-1} \cdot Na = N(a^{-1}a) = Ne = N \end{array}$$

Teorema 1.28 Sea N normal en G, entonces G/N es un grupo y

$$\mathtt{Ord}(G/N) = \frac{\mathtt{Ord}(G)}{\mathtt{Ord}(N)}.$$

Demostración. Hemos probado que G/N es un grupo con la operación de multiplicación dada en (1.3) Por otro lado el orden del grupo cociente G/N es igual al número de clases laterales de G en N, el cual viene dado por el índice de N en G, esto es:

$$\texttt{Ord}(G/N) = [G : N]$$

De acuerdo a la fórmula (1.2), se tiene

$$\texttt{Ord}(G/N) = \frac{\texttt{Ord}(G)}{\texttt{Ord}(N)}$$

□

1.6. Homomorfismos

Nos proponemos a definir ahora un cierto tipo de aplicación entre dos grupos, el cual sea compatible con las operaciones definidas en cada grupo.

Definición 1.29 Sean $(G, *)$ y $(\overline{G}, \circ)$ dos grupos. Una aplicación

$$\phi : G \longrightarrow \bar{G},$$

se llama **homomorfismo de grupos**, si y sólo si

$$\phi(a * b) = \phi(a) \circ \phi(b) \quad \text{para todo} \quad a, b \in G.$$

Observación: Usualmente utilizamos la misma notación para el producto en ambos grupos entonces la condición de homorfismo se escribe $\phi(ab) = \phi(a)\phi(b)$.

Lema 1.30 Sea G un grupo y sea N un subgrupo normal de G. Definamos

$$\begin{array}{rcl} \phi & : & G \longrightarrow G/N \\ & & \phi(x) = Nx \end{array}$$

entonces ϕ es un homomorfismo sobre. A este homomorfimo se llama la **proyección canónica sobre** N.

Demostración. Sea x, y en G. Entonces $\phi(xy) = Nxy = Nx \cdot Ny = \phi(x) \cdot \phi(y)$, con esto se demuestra que ϕ es un homorfismo. Además, si $Nx \in G/N$, se tiene que $\phi(x) = Nx$, con $x \in G$. Luego ϕ es sobre. □

Dos propiedades muy importantes de los homomorfismos son las siguientes:

Lema 1.31 Sea $\phi : G \longrightarrow \overline{G}$ un homomorfismo de grupos y $e, \overline{e}$ los elementos neutros de G y $\overline{G}$ respectivamente. Entonces

1. $\phi(e) = \bar{e}$.

2. $\phi(x^{-1}) = [\phi(x)]^{-1}$, para todo $x \in G$.

Demostración.

1. Tenemos que $\phi(ee) = \phi(e)\phi(e)$, y por otra parte $\phi(ee) = \phi(e)$. Igualando ambas expresiones tenemos que $\phi(e)\phi(e) = \phi(e)$, usamos la ley de cancelación en el grupo $\overline{G}$ se obtiene $\phi(e) = \bar{e}$.
2. Sea $x \in G$. Entonces $\bar{e} = \phi(e) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$. Luego el inverso de $\phi(x)$ en el grupo $\overline{G}$, viene dado por $[\phi(x)]^{-1} = \phi(x^{-1})$.

□

Definición 1.32 Sea $\phi : G \longrightarrow \overline{G}$, entonces el **Kernel de** ϕ, o **núcleo** es el subconjunto de G

$$\operatorname{Kern}\phi = \{x \in G : \phi(x) = e\}.$$

Teorema 1.33 Sea $\phi : G \longrightarrow \overline{G}$ un homomorfismo de grupos. Entonces $\operatorname{Kern}\phi$ es un subgrupo normal de G.

Demostración. En primer lugar demostramos que $\operatorname{Kern}\phi$ es un subgrupo de G. Sean $a, b \in \operatorname{Kern}\phi$, entonces: $\phi(ab) = \phi(a)\phi(b) = \bar{e}\bar{e} = \bar{e}$, luego $ab \in \operatorname{Kern}\phi$.

Por otro lado, sea $a \in G$, luego se tiene $\phi(a^{-1}) = \phi^{-1}(a) = \bar{e}^{-1} = \bar{e}$, de donde $a^{-1} \in \operatorname{Kern}\phi$. Por lo tanto $\operatorname{Kern}\phi$ es un subgrupo de G.

Finalmente para demostrar la normalidad, sea $g \in G$ y $n \in \operatorname{Kern}\phi$. Luego $\phi(g^{-1}ng) = \phi^{-1}(g)\phi(n)\phi(g) = \phi^{-1}(g)\bar{e}\phi(g) = \phi^{-1}(g)\phi(g) = \bar{e}$. Así se ha demostrado que

$$g^{-1}\, n\, g \subseteq \operatorname{Kern}\phi, \quad \forall n \in \operatorname{Kern}\phi$$

Por lo tanto

$$g^{-1}\,(\operatorname{Kern}\phi)\, g \subseteq \operatorname{Kern}\phi \quad \forall g \in G.$$

y así $\operatorname{Kern}\phi$ es normal en G. □

Definición 1.34 Un homomorfismo de grupo $\phi : G \longrightarrow \overline{G}$ se dice **isomorfismo** si y sólo si ϕ es una biyección.

En tal situación diremos que los grupos G y $\overline{G}$ **son isomorfos** y lo denotamos por

$$G \cong \overline{G}.$$

1.7. Grupos de automorfismos

Definición 1.35 Sea G un grupo. Una aplicación $\phi : G \longrightarrow G$, la cual es un isomorfismo, entonces a ϕ se le llama un **automorfismo** de G.

El conjunto de todos los automorfismo de G, se denota por $\texttt{Aut}(G)$

Teorema 1.36 Sea G un grupo, entonces $\texttt{Aut}(G)$ es un grupo bajo la composición de funciones.

Demostración. Sean $\phi_1, \phi_2 \in \texttt{Aut}(G)$. Entonces

$$\begin{aligned} \phi_1\phi_2(xy) &= \phi_1(xy)\phi_2 \\ &= [\phi_1(x)\phi_1(y)]\phi_2 \\ &= \phi_1\phi_2(x)\phi_1\phi_2(y) \end{aligned}$$

Luego

$$\phi_1\phi_2 \in \texttt{Aut}(G), \quad \forall x, y \in G$$

Además si $\phi \in \texttt{Aut}(S)$, ϕ^{-1} existe y es biyectiva. Sean $x_1, x_2 \in G$. Luego

$$\phi^{-1}(x_1) = y_1, \quad \phi^{-1}(x_2) = y_2$$

y

$$\begin{aligned} \phi(\phi^{-1}(y_1y_2)) &= y_1y_2 \\ &= \phi^{-1}(x_1)\phi^{-1}(x_2) \\ &= \phi^{-1}(\phi(y_1))\phi^{-1}(\phi(\phi(y)) \\ &= \phi(\phi^{-1}(y_1))\phi(\phi^{-1}(y_2)) \\ &= \phi(\phi^{-1}(y_1)\phi^{-1}(y_2)) \end{aligned}$$

Como ϕ es inyectiva, se tiene entonces

$$\phi^{-1}(y_1y_2) = \phi^{-1}(y_1)\phi^{-1}(y_2).$$

Con esto termina la demostración. □

El problema que abordaremos ahora es el de determinar el conjunto $\texttt{Aut}(G)$, dado un grupo G.

Definición 1.37 Si G es no abeliano entonces para cada $g \in G$, definimos

$$\begin{array}{rccc} \sigma_g & : & G & \longrightarrow & G \\ & & x & \longrightarrow & g^{-1}xg \end{array}$$

Entonces σ_g es un automorfismo llamado **automorfismo interno** de G. El conjunto de los automorfismo internos de G, será denotado por $I(G)$

Teorema 1.38 Sea G un grupo cualquiera, entonces $I(G) = \{\sigma_g \mid g \in G\}$ es un subgrupo del grupo $\texttt{Aut}(G)$.

Demostración. Sean $\sigma_{g_1}, \sigma_{g_2} \in I(G)$. Luego

$$\begin{aligned} \sigma_{g_1}\sigma_{g_2}(x) &= \sigma_{g_2}(g_1^{-1}xg_1) \\ &= g_2^{-1}g_1^{-1}xg_1g_2 \\ &= (g_1g_2)^{-1}x(g_1g_2) \\ &= \sigma_{g_1g_2}(x) \quad \forall x \in G \end{aligned}$$

Luego

$$\sigma_{g_1}\sigma_{g_2} = \sigma_{g_1g_2} \tag{1.5}$$

y por lo tanto $I(G)$ es cerrado bajo el producto. Además si $\sigma_g \in I(G)$

$$\sigma_g\sigma_{g^{-1}} = \sigma_e = I, \quad \text{por la fórmula (1,5)}$$

Luego $(\sigma_g)^{-1} = \sigma_{g^{-1}} \in I(G.)$ □

Definición 1.39 Sea G un grupo. Un subgrupo H de G se llama **subgrupo característico**, si para todo automorfismo σ_g de G, se tiene $\sigma_g(H) \subset H$.

Observación: Si H es un subgrupo característico de G, entonces H es normal en G. Para ver esto, sea $g \in G$, entonces el automorfismo interno $\sigma_g : G \longrightarrow G$ satisface $\sigma_g(H) \subset H$. Luego se tiene $ghg^{-1} \in H$, para todo h en H. Por lo tanto H es normal.

Teorema 1.40 Sea G un grupo y $I(G)$ el grupo de automorfismos internos, entonces

$$I(G) \cong G/\mathcal{Z}.$$

Demostración. Sea

$$\begin{array}{rccc} \phi & : & G & \longrightarrow & I(G) \\ & & g & \longrightarrow & \sigma_g \end{array}$$

Entonces ϕ es un morfismo sobreyectivo.

En efecto, sean $g_1, g_2 \in G$. Luego

$$\phi(g_1g_2) = \sigma_{g_1g_2} = \sigma_{g_1}\sigma_{g_2} \quad \text{por fórmula (1,5)}$$

Además ϕ es sobre. Por otro lado, si $g \in \mathcal{Z}$ entonces es claro que $\sigma_g = Id$ es la identidad. Luego

$$\mathcal{Z} \subseteq \operatorname{Kern}\phi$$

Si $g \in \operatorname{Kern} g$ entonces

$$\sigma_g(x) = g^{-1}xg = x, \quad \text{para todo } x \in G.$$

Luego

$$xg = gx, \quad \text{para todo } x \in G$$

lo cual implica que

$$\operatorname{Kern}\phi \subseteq \mathcal{Z}$$

Por lo tanto hemos demostrado que $\text{Kern}(\phi) = \mathcal{Z}$, y usando el primer teorema de isomorfismos[1], se concluye

$$G/\operatorname{Kern}\phi \cong I(G)$$

Luego

$$G/\mathcal{Z} \cong I(G)$$

. □

A continuación, determinaremos todos los automorfismos de un grupo cíclico G, de orden r.

Teorema 1.41 Sea $G = \langle g \rangle$ un grupo cíclico de orden r, entonces $\texttt{Aut}(G) \cong U_r$, donde U_r es el grupo de enteros módulo r con la multiplicación.

Demostración. Sea $T \in \texttt{Aut}(G)$, entonces si g es un generador se tiene

$$T(g^i) = T^i(g) \quad \text{para todo } 1 \leq i$$

Luego para determinar un automorfismo T, basta con determinar la imagen de $T(g)$.

Ahora bien, como $T(g)$ debe tener el mismo orden que g, se tiene que $T(g)$ es un generador de G. Luego la aplicación

$$\begin{array}{rccc} \psi & : & \texttt{Aut}(G) & \longrightarrow & U_r \\ & & T_i & \longrightarrow & i \end{array}$$

donde $T_i(g) = g^i$ es un isomorfismo.

□

[1] Primer Teorema de Isomorfismo: Sea $\phi : G \longrightarrow \overline{G}$ un morfismo sobre, con $\operatorname{Kern}\phi = K$, entonces $G/K \cong \overline{G}$.

Capítulo 2

Estructura de los grupos finitos

La clasificación de todos los grupos abelianos finitos es sin duda alguna, una de las más altas realizaciones de toda el álgebra. El primer paso en alcanzar esta meta viene dado por los teoremas Sylow, los cuales permiten obtener subgrupos de orden una potencia de un primo p, cuando dicha potencia es un divisor del orden del grupo dado. Los teoremas de Sylow son una herramienta poderosa que permite desmenuzar un grupo grande en pedazos más pequeños (a los que llamaremos $p-$grupos), de una manera rápida y eficiente, con tan sólo conocer el orden del grupo.

Producto directo de grupos

Sean A y B dos grupos y consideremos a A y B como conjuntos. Sea G el producto cartesiano $A \times B$. Podemos definir una operación binaria en $A \times B$ mediante

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

donde $a_1 a_2$ indica el producto de a_1 con a_2 en el grupo A_1, y $b_1 b_2$ indica el producto de b_1 con b_2 en el grupo B. Probaremos que G con la operación $*$, de multiplicación por coordenadas, es un grupo.

En primer lugar la operación es cerrada, pues los respectivos productos en A y B son cerrados, con lo cual se demuestra que $(a_1 a_2, b_1 b_2)$ es un elemento de G. Para demostrar la asociatividad, pongamos

$$\begin{aligned}
(a_1, b_1) * [(a_2, b_2) * (a_3, b_3)] &= (a_1, b_1) * (a_2 a_3, b_2 b_3) \\
&= (a_1 (a_2 a_3), b_1 (b_2 b_3)) \\
&= ((a_1 a_2) a_3), (b_1 b_2) b_3) \\
&= (a_1 a_2, b_1 b_2) * (a_3, b_3) \\
&= [(a_1, a_2) * (a_2, b_2)] * (a_3, b_3)
\end{aligned}$$

Sea e el elemento neutro de A y f el elemento neutro de B. Entonces el elemento (e, f) está en G. Además, si (a, b) es cualquier elemento de G se tendrá:

$$(e, f) * (a, b) = (ea, fb) = (a, b)$$

$$(a, b) * (e, f) = (ae, bf) = (a, b)$$

Luego (e, f) es el elemento neutro para la operación $*$. Finalmente, si $(a, b) \in G$, el elemento (a^{-1}, b^{-1}) estará en G, y se tiene entonces

$$(a, b) * (a^{-1}, b^{-1}) = (aa^{-1}, bb^{-1}) = (e, f)$$

y

$$(a^{-1}, b^{-1}) * (a, b) = (a^{-1}a, b^{-1}b) = (e, f)$$

luego el inverso de (a, b) es (a^{-1}, b^{-1}). En conclusión hemos probado que $(G, *)$ satisface todas las propiedades de la definición de grupo.

Además, si A y B son grupos abelianos, entonces $A \times B$ es un grupo abeliano.

Definición 2.1 Sean A y B dos grupos. El grupo $G = A \times B$, con la operación de multiplicación por coordenadas, se llama **producto directo externo** de A y B.

Observación: Si los grupos A y B son abelianos, entonces $G = A \times B$ se llama la suma directa de A y B y se denota por $A \oplus B$

El producto directo externo de dos grupos, se puede generalizar a cualquier número de grupos. Sean $G_1, \ldots, G_n$ grupos y sea $G = G_1 \times \cdots \times G_n$ el conjunto de $n-$uplas $(g_1, \ldots, g_n)$ con $g_i \in G_i$, $1 \leq i \leq n$.

Definimos la operación de producto en G, multiplicando componente por componente

$$(g_1, \ldots, g_n) * (h_1, \ldots, h_n) = (g_1h_1, \ldots, g_nh_n)$$

Entonces el grupo G con esta operación se llama el **producto directo externo** de $G_1, \ldots, G_n$

Observación: Si se tiene $G = A \times B$, entonces los conjuntos

$$H = \{(a, f) \mid a \in A\} \quad \text{y} \quad K = \{(e, b) \mid b \in B\}$$

son subgrupos de G y además

$$H \cap K = \{(e, f)\}.$$

Con las mismas notaciones anteriores, se tiene la siguiente proposición:

Proposición 2.2 Para todo $g \in A \times B$, existen únicos elementos $g_1 \in H$ y $g_2 \in K$ tales que $g = g_1g_2$.

Demostración. Sea $g = (a, b)$, entonces

$$\begin{aligned} g &= (a, b) \\ &= (a, f)(e, b) \\ &= g_1g_2 \end{aligned}$$

con $g_1 \in H$, $g_2 \in K$.

Supongamos ahora que $g = g_1' g_2'$, con $g_1' \in H$ y $g_2' \in K$. Luego $g = g_1 g_2 = g_1' g_2'$, de donde $(g_1')^{-1} g_1 = g_2 (g_2')^{-1} \in H \cap K$. Por lo tanto $(g_1')^{-1} g_1 = e$, lo cual implica $g_1' = g_1$. Similarmente se demuestra $g_2' = g_2$. □

Este resultado se puede generalizar de la manera siguiente:

Proposición 2.3 Sean $G_1, \ldots, G_n$ grupos, y consideremos el producto directo de ellos, $G = G_1 \times \cdots \times G_n$, para cada i, sea e_i el elemento neutro del grupo G_i y sea

$$H_i = \{(e_1, \ldots, e_{i-1}, h, e_{i+1}, \ldots, e_n) \mid h \in G_i\}$$

entonces los H_i son subgrupos de G y además

1. $H_i \cap H_j = e$, para $i \neq j$, donde e es elemento neutro de G.
2. Todo elemento $g \in G$ se expresa de manera única

$$g = h_1 h_2 \cdots h_n$$

donde los h_i están en H_i.

Definición 2.4 Sea G un grupo y $H_1, \ldots, H_n$ subgrupos normales de G, tales que

1. $G = H_1 \cdots H_n$
2. Para todo $g \in G$, existen elementos únicos $h_i \in H_i$, $1 \leq i \leq n$, tales que

$$g = h_1 \cdots h_n$$

Entonces G se llama el **producto directo interno** de $H_1, \ldots, H_n$.

Observación: Más adelante, probaremos que el producto directo externo es isomorfo al producto directo interno, y por lo tanto al quedar probado este isomorfismo hablaremos de producto directo, sin ser específicos. Antes de llegar a ese resultado, necesitamos la siguiente proposición:

Proposición 2.5 Sea $G = N_1 \cdots N_s$ producto directo interno, entonces para todo par de subíndices $i \neq j$ se tiene que

$$N_i \cap N_j = \{e\},$$

y además se cumple

$$ab = ba$$

para cualquier $a \in N_i$, $b \in N_j$.

Demostración. Sea $x \in N_i \cap N_j$, entonces de acuerdo con la definición de producto directo interno, existen elementos $g_1, \ldots, g_s$ con $g_i \in N_i$ tales que

$$x = g_1 \cdots g_s \tag{2.1}$$

Por otro lado, podemos representar a x de dos formas distintas

$$x = e_1 e_2 \cdots e_{i-1} x e_{i+1} \cdots e_n$$
$$x = e_1 e_2 \cdots e_{j-1} x e_{j+1} \cdots e_n$$

donde $e_s = e$, es el elemento neutro de G.

Usando la unicidad de la representación en (2.1) se concluye que $x = e$, de donde

$$N_i \cap N_j = \{e\}$$

Si suponemos que $a \in N_i$ y $b \in N_j$, se tiene que $aba^{-1} \in N_j$, puesto que N_j es normal.

Por estar b^{-1} en N_j, se debe tener $aba^{-1}b^{-1} \in N_j$. Pero por otro lado, usando la normalidad de N_i se sigue que $ba^{-1}b^{-1} \in N_i$, y entonces $aba^{-1}b^{-1} \in N_i$.

Combinando ambos resultados se obtiene $aba^{-1}b^{-1} \in N_i \cap N_j = \{e\}$, de donde $ab = ba$. □

Vamos a demostrar el siguiente lema:

Lema 2.6 Sea G un grupo y H y K, subgrupos normales en G tales que cumplen las siguientes condiciones:

1. $G = HK$,
2. $H \cap K = \{e\}$,

entonces $hk = kh$ para todo $h \in H$ y $k \in K$ y por lo tanto $G = H \times K$.

Demostración. Si se considera el elemento $a = hkh^{-1}k^{-1}$, con $h \in H$ y $k \in K$, o lo que es lo mismo $a = (hkh^{-1})k^{-1}$, de la normalidad de K se deduce que $hkh^{-1} \in K$, lo cual implica que $a \in K$; análogamente se demuestra que $a \in H$, considerando $a = h(kh^{-1}k^{-1})$, y entonces $a \in H \cap K$, pero por la condición 2) tenemos que $H \cap K = \{e\}$, por lo que $a = e$, y así $hk = kh$ para $h \in H$ y $k \in K$. □

Teorema 2.7 Sea $G = N_1 \cdots N_s$ producto directo interno y $G' = N_1 \times \cdots \times N_s$ producto directo externo, entonces

$$G \cong G'.$$

Demostración. Consideremos la aplicación

$$\psi : G' \longrightarrow G$$
$$\psi(g_1, \ldots, g_s) = g_1 \cdots g_s$$

Entonces ψ está bien definida, pues cada g_i pertenece a G, luego el producto de los g_i está en G. Sean $x, y \in G'$ y probemos que

$$\psi(x, y) = \psi(x)\psi(y)$$

Se tiene

$$x = (g_1, \ldots, g_s),\ y = (h_1, \ldots, h_s) \quad \text{con } g_i, h_i \in N_i,$$

para todo $(1 \leq i \leq s)$. Luego, usando la proposición anterior, se deduce

$$\begin{aligned} \psi(x, y) &= \psi(g_1 h_1, \ldots, g_s h_s) \\ &= (g_1 h_1)(g_2 h_2) \cdots (g_s h_s) \\ &= (g_1 \cdots g_s)(h_1 \cdots h_s) \\ &= \psi(x)\psi(y) \end{aligned}$$

Además ψ es sobreyectiva, por la definición de producto interno. Falta probar la inyectividad de ψ.

Sea $x = (g_1, \ldots, g_s) \in G'$ tal que $\psi(x) = e$, luego se tiene

$$g_1 \cdots g_s = e$$

Usando la unicidad de la representación de

$$g_1 \cdots g_s = e_1 \cdots e_s$$

donde $e_i = e$ para todo $1 \leq i \leq s$, se concluye $g_i = e$, para todo $1 \leq i \leq s$. Luego $x = (e, \ldots, e) = e$ en G'. Por lo tanto hemos probado $\operatorname{Kern} \psi = \{e\}$ y se puede concluir entonces que ψ es inyectiva. □

Producto semidirecto de grupos

Definición 2.8 (Producto semidirecto externo). Sean H, K grupos, $\rho : H \to \texttt{Aut}\ (K)$ un morfismo. El **producto semidirecto externo** de H con K es el conjunto $H \times K$ con el producto:

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, \rho(h_2)(k_1)k_2)$$

Lo denotamos $H \times_\rho K$ si se desea hacer énfasis en el morfismo ρ, o simplemente $H[K]$. Decimos que K actúa sobre H por automorfismos.

Definición 2.9 (Producto semidirecto interno). Un grupo G es **producto semidirecto interior** del subgrupo H por el subgrupo K cuando:

1. Para todo $g \in G$ existen $x \in H, u \in K$, únicos, de manera que

$$g = xu.$$

2. Cualesquiera que sean $x \in H, u \in K$, se cumple

$$x^{-1}ux \in K.$$

y lo escribiremos $G = H[K]$

Proposición 2.10 Si dado un grupo K y si H es un grupo de operadores de K mediante un morfismo

$$\rho : H \to \mathtt{Aut}(K),$$

la operación del conjunto $H \times K$ definida por la ley

$$(x, u)(y, v) = (xy, \rho(y)(u)v)$$

dota al conjunto $H \times K$ de la estructura de grupo.

Antes de ver la demostración de la proposición anterior veamos un resultado de mucho interés:

Resultado 2.11 Si H es un grupo de operadores de K mediante un morfismo $\rho : H \to \mathtt{Aut}(K)$, entonces la operación: $\rho(h_1)\rho(h_2) = \rho(h_2) \circ \rho(h_1)$ establece estructura de grupo en $\mathtt{Aut}(K)$.
En efecto, verifiquemos que se cumplen los cuatro axiomas de grupo: Empezamos identificando el significado de esta operación en $\mathtt{Aut}(K)$, $h_1h_2 \mapsto \rho(h_1h_2) = \rho(h_1)\rho(h_2)$ por ser ρ morfismo, además: $\rho(h_1)\rho(h_2) = \rho(h_2) \circ \rho(h_1)$.

1. Cerradura de la operación definida: Es claro que si $\rho(h_1)$, $\rho(h_2) \in \mathtt{Aut}(K)$ entonces $\rho(h_1h_2) = \rho(h_1)\rho(h_2) \in \mathtt{Aut}(K)$.

2. Asociatividad:

$$\begin{aligned}(\rho(h_1)\rho(h_2))\rho(h_3) &= (\rho(h_2) \circ \rho(h_1))\rho(h_3)\\ &= \rho(h_3) \circ (\rho(h_2) \circ \rho(h_1))\\ &= \rho(h_3)(\rho(h_2)(\rho(h_1)))\\ &= (\rho(h_3) \circ \rho(h_2))(\rho(h_1))\\ &= (\rho(h_2)\rho(h_3)) \circ (\rho(h_1))\\ &= \rho(h_1)(\rho(h_2)\rho(h_3))\end{aligned}$$

3. Elemento neutro: $\exists \rho(e) = \mathtt{Id} \in \mathtt{Aut}(K)$ la función identidad, tal que: $\rho(h) \circ \rho(e) = \rho(eh) = \rho(h)$ y $\rho(e) \circ \rho(h) = \rho(he)\rho(h)$.

4. Elemento simétrico: Sea $\rho(h)$, $\rho(e) \in \mathtt{Aut}(K)$, entonces si $\rho(h)\rho(h^*) = \rho(e) = \rho(hh^*)$, entonces $hh^* = e$, de donde $h^* = h^{-1}$, por lo que $(\rho(h))^{-1} = \rho(h^{-1})$

Y así se demuestra que la operación definida establece una estructura de grupo en $\mathtt{Aut}(K)$.

Ahora pasamos a la demostración de la proposición:

Demostración. Ahora vamos a verificar que en $A \times B$ se tiene la estructura de grupo:

1. La cerradura de la operación definida es clara.

2. La parte delicada es demostrar la asociatividad: (para no hacer engorrosa la notación vamos a omitir los paréntesis, esto es al elemento $(xy)z$ lo denotaremos simplemente por xyz en virtud

de la estructura de grupo de H)

$$\begin{aligned}[(x,u)(y,v)](z,w) &= (xy, \rho(y)(u)v)(z,w)\\ &= (xyz, \rho(z)(\rho(y)(u)v)w)\\ &= (xyz, \rho(z)(\rho(y)(u))\rho(z)(v)w)\\ &= (xyz, (\rho(z)\circ\rho(y))(u)\rho(z)(v)w)\\ &= (xyz, (\rho(yz)(u)\rho(z)(v)w)\\ &= (x,u)(yz, \rho(z)(v)w)\\ &= (x,u)[(y,v)(z,w)]\end{aligned}$$

3. El elemento neutro es (e_H, e_K) donde e_H y e_K son los elementos neutros de los subgrupos H y K respectivamente:

$$\begin{aligned}(e_H, e_K)(h,k) &= (e_H h, \rho(h)(e_K)k)\\ &= (e_H h, e_K k)\\ &= (h,k)\end{aligned}$$

También:

$$\begin{aligned}(h,k)(e_H, e_K) &= (he_H, \rho(e_H)(k)e_K)\\ &= (he_H, ke_K)\\ &= (h,k)\end{aligned}$$

4. Para encontrar el inverso de cualquier elemento (h,k) del conjunto puede razonarse de la siguiente manera:

$$\begin{aligned}(h,k)(h_*,k_*) &= (e_H, e_K)\\ (hh_*, \rho(h_*)(k)k_*) &= (e_H, e_K)\\ hh_* = e_H \qquad & \rho(h_*)(k)k_* = e_K\\ h_* = h^{-1} \qquad & k_* = (\rho(h_*)(k))^{-1} = \rho(h_*)(k^{-1}) = \rho(h^{-1})(k^{-1})\end{aligned}$$

así entonces

$$(h_*, k_*) = (h^{-1}, \rho(h^{-1})(k^{-1}))$$

□

El grupo así construido se conoce como producto semidirecto (*exterior*) de H por K mediante el morfismo $\rho : H \to \mathtt{Aut}(K)$, y se denota $H \times_\rho K$.

2.1. La ecuación de la clase

En esta sección estudiaremos una nueva técnica para contar los elementos dentro de un grupo G, conocida con el nombre de relación de conjugación. Por medio de ésta, es posible demostrar un

resultado muy interesante sobre grupos finitos debido a Cauchy. Este resultado establece que si un número primo p divide al orden de un grupo finito G, entonces G tiene un subgrupo de orden p.

Definición 2.12 Sea G un grupo y $a, b \in G$. Diremos que b es **conjugado** de a, si existe $c \in G$, tal que

$$b = c^{-1}ac$$

Si b es un conjugado de a, lo denotamos por

$$a \sim b$$

Se puede verificar que la relación "$\sim$" es de equivalencia en el conjunto G. Para cada $a \in G$ se tiene su clase de conjugación:

$$C(a) = \{x \in G, \mid a \sim x\}$$

Si $C(a)$ tiene C_a elementos, se tiene la siguiente fórmula de conteo en G.

$$\texttt{Ord}(G) = \sum C_a$$

donde C_a recorre todas las clases de equivalencia, a esta relación se conoce con el nombre de **ecuación de la clase en** G.

Definición 2.13 Sea G un grupo y $a \in G$. Definimos el **normalizador** de a como

$$N(a) = \{x \in G, \mid xa = ax\}.$$

Entonces es fácil probar que $N(a)$ es un subgrupo de G. El normalizador $N(a)$ es el conjunto de todos los elementos del grupo que conmutan con a.

Teorema 2.14 Para cada $a \in G$,

$$C_a = \frac{\texttt{Ord}(G)}{\texttt{Ord}(N(a))}.$$

Demostración. Definimos una función

$$\begin{array}{rccc} \phi & : & C(a) & \longrightarrow & G/N(a) \\ & & T = x^{-1}ax & \longrightarrow & N(a)x \end{array}$$

Probaremos que ϕ es una biyección

1. ϕ está bien definida. Es decir, dos clases de conjugados iguales, pero con distintos representantes, tienen la misma imagen bajo el momorfismo ϕ.
   Si $x^{-1}ax = y^{-1}ay$, entonces $yx^{-1}axy^{-1} = a$, lo cual implica

   $$(xy^{-1})^{-1}axy^{-1} = a.$$

   Luego debemos tener $xy^{-1} \in N(a)$ y de aquí se deduce que $xN(a) = yN(a)$. Por lo tanto ϕ está bien definida.

2. ϕ es inyectiva.
   Supongamos que para $T_1, T_2 \in C(a)$, donde $T_1 = x^{-1}ax$, $T_2 = y^{-1}ay$, se tiene $\phi(T_1) = \phi(T_2)$. Por lo tanto
   $$N(a)x = N(a)y$$
   Luego $xy^{-1} \in N(a)$, lo cual implica $xy^{-1}a = axy^{-1}$. Por lo tanto $y^{-1}ay = x^{-1}ax$, y de esto se obtiene $T_1 = T_2$.

3. Además es claro que ϕ es sobre.

□

Corolario 2.15 Si G es un grupo finito, se tiene

$$\mathtt{Ord}(G) = \sum \frac{\mathtt{Ord}(G)}{\mathtt{Ord}(N(a))}$$

donde cada elemento a pertenece a una clase conjugada.

Definición 2.16 Sea G un grupo, entonces el **centro** de G es el conjunto

$$\mathcal{Z}(G) = \{g \in G \mid gx = xg,\ \forall x \in G\}.$$

Usaremos el símbolo $\mathcal{Z}$ o $\mathcal{Z}(G)$, indistintamente para indicar este grupo.

Es fácil verificar que $\mathcal{Z}(G)$ es un subgrupo abeliano de G. En efecto: $e \in \mathcal{Z}(G)$. Si $a, b \in \mathcal{Z}(G)$, entonces para cualquier $x \in G$, $x(ab) = (xa)b = (ax)b = a(xb) = a(bx) = (ab)x$ y $ab \in \mathcal{Z}(G)$. También de la igualdad $xa = ax$ obtenemos que $a^{-1}xaa^{-1} = a^{-1}axa^{-1}$, esto es $a^{-1}x = xa^{-1}$ y por consiguiente $a^{-1} \in \mathcal{Z}(G)$. Y así $\mathcal{Z}(G) < G$.

Observación: Si $a \in \mathcal{Z}(G)$, entonces $N(a) = G$, luego

$$\frac{\mathtt{Ord}(G)}{\mathtt{Ord}(N(a))} = 1$$

Usando esta observación tenemos el corolario:

Corolario 2.17 Si G es finito

$$\mathtt{Ord}(G) = \mathtt{Ord}(\mathcal{Z}(G)) + \sum_{a \notin \mathcal{Z}(G)} \frac{\mathtt{Ord}(G)}{\mathtt{Ord}(N(a))}.$$

Corolario 2.18 Si $\mathtt{Ord}(G) = p^n$, donde p es un número primo, entonces $\mathcal{Z}(G) \neq \{e\}$.

Demostración. Si $a \notin \mathcal{Z}(G)$, entonces $N(a) \neq G$, luego por el teorema de Lagrange

$$\mathtt{Ord}(N(a)) | \mathtt{Ord}(G)$$

y por lo tanto

$$\mathtt{Ord}(N(a)) = p^\alpha \quad \text{con } 1 \leq \alpha < n$$

luego

$$p \left| \frac{\mathtt{Ord}(G)}{\mathtt{Ord}(N(a))} \right. ,$$

para todo $a \notin \mathcal{Z}(G)$.

Así

$$p \left| \mathtt{Ord}(G) - \sum_{a \notin \mathcal{Z}(G)} \frac{\mathtt{Ord}(G)}{\mathtt{Ord}(N(a))} \right.$$

y por lo tanto

$$p \mid \mathtt{Ord}(\mathcal{Z}(G))$$

Esto es $\mathtt{Ord}(\mathcal{Z}(G)) > 1$ □

Teorema 2.19 (Teorema de Cauchy). Sea G un grupo finito y p un número primo tal que $p|\mathtt{Ord}(G)$, entonces G tiene un elemento de orden p.

Demostración.

1. Supongamos que G es abeliano. Usaremos inducción sobre el orden de G. Si $\mathtt{Ord}(G) = 1$ no hay nada que probar.

   Supongamos el teorema cierto para subgrupos de orden menor que $n = \mathtt{Ord}(G)$

   a) Si $\mathtt{Ord}(G) = p$, con p un número primo, entonces G es un grupo cíclico generado por un elemento $g \in G$. Luego $\mathtt{Ord}(g) = p$ y g es el elemento buscado.

   b) G no tiene subgrupos triviales distintos de $\{e\}$ y G, entonces G es cíclico de orden primo.

   c) Supongamos que G tiene un subgrupo H no trivial, y $\mathtt{Ord}(H) < \mathtt{Ord}(G)$. Si $p|\mathtt{Ord}(H)$ habríamos terminado.

   Supongamos que $p \not| \mathtt{Ord}(H)$. Luego

   $$p \left| \frac{\mathtt{Ord}(G)}{\mathtt{Ord}(H)} \right.$$

   y por lo tanto

   $$p| \ \mathtt{Ord} \left(\frac{G}{H} \right)$$

   Como G/H es abeliano y

   $$\mathtt{Ord} \left(\frac{G}{H} \right) < \mathtt{Ord}(G),$$

   aplicamos hipótesis de inducción a G/H. Luego existe un elemento $Hg \in G/H$ de orden p. Luego

   $$(Hg)^p = Hg^p = H$$

   es decir, $g^p \in H$ y $g \notin H$, luego

   $$(g^p)^{\mathtt{Ord}(H)} = e$$

Sea $x = g^{\mathtt{Ord}(H)}$, entonces probaremos que $x \neq e$.
En efecto si

$$g^{\mathtt{Ord}(H)} = e$$

tenemos que

$$(Hg)^{\mathtt{Ord}(H)} = H.$$

Como $\mathtt{Ord}(Hg) = p$, se debe tener $p|\mathtt{Ord}(H)$, lo cual es imposible.
Así $x \neq e$ y $x^p = e$. Luego

$$\mathtt{Ord}(x) = p$$

Con esto termina la demostración del primer caso.

2. G no abeliano.

   Nuevamente usamos inducción sobre el orden de G.

   Si $\mathtt{Ord}(G) = 1$ no hay nada que probar.

   Si G tiene un subgrupo H, tal que $p|\mathtt{Ord}(H)$ tenemos la conclusión del teorema.

   Supongamos que p no divide al orden de ningún subgrupo de G. En particular, si $a \notin \mathcal{Z}(G)$ entonces $N(a) \neq G$ y por lo tanto $p \not| N(a)$. Luego se tiene la ecuación de la clase

$$\mathtt{Ord}(G) = \mathtt{Ord}\left(\mathcal{Z}(G)\right) + \sum_{a \notin \mathcal{Z}(G)} \frac{\mathtt{Ord}(G)}{\mathtt{Ord}(N(a))}$$

   Puesto que $p|\mathtt{Ord}(G)$ y $p \not|\mathtt{Ord}(N(a))$ se tiene que $p|\frac{\mathtt{Ord}(G)}{\mathtt{Ord}(N(a))}$, si $a \notin \mathcal{Z}(G)$. Luego

$$p \left| \mathtt{Ord}(G) - \sum_{a \notin \mathcal{Z}(G)} \frac{\mathtt{Ord}(G)}{\mathtt{Ord}(N(a))} \right.$$

   y por lo tanto

$$p|\mathtt{Ord}(\mathcal{Z}(G))$$

   Pero hemos supuesto que p no dividía al orden de ningún subgrupo propio de G. Como consecuencia de esto debemos tener $\mathcal{Z}(G) = G$, con lo cual G es abeliano. Luego aplicamos el primer caso.

□

2.2. Teoremas de Sylow

En esta sección probaremos unos de los teoremas más importantes de toda la teoría de grupos finitos, como lo son los teoremas de Sylow. Si G es un grupo cuyo orden es divisible por una potencia de un primo p, entonces los teoremas de Sylow garantizan la existencia de un subgrupo de G, cuyo orden es la potencia dada de p.

Para demostrar estos teoremas necesitamos aplicar una técnica nueva para contar elementos dentro de un conjunto, a partir de un grupo dado, la cual se conoce con el nombre de Acción de Grupos.

Definición 2.20 Sea A un conjunto y G un grupo. Diremos que G **actúa** sobre A, si existe una función $\phi : G \times A \longrightarrow A$ que satisface

1. Para todo $g \in G$, la aplicación
$$\begin{aligned} \phi_g : A &\longrightarrow A \\ a &\longrightarrow \phi(g, a) \end{aligned}$$
es una permutación del conjunto A.

2. La aplicación
$$\begin{aligned} G &\longrightarrow S(A) \\ g &\longrightarrow \phi_g \end{aligned}$$

es un morfismo de grupos, donde $S(A)$ denota el conjunto de todas las permutaciones del conjunto A.

Observación: De acuerdo con la condición 2 se tienen las siguientes fórmulas de composición.

1. $\phi_a \phi_b = \phi_{ab}$, para todo a y b en G.
2. $\phi_{g^{-1}} \phi_g = \phi_e = Id$, para todo g en G.

Introducimos a continuación un par de conceptos muy útiles para el conteo de los elementos de un conjunto en donde está definida una acción.

Definición 2.21 Sea G un grupo, el cual actúa sobre un conjunto A, entonces para todo a en A, se define la **órbita** de a bajo G como el conjunto

$$A_a = \{\phi(g, a) \mid g \in G\}$$

Observación: Es fácil verificar que el conjunto de las distintas órbitas de A bajo todos los elementos de G establece una partición del conjunto A.

Definición 2.22 Sea G un grupo, el cual actúa sobre un conjunto A, entonces para todo $a \in A$ se define el **estabilizador** de a en G como el conjunto

$$Est_a = \{g \in G \mid \phi(g, a) = a\}$$

Observación: Para todo a en A, Est_a es un subgrupo de G.

El siguiente teorema permite calcular el número de elementos dentro de cada órbita.

Teorema 2.23 Sea G un grupo finito, el cual actúa sobre un conjunto A finito, entonces para todo $a \in A$ se tiene

$$\texttt{Ord}(A_a) = [G : Est_a] = \frac{\texttt{Ord}(G)}{\texttt{Ord}(Est_a)}$$

Demostración. Sea $\mathcal{C}_a$ el conjunto de las clases laterales derechas de Est_a en G. Consideremos la aplicación

$$\begin{aligned} \Psi : \mathcal{C}_a &\longrightarrow A_a \\ g\ Est_a &\longrightarrow \phi_g(a) \end{aligned}$$

donde $\phi_g(a)$ denota la aplicación de g sobre el elemento a.

En primer lugar probaremos que ϕ está bien definida, para lo cual supongamos que $g_1\ Est_a = g_2\ Est_a$ para algunos g_1, g_2 en G, entonces se tiene $g_1 g_2^{-1} \in Est_a$ si y sólo si $\phi_{g_1^{-1}g_2}(a) = a$.

Luego $\phi_{g_1^{-1}}\phi_{g_2}(a) = a$, si y sólo si $\phi_{g_2}(a) = \phi_{g_1}(a)$. Con esto hemos probado que la función está bien definida. Repitiendo los pasos en sentido inverso, se prueba la inyectividad de ψ. Luego la función es biyectiva y de esto se deduce la conclusión del teorema. □

Damos inicio ahora a una serie de resultados combinatorios necesarios para probar el primer teorema de Sylow. Sea S un conjunto de n elementos, entonces el número de formas de escoger k elementos entre los n es dado por:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{2.2}$$

Lema 2.24 Sea $n = p^\alpha m$, donde p es primo y $p^r | m$ pero $p^{r+1} \nmid m$. Entonces

$$p^r \left| \binom{n}{p^\alpha} \quad \text{pero} \quad p^{r+1} \nmid \binom{n}{p^\alpha} \right.$$

Demostración. De (2.2) obtenemos

$$\begin{aligned} \binom{p^\alpha m}{p^\alpha} &= \frac{(p^\alpha m)!}{(p^\alpha)!(p^\alpha m - p^\alpha)!} \\ &= \frac{p^\alpha m(p^\alpha m - 1)\cdots(p^\alpha m - p^\alpha + 1)}{p^\alpha(p^\alpha - 1)(p^\alpha - 2)\cdots(p^\alpha - p^\alpha + 1)} \end{aligned} \tag{2.3}$$

Observando la expresión (2.3), vemos que si una potencia de p, digamos p^i divide el numerador, entonces esta potencia también divide al denominador. En efecto, si $p^i | p^\alpha m - k$, $(k \geq 1)$, entonces $p^i | k$ y por lo tanto

$$p^i | p^\alpha - k.$$

Luego toda potencia de p en el numerador, se cancela con la correspondiente potencia de p en el denominador. Luego la única potencia de p en (2.3) es la que contiene m. De donde se obtiene el resultado. □

Teorema 2.25 (Primer Teorema de Sylow). Sea G un grupo finito, p es un número primo y $p^\alpha | \texttt{Ord}(G)$, entonces G tiene un subgrupo de orden p^α.

Demostración. Sea

$$\texttt{Ord}(G) = p^{\alpha}m,$$

tal que $p^r | m$, y $p^{r+1} \not| m$. Sea $\mathcal{A} = \{A_1, \ldots, A_s\}$ la familia de subconjuntos de G de tamaño p^{α}, entonces

$$s = \binom{p^{\alpha}m}{p^{\alpha}}$$

Definimos una relación sobre $\mathcal{A}$, mediante: A_i, A_j en $\mathcal{A}$ están relacionados, sí y sólo si existe un elemento $g \in G$, tal que $A_i = gA_j$. Es fácil ver que esta relación es de equivalencia.

Afirmamos que existe una clase de equivalencia, digamos $\overline{A_1}$ tal que

$$p^{r+1} | \ \texttt{Ord}(\overline{A_1})$$

Caso contrario p^{r+1} divide a todas las clases de equivalencia y por lo tanto

$$p^{r+1} | \ \texttt{Ord}(\mathcal{A})$$

entonces

$$p^{r+1} | \ \binom{p^{\alpha}m}{p^{\alpha}}$$

lo cual es imposible por el lema anterior.

Sea

$$\overline{A_1} = \{A_1, \ldots, A_n\} = \{gA_1 \mid g \in G\}$$

donde $p^{r+1} \not| n$ y sea

$$H = \{g \in G \mid gA_1 = A_1\}$$

entonces H es un subgrupo de G, y además se tiene

$$\texttt{Ord}(H) = \frac{\texttt{Ord}(G)}{n} \tag{2.4}$$

En efecto, la demostración de 2.4 se sigue de lo siguiente:

Si para algunos g_1, g_2 en G se tiene que $g_1A_1 = g_2A_1$, entonces $g_2^{-1}g_1A_1 = A_1$. Luego $g_2^{-1}g_1 \in H$, y por lo tanto las clases laterales g_1H y g_2H son iguales. Por lo tanto, el número de elementos de $\overline{A_1}$, el cual denotamos por n, es igual al número de clases laterales de H en G. Luego

$$n = \frac{\texttt{Ord}(G)}{\texttt{Ord}(H)}$$

de donde

$$\texttt{Ord}(H) = \frac{\texttt{Ord}(G)}{n}$$

Como $\texttt{Ord}(G)/n$ es un entero se tiene que todas las potencias de p que aparecen en n, se cancelan con las respectivas potencias de $\texttt{Ord}(G)$. Como la mayor potencia que divide a n es p^r, se tiene que

$$p^{\alpha} | \texttt{Ord}(H)$$

y por lo tanto

$$\texttt{Ord}(H) \geq p^{\alpha} \tag{2.5}$$

Por otro lado, $hA_1 = A_1$, para todo $h \in H$. Si tomamos $a_1 \in A_1$ fijo se obtiene

$$ha_1 \in A_1, \quad \forall h \in H$$

Luego

$$\texttt{Ord}(H) \leq \texttt{Ord}(A_1) = p^{\alpha} \tag{2.6}$$

Usando (2.5) y (2.6) obtenemos

$$\texttt{Ord}(H) = p^{\alpha}$$

Luego H es el subgrupo buscado y con esto termina la demostración. □

Definición 2.26 Sea G un grupo finito de orden $p^{\alpha}m$, donde p no divide a m, entonces un subgrupo H de G de orden p^{α} se llama un $p-$**grupo de Sylow** de G.

Más adelante veremos los otros dos teoremas de Sylow, que nos darán información sobre la cantidad de $p-$grupos de Sylow dentro de un grupo G. Antes de llegar a estos teoremas necesitamos una serie de definiciones y resultados sobre grupos conjugados.

Definición 2.27 Sea G un grupo y H subgrupo de G. Para cualquier $a \in G$, el conjunto

$$aHa^{-1} = \{aha^{-1} \mid h \in H\}$$

se llama **grupo conjugado** de H inducido por a.

Es fácil comprobar que dicho conjunto es un subgrupo de G.

Observación: Es claro que si H' es un conjugado de H, entonces H' y H tienen el mismo orden.

Definición 2.28 Sea G un grupo. Un subgrupo H de G se dice **invariante** o **autoconjugado bajo** a si y sólo si

$$aHa^{-1} = H.$$

Observación: Es claro que si $a \in H$, entonces H es invariante bajo a.

Si H es un subgrupo normal de G, entonces H es invariante bajo todos los elementos de G.

Definición 2.29 Sea G un grupo y H, K subgrupos de G, entonces el conjunto:

$$N_k(H) = \{k \in K \mid kHk^{-1} = H\}$$

se denomina el **normalizador** de H en K.

Observación: Si en la definición anterior tenemos $K = G$, entonces denotamos $N_G(H)$ por $N(H)$ y lo llamamos el **normalizador** de H.

Proposición 2.30 Sean H y K subgrupos de G. El número de conjugados de H, inducidos por todos los elementos de K, es igual al índice

$$[K \ : \ N_K(H)]$$

Demostración. Sea $\mathcal{B}$ el conjunto de todos los conjungados de H, inducidos por los elementos de K y definamos la función

$$\begin{array}{rccc} f & : & K & \longrightarrow & \mathcal{B} \\ & & k & \longrightarrow & kHk^{-1} \end{array}$$

Es claro que f es sobre. Veamos en que situación dos elementos distintos de K, digamos k_1 y k_2 pueden tener imágenes iguales.

Sea

$$k_1Hk_1^{-1} = k_2Hk_2^{-1}$$

si y sólo si

$$k_1^{-1}k_2H(k_1^{-1}k_2)^{-1} = H$$

si y sólo si

$$k_1^{-1}k_2 \in N_K(H)$$

Luego las imágenes de k_1 y k_2 son iguales si y sólo si estos elementos están en la misma clase lateral de $N_K(H)$ en K. Por lo tanto el número de elementos distintos de $\mathcal{B}$ es igual al número de clases laterales de $N_K(H)$ en K, el cual viene dado por:

$$[K \ : \ N_K(H)]$$

□

Teorema 2.31 (Segundo Teorema de Sylow). Sea G un grupo finito y p un número primo con $p|\mathtt{Ord}(G)$, entonces el número de $p-$grupos de Sylow de G, el cual denotaremos por s_p, satisface:

$$s_p \equiv 1 \quad \text{mód} \ \ p \ \ \text{y} \ \ s_p|\mathtt{Ord}(G).$$

Demostración. Sea $\mathcal{D}$ el conjunto de todos los $p-$grupos de Sylow de G ($\mathcal{D}$ es diferente del vacío por el primer teorema de Sylow). Sea P un elemento de $\mathcal{D}$, entonces P actúa sobre $\mathcal{D}$ por conjugación, es decir mediante la acción

$$\begin{array}{l} \phi : P \times \mathcal{D} \longrightarrow \mathcal{D} \\ (g, P_i) \longrightarrow gP_ig^{-1} \end{array}$$

Es claro que esta acción es sobreyectiva, pues si P_i es cualquier elemento de $\mathcal{D}$, se tiene

$$P_i = eP_ie^{-1}$$

donde e es el elemento neutro de P.

Entonces, el número de elementos de $\mathcal{D}$, el cual llamamos s_p, se obtiene

$$s_p = \sum_{Q \in \mathcal{D}} \mathtt{Ord}(\mathcal{D}_Q)$$

donde $\mathcal{D}_Q$ es la órbita del elemento Q en $\mathcal{D}$.

Tenemos dos posibilidades para Q.

1. Si $Q = P$, entonces
$$\mathcal{D}_P = \{gPg^{-1} | g \in P\} = P$$
luego esta órbita consiste de un sólo elemento.

2. Si $Q \neq P$, entonces
$$\texttt{Ord}(\mathcal{D}_Q) = \frac{\texttt{Ord}(P)}{\texttt{Ord}(Est_Q)} = \frac{p^\alpha}{\texttt{Ord}(N_P(Q))} = p^\beta$$
con $\beta \geq 0$.
Como $P \neq Q$, se tendrá $N_P(Q) \neq P$ y por lo tanto $\beta > 0$.

En conclusión se tiene que
$$s_p = 1 + p^{\alpha_1} + p^{\alpha_2} + \cdots + p^{\alpha_n} \tag{2.7}$$
y por lo tanto $s_p \equiv 1 \mod p$. □

En el tercer teorema de Sylow probaremos que todos los $p-$grupos de Sylow son conjugados entre sí, entonces si se elige un $p-$grupo P los restantes $p-$grupos aparecen en la órbita de P cuando el grupo G actúa sobre $\mathcal{D}$ por conjugación. El tamaño de dicha órbita viene dado por
$$\texttt{Ord}(\mathcal{D}_P) = \frac{\texttt{Ord}(G)}{\texttt{Ord}(Est_P)} = \frac{\texttt{Ord}(G)}{\texttt{Ord}(N(P))} = [G : N(P)]$$
donde $N(P)$ es el normalizador de P.

Teorema 2.32 (Tercer Teorema de Sylow). Sea G un grupo finito y $p|\texttt{Ord}(G)$, entonces todos los $p-$grupos de Sylow son conjugados.

Demostración. Sean P un $p-$subgrupo de Sylow y Q otro $p-$subgrupo de Sylow que no se encuentre entre los conjugados de P.

Entonces calculemos el número total de conjugados de Q, usando la acción del grupo P sobre el conjunto de los conjugados de Q.

En primer lugar, el número de conjugados de Q, por elementos de P (la órbita de Q) viene dado por:
$$[P \ : \ N_P(Q)] = \frac{\texttt{Ord}(P)}{\texttt{Ord}(N_P(Q))} = p^\beta \quad \text{con } \beta \geq 0 \tag{2.8}$$
Si asumimos $\beta = 0$, se tendrá
$$\texttt{Ord}(P) = \texttt{Ord}(N_P(Q)))$$

lo cual implica

$$P = N_P(Q)$$

y por lo tanto $P = Q$, lo cual es una contradicción.

Si hay otro conjugado de Q, aparte de los señalados en (2.8), sea Q_1 otro conjugado y repitamos el proceso. Luego el número total de conjugados de Q (contando todas las órbitas) vendrá dado por

$$h' = p^{\beta_1} + p^{\beta_2} + \cdots + p^{\beta_s} \quad \text{con} \quad \beta_i > 0.$$

donde ($\beta = \beta_1$) Por lo tanto $h' \equiv 0 \mod p$, lo cual es imposible por (2.7).

Con esto se finaliza la demostración. □

Capítulo 3

Clasificación teórica de grupos finitos

3.1. Grupos de orden p

Resultado 3.1 Cualquier grupo de orden p, donde p es un número primo, es isomorfo al grupo cíclico $\mathbb{Z}_p$

Demostración. La demostración del resultado sigue del Teorema de Cauchy (2.19). Sea G un grupo de orden p. Como p divide a p tenemos que existe algún elemento de orden p, digamos g, de orden p (el orden del grupo G). Entonces tenemos que $\langle g \rangle$, es isomorfo a $\mathbb{Z}_p$, tiene orden p y entonces necesariamente $\mathbb{Z}_p \cong G$. □

3.2. Grupos de orden p^2

Resultado 3.2 Cualquier grupo de orden p^2, donde p es un número primo, es isomorfo a $\mathbb{Z}_{p^2}$ o $\mathbb{Z}_p \times \mathbb{Z}_p$

Demostración. En este caso G es un p-grupo. Si G tiene un elemento de orden p^2, entonces G es cíclico y por tanto isomorfo a $\mathbb{Z}_{p^2}$. En el caso de que G no tenga algún elemento de orden p^2, entoces por el Teorema de Cauchy (2.19) se tiene que G contiene un elemento a de orden p. Sea A el grupo cíclico generado por a, deducimos que el orden de A es p, por lo que A no es todo G, además por el Primer Teorema de Sylow (2.25) se afirma que $A \triangleleft G$. Sea $b \in G \setminus \langle a \rangle$, el orden de b divide al orden de G y no es 1 o p^2, por lo que b es también de orden p. Denotamos por B el subgrupo cíclico de G generado por b, por el mismo argumento concluimos que $B \triangleleft G$. Entonces $A \cap B = \{e\}$, pues si $c \in (A \cap B) \setminus \{e\}$, c sería un generador para A y B, y se concluiría que $A = B$, lo cual es falso. Así tenemos que AB es un subgrupo de G y su orden es p^2, por lo que $AB = G$. En este punto se han logrado las condiciones del lema (2.6), de donde se concluye que G es producto directo de A y B, y por tanto isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_p$. □

3.3. Grupos de orden pq

En esta sección se enuncian y demuestran con detalle los siguientes resultados:

Resultado 3.3 Siendo $n = pq$, con $2 \leq p < q$, donde p y q son números primos absolutos, si existe un grupo G de orden n para el cual el centro $\mathcal{Z}$ es $\{e\}$, necesariamente se cumple $q \equiv 1 \mod p$.

Resultado 3.4 Siendo $n = pq$, con $2 \leq p < q$, donde p y q son números primos absolutos, si $q \not\equiv 1$ mód p, el único grupo de orden n es el $\mathbb{Z}_n$.
Además en el caso en que $q \equiv 1 \mod p$ probaremos la existencia y unicidad de un grupo no conmutativo.

Estudio de las órbitas de conjugación

En esta sección empezamos el estudio elemental de los grupos cuyo orden es producto de dos números primos, para este G denotará un grupo con la característica que su orden es pq, donde p y q son primos absolutos diferentes.

Si G actúa sobre sí mismo tenemos que G actúa por conjugación, esto es de la definición de acción de grupo, se reduce a definir el isomorfismo $\sigma_g : G \to G$

$$\sigma_g(a) = gag^{-1}$$

así entonces si $a \in G$ entonces la órbita de a es el conjunto:

$$A_a = \{gag^{-1} \ : \ g \in G\}$$

y es llamada también *clase de conjugación de a*. Obsérvese que si $a \in \mathcal{Z}(G) = \{g \in G \ : \ gz = zg \, \forall z \in G\}$, entonces $A_a \ni gag^{-1} = gg^{-1}a = ea = a \quad \forall g \in G$, esto es $A_a = \{a\}$. Si $a \in G$ entonces el estabilizador de a es el conjunto

$$C_G(a) = \{g \in G \ : \ ga = ag\}$$

en este caso (G actuando sobre sí mismo) también se le llama el centralizador de a en G.

Otra observación: Si $a \in \mathcal{Z}(G)$ entonces $C_G(a) = G$, en efecto: la inclusión $C_G(a) \subset G$ es inmediata, veamos la otra: sea $g \in G$, entonces $G \ni aga^{-1} = aa^{-1}g = g$, esto es: $ag = ga$ y así $g \in C_G(a)$ y así conseguimos la igualdad.

Haciendo que G actúe sobre sí mismo mediante los automorfismos internos, tendremos las correspondientes órbitas de conjugación. Cada una de ellas tiene cardinal divisor de n (desde que son subgrupos). Como ya vimos las órbitas de cardinal uno corresponden a elementos centrales de G. Si denotamos por $\mathcal{Z}(b)$ al centralizador de un elemento $b \in G$, $\mathcal{Z}$ al centro del grupo y $\alpha = \texttt{Ord}(\mathcal{Z})$ la cantidad de órbitas de cardinal uno, caben tres posibilidades:

1. $\alpha = n$.
   En este caso G es abeliano. Como p y q son primos entre sí, existen subgrupos H y K tales que
   $$G = HK \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq} = \mathbb{Z}_n.$$

2. $1 < \alpha < n$.
   Supongamos que hay al menos una órbita de cardinal p siendo b un elemento de esta órbita que no es la identidad (pues tiene orden p), su estabilizador tiene orden q, pues en virtud del teorema (2.23):

   $$\mathtt{Ord}(A_a) = \frac{\mathtt{Ord}(G)}{\mathtt{Ord}(\mathcal{Z}(b))} = \frac{pq}{\mathtt{Ord}(\mathcal{Z}(b))} = p, \text{ de donde se deduce que } \mathtt{Ord}(\mathcal{Z}(b)) = q$$

   Será cíclico y como $b \in \mathcal{Z}(b)$, se tiene $\mathcal{Z}(b) = \langle b \rangle$. Más aún, como $\mathcal{Z} \subseteq \mathcal{Z}(b)$ y $\mathcal{Z} \neq \{e\}$, entonces $\mathcal{Z} < \mathcal{Z}(b)$ esto es que $\mathtt{Ord}(\mathcal{Z})|q$, por lo que $\mathtt{Ord}(\mathcal{Z}) = q$ y se tiene $\mathcal{Z} = \langle b \rangle$. Como $\mathcal{Z}$ es normal en G se cumple la igualdad $\mathtt{Ord}(G/\mathcal{Z}) = \mathtt{Ord}(G)/\mathtt{Ord}(\mathcal{Z}) = pq/q = p$, entonces el cociente $G/\mathcal{Z}$ será cíclico, de orden p, luego existe un $a \in G$ tal que

   $$G/\mathcal{Z} = \{\mathcal{Z}, a\mathcal{Z}, a^2\mathcal{Z}, \ldots, a^{p-1}\mathcal{Z}\}.$$

   Entonces,

   $$p = \mathtt{Ord}(a\mathcal{Z}) = \mathtt{Ord}(A_a)|\mathtt{Ord}(a) \Rightarrow \mathtt{Ord}(a) = p$$

   (También podría ser el orden de a igual a n, pero ello contradice la hipótesis $\alpha < n$). Como b es central, se tiene $ab = ba$, luego ab es de orden n. Esto contradice de nuevo la hipótesis $\alpha < n$, luego en este supuesto es imposible la existencia de órbitas de cardinal p.
   Puesto que no se ha usado para nada el hecho de que $p < q$, cambiando el papel de ambos números, se concluye también que no pueden existir órbitas de cardinal q.
   De ambas exclusiones, lo que deducimos es el caso $1 < \alpha < n$ es imposible.

3. $\alpha = 1$.
   Si hay β de cardinal p y γ de cardinal q, se tiene

   $$1 + \beta p + \gamma q = pq \Rightarrow \beta p \equiv q - 1 \mod q.$$

   Como $q > 1$ y $\mathbb{Z}_q$ es un campo, se deduce que β no puede ser nulo. Existiendo, pues, al menos una órbita de cardinal p, deducimos como en la parte anterior la existencia de un elemento b de orden q, tal que

   $$\mathcal{Z}(b) = \langle b \rangle,$$

   si bien ahora no se trata del centro porque éste lo estamos suponiendo neutro.

A continuación vamos a demostrar varios lemas de interés para nuestro estudio, después de demostrar los lemas estableceremos estas conclusiones para los subgrupos $H = \langle a \rangle$ y $K = \langle b \rangle$ donde $a \notin \langle b \rangle$.

Lema 3.5 Sea G un grupo de orden pq no conmutativo, donde p y q son primos absolutos distintos, si $K = \langle b \rangle$ tiene orden q donde $b \in G$ y $H = \langle a \rangle$ donde $a \in G \setminus K$ entonces:

1. $H \cap K = \{e\}$.
2. Al suponer dos exponentes $0 \leq x < y < \mathtt{Ord}(a)$, entonces, $a^x K \neq a^y K$.
3. $\mathtt{Ord}(a) = p$

4. $G = HK$

Demostración.

1. Sea $h \in H \cap K$, entonces existe x tal que $0 \leq x < \texttt{Ord}(a)$ que satisface que $a^x = h$, como las opciones para $\texttt{Ord}(a)$ son p o q, entonces $\texttt{MCD}(\texttt{Ord}(a), x) = 1$ y así se verifica que $\langle a^x \rangle = \langle a \rangle = H$, por lo que $a^x \in H$ y también existe y tal que $(a^x)^y = a$. Como $h \in K$, implica que $a^x \in K$ y como K es cíclico se garantiza que: $(a^x)^y = a \in K$ y así se ha establecido que:

$$\text{Si } a^x \in K \Rightarrow a \in K, \text{ si } x \neq 0$$

en contra de su elección. Por tanto, $x = 0$. Esto prueba que $H \cap K = \{e\}$.

2. Si se diera la igualdad, tendríamos $a^x K = a^y K \Leftrightarrow a^x \equiv a^y \mod K \Leftrightarrow a^y (a^x)^{-1} = a^y a^{-x} = a^{y-x} \in K$
$$\Rightarrow a^{y-x} \in H \cap K \Rightarrow a^{y-x} = e \Rightarrow y - x = 0 \Rightarrow x = y.$$

3. Supongamos que $\texttt{Ord}(a) = q$, según lo anterior, habría al menos q clases laterales. Esto es imposible porque, al ser K de orden q, su índice es

$$n/q = p < q.$$

(Como la única condición para a es la $a \notin K$, se tiene que todos los elementos del complemento conjuntista de K son de orden p, si $x \notin K$, es decir $x \in K^c = \{hk : h \in H \text{ y } k \in K \text{ y } k \neq e\}$,[1] es de orden p, esto es, si $x \in K^c$, existen $a \in H$ y $K \ni b \neq e$ tal que $x = ab$, y el orden de este elemento es p.

4. Puesto que $G = K \sqcup aK \sqcup a^2K \sqcup \cdots \sqcup a^{p-1}K$, todo elemento $g \in G$ es de la forma $g = a^x b^u$, con $0 \leq x < p, 0 \leq u < q$.

□

Teorema 3.6 Si G es un grupo no abeliano de orden pq, donde p y q son primos absolutos distintos y si K es un subgrupo de G de orden q, entonces K es normal en G.

Demostración. Sea u un número entero tal que $0 \leq u < q$. Si $u = 0$, $g^{-1}b^u g = g^{-1}b^0 g = e \in K$, para cualquiera que sea $g \in G$. En caso contrario ($u \neq 0$), se tiene

$$\texttt{Ord}(g^{-1}b^u g) = \texttt{Ord}(b^u) = q \Rightarrow g^{-1}b^u g \in K.$$

Vamos a demostrar que $\texttt{Ord}(g^{-1}b^u g) = \texttt{Ord}(b^u)$. Sea $\texttt{Ord}(g^{-1}b^u g) = r$ y $\texttt{Ord}(b^u) = s$:

- $(g^{-1}b^u g)^r = g^{-1}(b^u)^r g = e$, entonces $s|r$
- Ahora como $(b^u)^s = e$, tenemos que $g^{-1}(b^u)^s g = (g^{-1}b^u g)^s = e$, de donde $r|s$

[1] la demostración de que el complemento de K coincide con este conjunto se argumenta ocupando el lema (3.5).

de donde se concluye que $r = s$. □

Corolario 3.7 Sea G un grupo de orden pq no conmutativo, donde p y q son primos absolutos distintos, si $K = \langle b \rangle$ tiene orden q donde $b \in G$ y $H = \langle a \rangle$ donde $a \in G \setminus K$ entonces, existe un exponente μ tal que $2 \leq \mu \leq q-1$ para el cual

$$a^{-1}ba = b^{\mu}.$$

Demostración. Por la normalidad de K, este exponente existe y no supera a $q-1$. No puede valer 0 porque ello implicaría $b = e$. No puede valer 1 porque ello nos conduciría al caso conmutativo. □

Observaciones:

1. Para todo $v \in [0, q-1]$ se cumple $a^{-1}b^v a = b^{\mu v}$, basta ver que $a^{-1}b^v a = (a^{-1}ba)^v = (b^{\mu})^v = b^{\mu v}$. Más aún , para todo $x \in [0, p-1]$ se cumple

$$a^{-x}ba^x = b^{\mu^x}$$

Si se razona por recurrencia: Para $x = 0$, 1 es de inmediata comprobación. En general,

$$\begin{aligned} a^{-(x+1)}ba^{x+1} &= a^{-1}(a^{-x}ba^x)a \\ &= a^{-1}b^{\mu^x}a \\ &= a^{-1}\underbrace{bb\cdots b}_{\mu^x-\text{veces}}a \\ &= \underbrace{a^{-1}baa^{-1}ba\cdots a^{-1}ba}_{\mu^x-\text{veces}} \\ &= \underbrace{b^{\mu}b^{\mu}\cdots b^{\mu}}_{\mu^x-\text{veces}} \\ &= (b^{\mu})^{\mu^x} = b^{\mu\mu x} = b^{\mu^{x+1}} \end{aligned}$$

2. Para todo x tal que $1 \leq x \leq p$, se cumple

$$(ab)^x = a^x b^{(\mu^{x-1}+\cdots+\mu^2+\mu+1)}.$$

Se razona por recurrencia: Para $x = 1$ es trivial. En general, usando la igualdad $ba^x = a^x b^{\mu^x}$, se tiene:

$$\begin{aligned} (ab)^{x+1} = (ab)(ab)^x &= (ab)(a^x b^{(\mu^{x-1}+\cdots+\mu^2+\mu+1)}) \\ &= a(ba^x)b^{(\mu^{x-1+\cdots+\mu^2+\mu+1})} \\ &= a(a^x b^{\mu^x})b^{(\mu^{x-1+\cdots+\mu^2+\mu+1})} \\ &= a^{x+1}b^{(\mu^x+\mu^{x-1}+\cdots+\mu^2+\mu+1)} \end{aligned}$$

Resultado 3.8 Siendo μ el exponente tal que $a^{-1}ba = b^{\mu}$ y bajo las condiciones de las observaciones anteriores, se cumple

$$\mu^{p-1} + \cdots + \mu^2 + \mu + 1 \equiv 0 \mod q.$$

Demostración. Aplicando la fórmula de la observación (2.) para $x = p$, y teniendo en cuenta la demostración del lema (3.5) literal 3 donde se dijo que tanto a y ab son de orden p, se tiene:

$$e = (ab)^p = a^p b^{\mu^{p-1}+\cdots+\mu^2+\mu+1} = b^{\mu^{p-1}+\cdots+\mu^2+\mu+1}$$

y esta igualdad es equivalente a la relación propuesta. □

Resultado 3.9 Siendo μ el exponente tal que $a^{-1}ba = b^{\mu}$, se cumple

$$\mu^p - 1 \equiv 0 \mod q.$$

Demostración. Usando la igualdad

$$\mu^p - 1 = (\mu^{p-1} + \cdots + \mu^2 + \mu + 1)(\mu - 1),$$

por ser $\mu \geq 2$, $\mathbb{Z}_q$ es un campo, y así la última igualdad es equivalente a la del resultado (3.8). □

Así llegamos a la demostración de los siguientes resultados:

Teorema 3.10 Siendo $n = pq$, con $2 \leq p < q$, donde p y q son números primos absolutos, si existe un grupo G de orden n para el cual $\mathcal{Z} = \{e\}$, necesariamente se cumple $q \equiv 1 \mod p$.

Demostración. La última fórmula indica que μ, como elemento del grupo multiplicativo U_q, debe ser de orden divisor de p, en realidad, es de orden p, porque $\mu > 1$ no puede ser de orden 1, junto con el Teorema de Fermat: $\mu^{q-1} \equiv 1 \mod q$, puede concluirse que, $p|(q-1)$ o lo que es lo mismo que $q \equiv 1 \mod p$ □

Teorema 3.11 Siendo $n = pq$, con $2 \leq p < q$, donde p y q son números primos absolutos, si $q \not\equiv 1$ mód p, el único grupo de orden n es $\mathbb{Z}_n$

Demostración. Supongamos que $\mathcal{Z} = \{e\}$, entonces por el teorema anterior concluimos que $q \equiv 1$ mód p, en contra de nuestra hipótesis. Así entonces $\mathcal{Z} \neq \{e\}$. Sea pues $\alpha = \texttt{Ord}(\mathcal{Z})$, desde que $\mathcal{Z} \neq \{e\}$, entonces $\alpha \neq 1$ y como $\mathcal{Z} < G$, entonces las posibilidades para α son p, q, y n. Vamos a demostrar que las dos primeras son imposibles:
Como el orden del grupo G es pq, el teorema de Cauchy afirma que existen subgrupos $H = \langle a \rangle$ y K de G de orden p y q respectivamente (que son cíclicos, por tener orden un primo). En efecto:
Si $\alpha = p$ entonces $\alpha = \texttt{Ord}(\langle a \rangle)$ para $a \in H$. Ahora consideremos $\langle ka \rangle < G$, con $k \notin H$, entonces $\texttt{Ord}(\langle ka \rangle) | \texttt{Ord}(G)$ y así las posibilidades para $\texttt{Ord}(\langle ka \rangle)$ son 1, p, q y pq.
Si $\texttt{Ord}(\langle ka \rangle) = 1$, entonces $\langle ka \rangle = \{e\}$ y así $ka = e$, de donde: $k = a^{-1}$ y entonces $k \in \langle a \rangle$ lo cual es un absurdo.
Supongamos que $\texttt{Ord}(\langle ka \rangle) = p$, entonces existe $j \in \mathbb{N}$ tal que $ka = a^j$ y así $k = a^{j-1}$ y entonces

$k \in \langle a \rangle$, lo cual también es imposible.
Si suponemos que $\texttt{Ord}(\langle ka \rangle) = q$ entonces $\langle ka \rangle = \langle k' \rangle$ para $k' \in G \backslash \langle a \rangle$ y entonces

$$\texttt{Ord}(\langle a \rangle \times \langle k' \rangle) = \frac{\texttt{Ord}(\langle a \rangle) \cdot \texttt{Ord}(\langle k' \rangle)}{\texttt{MCD}(\texttt{Ord}(\langle a \rangle), \texttt{Ord}(\langle k' \rangle))} = \frac{pq}{1} = pq = n$$

y así $G = \langle a \rangle \times \langle k' \rangle = \langle (a, k') \rangle = \mathcal{Z}$, así entonces $\texttt{Ord}(\mathcal{Z}) = n$ lo cual es imposible porque hemos supuesto que $\alpha = p$.
Como no se ha utilizado la hipótesis que $p < q$, el mismo procedimiento deja concluir que la posibilidad $\alpha = q$ no puede ser consistente, y así llegamos a que la única opción para α es que sea n, es decir $\mathcal{Z}$ coincide con G es decir el grupo G es cíclico de orden n: $G = \mathbb{Z}_n$ □

Simplificación con los teoremas de Sylow

El anterior estudio es elemental y por ello ha resultado prolijo. Si se recurre a los teoremas de Sylow, tenemos significativas simplificaciones

Proposición 3.12 Sea G un grupo de orden $n = pq$, donde p y q son primos tales que $2 \leq p < q$, entonces, G admite un único subgrupo K de orden q, el cual es cíclico y normal.

Demostración. Siendo s_q la cantidad de subgrupos de orden q, los teoremas de Sylow aseguran que

$$s_q \neq 0, \quad s_q \equiv 1 \mod q, \quad s_q | n.$$

Como los divisores de $n = pq$ son $1,\ p,\ q,\ pq$, y los dos últimos son nulos módulo q, se tendrá $s_q = 1$ o $s_q = p$. Pero, siendo $1 < p < q$, el valor $s_q = p$ no puede verificar la condición $s_q \equiv 1$ mód q, luego necesariamente es $s_q = 1$. Si K es tal subgrupo, será cíclico por tener orden primo y será normal por ser el único $q-$subgrupo de Sylow que admite G. □

Proposición 3.13 Si G es un grupo de orden pq, donde p y q son primos absolutos, si $q \not\equiv 1$ mód p, G admite un único subgrupo H de orden p, el cual será cíclico y normal en G. En caso contrario, o bien G admite un único subgrupo H de orden p, cíclico y normal, o bien admite q subgrupos $H_1, H_2, \ldots, H_q$, de orden p, cíclicos y conjugados entre sí.

Demostración. Siendo s_p la cantidad de subgrupos de orden p, los teoremas de Sylow aseguran que

$$s_p \neq 0, \quad s_p \equiv 1 \mod p, \quad s_p | n.$$

De los cuatro divisores $1,\ p,\ q,\ pq$, quedan descartados los valores segundo y cuarto por ser nulos módulo p. Si además, $q \not\equiv 1 \mod p$, necesariamente debe ser $s_p = 1$. En este caso, el subgrupo H de orden p será cíclico por tener orden primo y será normal por ser el único $p-$subgrupo de Sylow en G. En cambio, si $q \equiv 1 \mod p$, pueden darse las dos posibilidades $s_p = 1$ o $s_p = q$. En la segunda de ellas, los correspondientes subgrupos $H_1, H_2, \ldots, H_q$ de orden p serán cíclicos por tener orden primo y conjugados unos con otros por ser todos ellos $p-$subgrupos de Sylow de G. □

Proposición 3.14 Siendo H uno de los $p-$subgrupos (haya uno o varios) y siendo K el $q-$subgrupo normal, se prueba que

$$G = H[K].$$

Demostración. Como el orden de cualquier elemento de $H \cap K$ es divisor común de p y q, y estos números son primos entre sí, queda que el subgrupo intersección está formado por los elementos de orden uno, o sea, se reduce a $\{e\}$. Por otra parte, la normalidad de K implica que HK sea un subgrupo de G. Al ser trivial la intersección, se cumple

$$\texttt{Ord}(HK) = \texttt{Ord}(H)\texttt{Ord}(K) = pq = n = \texttt{Ord}(G) \Rightarrow HK = G.$$

Con estas condiciones, G es efectivamente producto semidirecto de H y K. □

Proposición 3.15 Si G admite un único subgrupo H de orden p, necesariamente $G \cong \mathbb{Z}_n$.

Demostración. En este caso, además de las condiciones

$$H \cap K = \{e\},\ K \text{ normal en } G,\ HK = G,$$

se tiene que también H es normal, entonces,

$$G = H[K] \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq} = \mathbb{Z}_n.$$

□

Proposición 3.16 Siendo $n = pq$, con $2 \leq p < q$, donde p y q son números primos absolutos, si $q \not\equiv 1 \mod p$, el único grupo de orden n es el $\mathbb{Z}_n$.

Demostración. Según la proposición (3.13), la condición $q \not\equiv 1 \mod p$, nos conduce a que H sea único. Ahora basta aplicar la proposición (3.15). □

Grupos de orden pq, con p y q primos distintos

En esta sección demostraremos la existencia de un grupo no conmutativo en el caso $q \equiv 1 \mod p$. Observamos que si $p = 2$, al ser $q > p$ primo, es un número impar y siempre cumple la condición $q \equiv 1 \mod 2$. En este caso sabemos que existe un grupo no conmutativo (único, además) de orden $n = 2q$, tratándose de grupo diédrico de orden q. Tratamos ahora de generalizar esta existencia y unicidad. Situémonos en el grupo multiplicativo U_q, cíclico y de orden $q - 1$ ya que q es primo. Sea γ un generador de U_q. Como ya hemos tenido ocasión de mostrar:

$$p|(q-1) \Leftrightarrow (q-1) = pc \Leftrightarrow q = pc + 1 \Leftrightarrow q \equiv 1 \mod p.$$

Luego en U_q existe un subgrupo de orden p. Será el generado por

$$\gamma^{(q-1)/p},$$

y todos sus elementos salvo el 1, serán de orden p. Sea $\mu \neq 1$ uno de ellos.

Tomemos los grupos $H = \mathbb{Z}_p = \langle a \rangle$ y $K = \mathbb{Z}_q = \langle b \rangle$. Puesto que $\mu < q$, será primo con él. Esto asegura que la aplicación

$$\alpha : K \to K, \text{ con la regla de asignación } \alpha(b^v) = b^{v\mu}$$

es un automorfismo de K. Para cada $x \in [1,p], \alpha^x$ será otro automorfismo. Cumplirá

$$\alpha^x(b) = b^{\mu^x}, \alpha^x(b^v) = b^{v\mu^x}$$

La aplicación

$$\rho : H \to \mathtt{Aut}(K), \text{ con la regla de asignación } \rho(a^x) = \alpha^x$$
$$\rho(a^x a^y)(b^v) \ = \rho(a^{x+y})(b^v) = b^{v\mu^{x+y}}$$
$$\rho(a^y)(\rho(a^x)(b^v)) = \rho(a^y)(b^{v\mu^x}) = b^{(v\mu^x)\mu^y}$$

Es inyectivo pues: $\rho(a^x)(b^v) = b^{v\mu^x} = b^v \Rightarrow v(\mu^x - 1) \equiv 0 \mod q \Rightarrow \mu^x - 1 \equiv 0 \Rightarrow x = 0$, entonces es un monomorfismo que aplica H sobre un subgrupo de $\mathtt{Aut}(K)$ que es isomorfo al subgrupo $\langle\mu\rangle$ de U_q.

Esto permite construir el grupo

$$G = H \times_\rho K,$$

que es un producto semidirecto exterior de H por K. La operación será

$$(a^x,\ b^u)(a^y,\ b^v) = (a^x a^y,\ \rho(a^y)(b^u)b^v) = (a^{x+y},\ b^{u\mu^y+v})$$

Este grupo es de orden $n = pq$ y es no conmutativo:

$$(e_H,\ b)(a,\ e_K) = (a,\ b^\mu) \neq (a,\ e_K)(e_H,\ b) = (a,\ b) \text{ porque } \mu > 1.$$

Hay un subgrupo $K^* = \{(e,\ b^u)\}$ de orden q, isomorfo a K. Este modelo responde a la propuesta.

Supongamos que existe otro grupo G' con las mismas características de G, entonces debe verificarse que son isomorfos. Sean $d,\ c$ en G' cumpliendo todos los requisitos del estudio. $c^{-1}dc = d^{\mu^h}$ y además el orden de c y d sean p y q respectivamente.

Se tiene $\varphi : H \times_\rho K \to G'$, con la regla de asignación

$$\varphi(a^x,\ b^u) = c^{kx}d^u$$

Si $\mu^h = \mu'$, debe ser $hk \equiv 1 \mod p$.

Veamos que φ es un morfismo de grupos: Veamos que $\varphi((a^x, b^u)(a^y, b^v)) = \varphi(a^{x+y},\ b^{u\mu^y+v}) = c^{kx+ky}d^{u\mu^y+v}$. Por otra parte:

$$\begin{aligned}
\varphi(a^x, b^u)\varphi(a^y,\ b^v) &= (c^{kx}d^u)(c^{ky}d^v) \\
&= c^{kx}c^{ky}(c^{-ky}d^u c^{ky})d^v \\
&= c^{kx+ky}(c^{-ky}dc^{ky})^u d^v \\
&= c^{kx+ky}(d^{(\mu^h)^{ky}})^u d^v \\
&= c^{kx+ky}d^{u\mu^{hky}+v} \\
&= c^{kx+ky}d^{u\mu^y+v}
\end{aligned}$$

Comprobemos que

$$c^{kx}d^u = e \Rightarrow x = u = 0,$$

en efecto, si $c^{kx}d^u = e$ entonces $c^{pkx}d^{pu} = e^p$ esto es $d^{pu} = e$, es decir $q|pu$ pero p y q son primos absolutos, significa que $q|u$ además desde que $0 \leq u < q$ tenemos que $u = 0$, por un argumento similar puede concluirse que $x = 0$, y así se demuestra que φ es un morfismo inyectivo.

Como (a^x, b^u) y $c^{kx}d^u$ son del mismo orden, esto prueba que es sobreyectiva y entonces $G \cong G'$.

En efecto: Es obvio que el orden de (a^x, b^u) es pq, sea $m = \texttt{Ord}(c^{kx}d^u)$:

$$(c^{kx}d^u)^{pq} = c^{pqkx}d^{pqu} = (c^p)^{qkx}(d^q)^{pu} = e$$

así $m|pq$, las posibilidades para m son 1, p, q y pq, es claro, que $m = 1$ no puede ser, pues c y d no son la identidad, además k, x no son múltiplos de p y u no es múltiplo de q.

La posibilidad $m = p$ es también inconsistente: $(c^{kx}d^u)^p = d^{px} = e$, entonces $q|px$, por lo que $q|x$, pero $x \in [1, p-1]$, lo cual es imposible. De manera análoga puede concluirse que el caso $m = q$ es también imposible, quedando como única posibilidad $m = pq$.

Capítulo 4

Grupos en GAP

En este capítulo se expone el uso de GAP (Groups, Algorithms, Programming) en la teoría de grupos especialmente finitos, además se muestran ejemplos detallados de algunos resultados que tienen aplicaciones concretas, algunas de estas exigen muchas operaciones y cálculos, que si se hicieran manualmente requieren un tiempo considerablemente largo; en este sentido es una ventaja disponer de un recurso computacional que permita efectuar cálculos y operaciones para soluciones en poco tiempo.

4.1. Grupos cíclicos, grupos abelianos y grupos diédricos

Comenzamos advirtiendo que la funcionalidad `IsFpGroup` estará disponible en GAP apartir de la versión 4.5

Los ejemplos más sencillos de los grupos son grupos cíclicos y el grupo de las unidades de enteros módulo m. Dado que los grupos en GAP están escritos en forma multiplicativa, los grupos cíclicos no pueden ser tomados simplemente como `Integers mod m`, en este sentido es necesario crear una estructura multiplicativa: esto se hace con el comando `CyclicGroup`.

Dicha representación se logra entender completamente cuando se estudia el Teorema Fundamental de los Grupos Abelianos Finitos. Debido a esto, es preferible crear los grupos como grupos finitamente generados, esto simplemente significa que el grupo tiene un solo generador y cada elemento es una potencia de este generador. Esto puede ser obtenido dándole como primer argumento `IsFpGroup`, por ejemplo:

```
gap> G:=CyclicGroup(IsFpGroup,6);
<fp group of size 6 on the generators [ a ]>
gap> Elements(G);
[ <identity ...>, a^-1, a, a^-2, a^2, a^3 ]
gap> List(Elements(G),Order);
[ 1, 6, 6, 3, 3, 2 ]
gap> GeneratorsOfGroup(G)[1];
a
```

Como muestra el ejemplo, el atributo `GeneratorsOfGroup` de tal grupo es una lista de longitud uno, que contiene el generador.

Los grupos abelianos finitos se pueden escribir como producto directo de grupos cíclicos, y pueden crearse de manera similar a través de `AbelianGroup` con un argumento que enumera los órdenes de factores cíclicos, por ejemplo, `AbelianGroup(IsFpGroup,[2,4])` crea $C_2 \times C_4$. Los elementos generadores naturales se pueden obtener a través de la función `GeneratorsOfGroup`.

```
gap> G:=AbelianGroup(IsFpGroup,[2,4,5]);
<fp group of size 40 on the generators [ f1, f2, f3 ]>
gap> gens:=GeneratorsOfGroup(G);
[ f1, f2, f3 ]
gap> List(gens,Order);
[ 2, 4, 5 ]
```

Lo mismo se aplica a los grupos diédricos, se crean utilizando `DihedralGroup(IsFpGroup,n)`, aunque en realidad para muchas aplicaciones podrían mejor representarse como grupos de permutaciones.

```
gap> ShowMultiplicationTable(DihedralGroup(IsFpGroup,8));
*     | <id>  r^-1  r     s     r^2   r*s   s*r   s*r^2
------+-----------------------------------------------
<id>  | <id>  r^-1  r     s     r^2   r*s   s*r   s*r^2
r^-1  | r^-1  r^2   <id>  s*r   r     s     s*r^2 r*s
r     | r     <id>  r^2   r*s   r^-1  s*r^2 s     s*r
s     | s     r*s   s*r   <id>  s*r^2 r^-1  r     r^2
r^2   | r^2   r     r^-1  s*r^2 <id>  s*r   r*s   s
r*s   | r*s   s*r^2 s     r     s*r   <id>  r^2   r^-1
s*r   | s*r   s     s*r^2 r^-1  r*s   r^2   <id>  r
s*r^2 | s*r^2 s*r   r*s   r^2   s     r     r^-1  <id>
```

4.2. Unidades en aritmética modular

Uno de los ejemplos más frecuentes de grupos son los grupos $\mathbb{Z}_m^*$. Estos pueden ser construidos a través del comando `Units`. (Más generalmente, el comando `Units` se puede aplicar a cualquier anillo, sin embargo GAP no siempre tiene un método factible para determinar, ni representar a las unidades. Así, por ejemplo, no hay una representación del grupo de los racionales no nulos $\mathbb{Q}^*$).

```
gap> Units(Integers mod 12);
<group with 2 generators>
```

4.3. Construcción de grupos a partir de objetos con nombre arbitrarios

El primer ejemplo de grupo esconde la estructura de cada elemento con un nombre. La forma más fácil de construir tales objetos en GAP es construirlos a partir de otra representación, y aplicar la funcionalidad de cambiar nombre a cada elemento del grupo, para que GAP pueda mostrarlos en la forma deseada.

Un ejemplo típico de esto (tomado del libro de texto de Gallian [13]) son las simetrías de un cuadrado, que consiste en las rotaciones $R_0, R_{90}, R_{180}, R_{270}$, y las cuatro reflexiones H, V, D, D'. En el ejemplo siguiente, se crea este grupo en GAP, utilizando permutaciones de grado 4 para codificar la aritmética de dichas simetrías. (Una observación importante: GAP opera desde la derecha, mientras que muchos libros de texto operan desde la izquierda. Para asegurar que el producto $D = H \cdot R_{90}$ sea correcto, las permutaciones se han escrito en sentido inverso al del libro de texto.)

```
gap> R90:=(1,2,3,4);;R180:=R90^2;;R270:=R90^3;;R0:=();;
gap> H:=(1,4)(2,3);;D:=H*R90;;V:=H*R180;;DP:=H*R270;;
gap> SetNameObject(R0,"R0");
gap> SetNameObject(R90,"R90");
gap> SetNameObject(R180,"R180");
gap> SetNameObject(R270,"R270");
gap> SetNameObject(H,"H");
gap> SetNameObject(V,"V");
gap> SetNameObject(D,"D");
gap> SetNameObject(DP,"D'");
gap> G:=Group(R90,H);
Group([ R90, H ])
gap> Elements(G);
[ R0, D, V, R90, D', R180, R270, H ]
gap> H*R90;
D
```

4.4. Operaciones básicas con grupos y sus elementos

Con la instrucción `Order` se puede determinar la cardinalidad de un grupo. Cuando se aplica a un elemento del grupo, lo que devuelve es el orden del elemento. La función `One` (o `Identity`) devuelve el elemento de identidad grupo. Si se desea hacer pruebas de conmutatividad en un grupo, puede auxiliarse de con la función `IsAbelian`.

Cuando se aplica la función `Elements` al grupo, ésta devuelve una lista con los elementos del grupo, que posteriormente se puede procesar usando el operador `List`.

```
gap> g:=Units(Integers mod 21);
<group with 2 generators>
gap> Order(g);
12
gap> One(g);
ZmodnZObj( 1, 21 )
gap> e:=Elements(g);
[ ZmodnZObj( 1, 21 ), ZmodnZObj( 2, 21 ), ZmodnZObj( 4, 21 ),
  ZmodnZObj( 5, 21 ), ZmodnZObj( 8, 21 ), ZmodnZObj( 10, 21 ),
  ZmodnZObj( 11, 21 ), ZmodnZObj( 13, 21 ), ZmodnZObj( 16, 21 ),
  ZmodnZObj( 17, 21 ), ZmodnZObj( 19, 21 ), ZmodnZObj( 20, 21 ) ]
```

```
gap> Order(e[3]);
3
gap> List(e,Order);
[ 1, 6, 3, 6, 2, 6, 6, 2, 3, 6, 6, 2 ]
gap>List(e,x->Position(e,Inverse(x)));
[ 1, 7, 9, 10, 5, 11, 2, 8, 3, 4, 6, 12 ]
```

Para un grupo o una lista de elementos, `ShowMultiplicationTable` devuelve la tabla de Cayley o de multiplicar.

```
gap> ShowMultiplicationTable(Units(Integers mod 8));
*        | ZnZ(1,8) ZnZ(3,8) ZnZ(5,8) ZnZ(7,8)
---------+-----------------------------------
ZnZ(1,8) | ZnZ(1,8) ZnZ(3,8) ZnZ(5,8) ZnZ(7,8)
ZnZ(3,8) | ZnZ(3,8) ZnZ(1,8) ZnZ(7,8) ZnZ(5,8)
ZnZ(5,8) | ZnZ(5,8) ZnZ(7,8) ZnZ(1,8) ZnZ(3,8)
ZnZ(7,8) | ZnZ(7,8) ZnZ(5,8) ZnZ(3,8) ZnZ(1,8)
```

4.5. Tabla de multiplicar

Una tabla de multiplicar es una matriz cuadrada de dimensión entera positiva n, que describe los productos de un conjunto de n elementos. La función `GroupByMultiplicationTable` crea un grupo a partir de la matriz dada (y devuelve `fail` si el resultado no es un grupo). Los elementos del grupo se muestran como m_i para $i = 1, \ldots,$ `Ord`(G), no hay numeración particular para el elemento identidad o inversos. Debido a que todos los elementos se enumeran como generadores, se puede acceder a ellos también como `g.`n, donde n es un número.

```
gap> m:=[ [ 4, 3, 2, 1 ], [ 3, 4, 1, 2 ], [ 2, 1, 4, 3 ], [ 1, 2, 3, 4 ] ];;
gap> g:=GroupByMultiplicationTable(m);
<group of size 4 with 4 generators>
gap> Elements(g);
[ m1, m2, m3, m4 ]
gap> One(g);
m4
gap> g.2*g.3;
m1
gap> m:=[[1,2,3,4,5],[5,1,2,3,4],[4,5,1,2,3],[3,4,5,1,2],[2,3,4,5,1]];
gap> g:=GroupByMultiplicationTable(m);
fail
```

Como una tabla de multiplicar es generalmente un objeto bastante grande, el método recomendado para la representación de los grupos en el ordenador es por ejemplo, con permutaciones, pero para cambiar la visualización de estos objetos, puede utilizarce nombres personalizados como se hizo anteriormente en los ejemplos.

Para construir la estructura multiplicativa de una tabla y sus propiedades, se puede utilizar la función `MagmaByMultiplicationTable` como se muestra acontinuación:

```
gap> m:=[ [ 1, 2, 3, 4 ], [ 2, 1, 4, 3 ], [ 3, 4, 1, 2 ], [ 4, 3, 2, 1 ] ];
[ [ 1, 2, 3, 4 ], [ 2, 1, 4, 3 ], [ 3, 4, 1, 2 ], [ 4, 3, 2, 1 ] ]
gap> g:=MagmaByMultiplicationTable(m);
<magma with 4 generators>
gap> IsAssociative(g);
true
gap> One(g);
m1
gap> List(Elements(g),Inverse);
[ m1, m2, m3, m4 ]
gap> m:=[[1,2,3,4,5],[5,1,2,3,4],[4,5,1,2,3],[3,4,5,1,2],[2,3,4,5,1]];;
gap> g:=MagmaByMultiplicationTable(m);
<magma with 5 generators>
gap> IsAssociative(g);
false
```

(Tenga en cuenta que GAP no reconoce estos objetos como "grupos", por lo que el comando `IsGroup` devolverá `false`, incluso si matemáticamente se trata de grupos. Esto significa en particular muchas operaciones teóricas del grupo no estarán disponibles para estos objetos.)

4.6. Subgrupos

Los subgrupos en GAP se crean y se almacenan típicamente dando el subgrupo de generadores. La función `Subgroup(grupo, generadores)` construye un subgrupo con generadores dados. en comparación con `Group`, las diferencias son:

- `Subgroup` comprueba si los generadores se encuentran actualmente en el grupo
- Un subgrupo puede heredar algunas de las propiedades del grupo (por ejemplo información sobre la acción de permutaciones, el orden de los grupos, o la resolubilidad) para acelerar los cálculos.

De lo contrario, no se comporta de manera diferente que `Group`, por lo que puede ser utilizado en su lugar. (Si se crea un subgrupo, su `Parent` es el grupo que se hizo como subgrupo de el) `IsSubset(group,sub)` pone a prueba la inclusión de subgrupos.

Ciertos subgrupos característicos se obtienen como `Centre`, `DerivedSubgroup`; para subgrupos de un grupo, los comandos `Normalizer(group,sub)` y `Centralizer(group,sub)` devuelven los subgrupos Normalizador y Centralizador respectivamente.

El comando `AllSubgroups` devuelve una lista de todos los subgrupos de un grupo. En general, esta lista es muy larga, y es preferible obtener los subgrupos usando clases de conjugación `ConjugacyClassesSubgroups`.

```
gap> AllSubgroups(DihedralGroup(IsPermGroup,10));
[ Group(()), Group([ (2,5)(3,4) ]), Group([ (1,2)(3,5) ]),
  Group([ (1,3)(4,5) ]), Group([ (1,4)(2,3) ]), Group([ (1,5)(2,4) ]),
  Group([ (1,2,3,4,5) ]), Group([ (1,2,3,4,5), (2,5)(3,4) ]) ]
```

Diversas series de subgrupos se pueden obtenerse con `DerivedSeries`, `CompositionSeries`, `ChiefSeries`, `LowerCentralSeries`, `UpperCentralSeries`.

4.7. Acciones de grupo

La acción de grupo sobre un conjunto es uno de los principales logros de la teoría de grupos, proporciona un marco formal para describir las simetrías de un objeto. Formalmente, la acción de un grupo G en un dominio Ω se describe por una función $\mu\colon \Omega \times G \to \Omega$ de tal manera que

$$\begin{aligned} \mu(\omega, 1) &= \omega \qquad \forall \omega \in \Omega, \\ \mu(\mu(\omega, g), h) &= \mu(\omega, gh) \qquad \forall g, h \in G, \omega \in \Omega. \end{aligned}$$

Debe observarse que esto describe una acción por la derecha, al igual que la convención general de GAP, también es coherente con la forma que GAP maneja la multiplicación de permutaciones.

Las acciones de grupo en GAP se aplican a través de un función GAP *`mu(omega,g)`*, que calcula la imagen de un punto. (GAP asume que la función prevista en efecto implementa una acción de grupo, ya que no hay manera fácil de verificar que lo sea). Aunque una función de este tipo puede ser proporcionada por el usuario, GAP en sí ya establece una serie de acciones de forma predeterminada:

`OnPoints` Esta función describe la acción a través del operador caret `^`, es decir `OnPoints(`*`p`*`,`*`g`*`)=`*`p`*`^`*`g`*. Este es por ejemplo la acción de una permutación en los puntos; la acción de un grupo en sus elementos o subgrupos a través de la conjugación ($g^h = h^{-1}gh$); o la acción de un grupo de automorfismos en sí mismo.

Esta es la acción por defecto (GAP asumirá esta acción si no se especifica alguna otra).

`OnRight` Esta función describe la acción a través de la multiplicación derecha es decir, `OnRight(`*`p`*`,`*`g`*`)=`*`p`*`*`*`g`*. Por ejemplo la acción del grupo de matrices sobre vectores fila; la acción regular de los elementos de un grupo, o de la acción derecha de un subgrupo sobre las clases laterales.

`OnTuples` Para una lista *`L`* de puntos, `OnPoints(`*`L`*`,`*`g`*`)` devuelve una lista obtenida mediante la acción sobre cada elemento *`p`* $\in$ *`L`* vía `OnPoints(`*`p`*`,`*`g`*`)`.

`Permuted` actúa permutando las entradas de una lista.

Las siguientes funciones están disponibles en GAP para calcular órbitas y estabilizadores. En todos los casos *`G`* es un grupo que actúa en el dominio *`Omega`* (normalmente en forma de lista) por la función *`mu`*, *`p`* es un punto en *`Omega`*:

`Orbit(G,p,mu)` determina la órbita de `p` bajo `G`, es decir, el conjunto de todas las imágenes diferentes.

`Orbits(G,Omega,mu)` devuelve la partición de `Omega` dada por las órbitas de `G`.

`IsTransitive(G,Omega,mu)` comprueba si todos los elementos de `Omega` se encuentran en la misma órbita en `G`.

`Stabilizer(G,p,mu)` determina el estabilizador de `p` según `G`, es decir, el subgrupo de los elementos de `G` que mantienen fijo a `p`. En particular, para algunas de las acciones predefinidas, un grupo que actúa sobre sí mismo o grupos de permutaciones que actúan sobre puntos, listas o conjuntos de puntos, GAP implementa métodos especiales para hacer cálculos eficientes a la hora de calcular los estabilizadores, incluso en el caso de grupos grandes. En el caso general, para calcular el estabilizador se necesita calcular la órbita, por esta razón se limita a los casos en los que la longitud de la órbita (el índice del estabilizador) es relativamente pequeña como para caber en la memoria de ordenador donde se realizan los cálculos.

```
gap> g:=SymmetricGroup(3);
Sym( [ 1 .. 3 ] )
gap> Orbit(g,1,OnPoints);
[ 1, 2, 3 ]
gap> Orbit(g,[1,2],OnSets);
[ [ 1, 2 ], [ 2, 3 ], [ 1, 3 ] ]
gap> Orbit(g,[1,2],OnTuples);
[ [ 1, 2 ], [ 2, 3 ], [ 2, 1 ], [ 3, 1 ], [ 1, 3 ], [ 3, 2 ] ]
gap> Stabilizer(g,2,OnPoints);
Group([ (1,3) ])
gap> Orbits(g,Cartesian([1..3],[1..3]),OnTuples);
[ [ [ 1, 1 ], [ 2, 2 ], [ 3, 3 ] ],
  [ [ 1, 2 ], [ 2, 3 ], [ 2, 1 ], [ 3, 1 ], [ 1, 3 ], [ 3, 2 ] ] ]
```

Los homomorfismos a grupos de permutaciones inducidas por las acciones de grupo se describen en la sección siguiente.

4.8. Homomorfismos de grupos

Fundamentalmente, hay tres formas de representar homomorfismos de grupos en GAP, con la ventaja que las operaciones con estos homomorfismos son independiente del modo en que se han creado. A continuación se describen las diferentes maneras de la crear homomorfismos:

Homomorfismos de acción

Una acción de un grupo G sobre un dominio finito Ω induce una acción mediante el homomorfismo $\varphi\colon G \to S_\Omega$ en el grupo de permutaciones en Ω. (Ver sección 4.7 para la representación general de las acciones de grupo.) Tales homomorfismos son probablemente los más fáciles de entender: como la imagen de una permutación que puede obtenerse simplemente mediante la acción de $g \in G$ en todos los puntos de Ω.

`ActionHomomorphism(`*G*`,`*Omega*`,`*mu*`)` crea un homomorfismo de acción de *G* en *Omega* a través de la función *mu*. El grupo S_Ω se representa como el grupo simétrico de los puntos $1, \ldots, n$; donde $n = \texttt{Ord}(\Omega)$, y x corresponde al x-ésimo elemento de la lista Ω.

`ActionHomomorphism(`*G*`,`*Omega*`,`*mu*`,"surjective")` crea el homomorfismo con la misma definición, pero sobre su imagen, (el último argumento es la cadena "surjective", el sinónimo "onto" también puede ser utilizado).

`Action(`*G*`,`*Omega*`,`*mu*`)` retorna la `Image` del correspondiente `ActionHomomorphism`.

```
gap> g:=SymmetricGroup(3);
Sym( [ 1 .. 3 ] )
gap> dosc:=[ [ 1, 2 ], [ 2, 3 ], [ 2, 1 ], [ 3, 1 ], [ 1, 3 ], [ 3, 2 ]
];
[ [ 1, 2 ], [ 2, 3 ], [ 2, 1 ], [ 3, 1 ], [ 1, 3 ], [ 3, 2 ] ]
gap> hom1:=ActionHomomorphism(g,dosc,OnTuples);
<action homomorphism>
gap> hom2:=ActionHomomorphism(g,dosc,OnTuples,"surjective");
<action epimorphism>
gap> Action(g,dosc,OnTuples);
Group([ (1,2,4)(3,6,5), (1,3)(2,5)(4,6) ])
gap> Image(hom1);
Group([ (1,2,4)(3,6,5), (1,3)(2,5)(4,6) ])
gap> Image(hom2);
Group([ (1,2,4)(3,6,5), (1,3)(2,5)(4,6) ])
gap> Range(hom1);
Sym( [ 1 .. 6 ] )
gap> Range(hom2);
Group([ (1,2,4)(3,6,5), (1,3)(2,5)(4,6) ])
```

Uso de generadores

Puesto que cada elemento de un grupo puede ser descrito mediante sus generadores (vea la sección 4.9), un homomorfismo $\varphi\colon G \to H$ se define de forma única por medio de los generadores $\{g_i\}$ de G, así como sus imágenes $\{g_i^\varphi\}$ en H. Esta es la forma predeterminada que GAP utiliza para representar homomorfismos que no provienen de una acción.

`GroupHomomorphismByImages(`*G*`,`*H*`,`*gens*`,`*imgs*`)` crea un homomorfismo donde *gens* es la lista g_i de los generadores de G y *imgs* la correspondiente lista de sus imágenes. El homomorfismo resultante tiene `Kernel` igual a *G* y `Rango` igual a *H*, es decir, no es necesario *imgs* para generar a *H*.

GAP pondrá a prueba que esta imagen asignada realmente corresponde a un homomorfismo, en caso que no corresponda a un homomorfismo la llamada a la función devolverá `fail`. Esta prueba puede llevar un tiempo considerable en el caso de grupos grandes. La función `GroupHomomorphismByImagesNC(`*G*`,`*H*`,`*gens*`,`*imgs*`)` se saltará esta prueba y confiará en el usuario.

```
gap> g:=Group((1,2,3,4),(1,2));
Group([ (1,2,3,4), (1,2) ])
gap>
hom:=GroupHomomorphismByImages(g,g,[(1,2,3,4),(1,2)],[(1,4,3,2),(1,2)]);
[ (1,2,3,4), (1,2) ] -> [ (1,4,3,2), (1,2) ]
gap>
hom:=GroupHomomorphismByImages(g,g,[(1,2,3,4),(1,2)],[(1,4,3,2),(1,3)]);
fail
```

Como muestra el ejemplo, tales homomorfismos se determinan simplemente por la lista de generadores y sus imágenes.

Mediante imágenes con una función

En el caso que no se encuentre una acción adecuada o no sea posible dar una descomposición en generadores, puede auxiliarse de `GroupHomomorphismByFunction(`*G*`,`*H*`,`*fct*`)`, donde *fct* es una función GAP que se utiliza para evaluar imágenes.

Operaciones con homomorfismos de grupo

Los homomorfismos de grupo son funciones *phi* : *G* $\rightarrow$ *H* de elementos *g* $\in$ *G* en *h* $\in$ *H*:

`Image(`*phi*`,`*g*`)` determina la imagen de *g* según *phi*. Esto también se puede escribir como *g*`^`*phi*, que nos permite tener un grupo de homomorfismos que actúan en otro grupo. `Image(`*phi*`)` determina la imagen de *G* según *phi*, es decir, el grupo que consiste en el conjunto de todas las imágenes de elementos de *G*.

`Source(`*phi*`)`: es el grupo donde *phi* está definida.

`Range(`*phi*`)`: devuelve el grupo de imágenes de definición del mapeo *phi*.

`Image(`*phi*`,`*g*`)`: determina la imagen del subgrupo *S* $\leq$ *G*.

`PreImagesRepresentative(`*phi*`,`*h*`)`: determina un elemento $x \in$ *G*, tal que *phi*$(x) =$ *(*h).

`PreImage(`*phi*`,`*T*`)`: determina para un subgrupo *T* $\leq$ *H* el subgrupo de *G* de todos los elementos que se asignan en *T*.

`IsInjective(`*phi*`)` (Sinónimo de `IsOneToOne(`*phi*`)`): Comprueba si *phi* es inyectiva o uno-a-uno.

`IsSurjective(`*phi*`)` (Sinónimo de `IsOnto(`*phi*`)`): Comprueba si *phi* es sobreyectiva.

`Kernel(`*phi*`)`: devuelve el kernel de *phi* como un subgrupo de *G*.

```
gap> g:=Group((1,2,3,4),(1,2));
Group([ (1,2,3,4), (1,2) ])
gap> conjuntos:=Combinations([1..4],2);
[ [ 1, 2 ], [ 1, 3 ], [ 1, 4 ], [ 2, 3 ], [ 2, 4 ], [ 3, 4 ] ]
```

```
gap> hom:=ActionHomomorphism(g,conjuntos,OnSets);
<action homomorphism>
gap> Image(hom,(1,2)); # Nota: [1,3] -- posición 2 es mapeado a
                       #       [2,3] -- posición 4
(2,4)(3,5)
gap> Image(hom);
Group([ (1,4,6,3)(2,5), (2,4)(3,5) ])
gap> Image(hom,DerivedSubgroup(g));
Group([ (1,3,2)(4,5,6), (1,6)(2,5), (1,6)(3,4) ])
gap> PreImagesRepresentative(hom,(2,4)(3,5));
(1,2)
gap> PreImage(hom,Group([(2,4)(3,5)]));
Group([ (1,2) ])
gap> IsInjective(hom);
true
gap> Range(hom);
Sym( [ 1 .. 6 ] )
gap> IsSurjective(hom);
false
```

4.9. Factorización

Una de las cosas que pasan a ser mucho más fácil con la disponibilidad de un equipo adecuado y GAP, es la factorización de los elementos del grupo como palabras de generadores. Esto tiene aplicaciones evidentes hacia la solución de los rompecabezas, siendo probablemente la solución al cubo de Rubik la más prominente.

La funcionalidad básica está dado por el comando `Factorization(G,elm)` que devuelve una factorización del elemento `elm` como un producto de los generadores de `G`. (Así, en particular, es posible utilizar `Length` para determinar la longitud de dicha palabra.)

```
gap> g:=Group((1,2,3,4),(1,2));
Group([ (1,2,3,4), (1,2) ])
gap> Factorization(g,(1,3):names:=["T","L","M"]);
x1*x2*x1^2*x2
gap> g:=Group((1,2,3,4,5),(1,2));
Group([ (1,2,3,4,5), (1,2) ])
gap> Factorization(g,(1,2,3));
x1^-1*x2*x1*x2
gap> Length(last);
4
gap> Source(EpimorphismFromFreeGroup(g));
<free group on the generators [ x1, x2 ]>
```

Se ha visto que es posible asignar nombres personalizados a los elementos del grupo a través de

la opción `names`, que se asignan con dos puntos la lista de nombres como argumento en la primera llamada a `Factorization` o `EpimorphismFromFreeGroup`. Una vez que se asignan los nombres no se pueden cambiar nuevamente.

```
gap> g:=Group((1,2,3,4,5),(1,2));
Group([ (1,2,3,4,5), (1,2) ])
gap> Factorization(g,(1,2,3):nombres:=["cinco","dos"]);
cinco^-1*dos*cinco*dos
gap> EpimorphismFromFreeGroup(g);
[ cinco, dos ] -> [ (1,2,3,4,5), (1,2) ]
```

`Factorization` devuelve una palabra de generadores con la longitud más corta. Para asegurar esta minimalidad, esencialmente se tiene que enumerar todos los elementos del grupo. Por tanto, la funcionalidad es limitada en la práctica a los órdenes de los grupos hasta aproximadamente 10^7.

Para grupos más grandes un enfoque diferente es necesario: se tratan de forma heurística para mantener longitud de palabra lo más corta posible, pero no se logra garantizar la minimalidad para éstos grupos. Se puede utilizar la funcionalidad: `PreImagesRepresentative(`*`hom,elm`*`)` para obtener el homomorfismo *`hom`* que asigna a *`elm`*, que es exactamente lo que queremos.

```
gap> g:=SymmetricGroup(16);
Sym( [ 1 .. 16 ] )
gap> Size(g);
20922789888000
gap> hom:=EpimorphismFromFreeGroup(g:names:=["a","b"]);
[ a, b ] -> [ (1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16), (1,2) ]
b^-1*a^-1*b^-1*a^-1*b^-1*a*b^-1*a^-2*b^-1*a^-1*b^-1*a^-1*b^-1*a^
-1*b*a*b*a*b*a*b*a*b*a*b*a^-1*b*a^2*b*a*b^-1*a^-1
```

4.10. Clases laterales

Consistente con las acciones derechas, GAP implementa sólo clases laterales derechas. Las Clases laterales se crean con `RightCoset(`*`S,elm`*`)`, o alternativamente, como producto *`S*elm`*.

```
gap> s:=SylowSubgroup(SymmetricGroup(4),2);
Group([ (1,2), (3,4), (1,3)(2,4) ])
gap> c:=RightCoset(s,(1,2));
RightCoset(Group( [ (1,2), (3,4), (1,3)(2,4) ] ),(1,2))
gap> Size(c);
8
gap> Elements(c);
[ (), (3,4), (1,2), (1,2)(3,4), (1,3)(2,4), (1,3,2,4), (1,4,2,3), (1,4)(2,3) ]
gap> d:=s*(3,4);
RightCoset(Group( [ (1,2), (3,4), (1,3)(2,4) ] ),(3,4))
gap> s=d;
```

```
true
gap> d:=s*(1,4);
RightCoset(Group( [ (1,2), (3,4), (1,3)(2,4) ] ),(1,4))
gap> Intersection(s,d);
[  ]
gap> Union(s,d);
[ (), (3,4), (2,3), (2,3,4), (1,2), (1,2)(3,4), (1,2,4,3), (1,2,4), (1,3,2),
  (1,3,4,2), (1,3)(2,4), (1,3,2,4), (1,4,3), (1,4), (1,4,2,3), (1,4)(2,3) ]
```

`RightCosets(G,S)`: devuelve una lista de todas las clases laterales, es posible actuar sobre ellas por la multiplicación derecha.

```
gap> rc:=RightCosets(SymmetricGroup(4),s);
[ RightCoset(Group( [ (1,2), (3,4), (1,3)(2,4) ] ),()),
  RightCoset(Group( [ (1,2), (3,4), (1,3)(2,4) ] ),(2,3)),
  RightCoset(Group( [ (1,2), (3,4), (1,3)(2,4) ] ),(2,4,3)) ]
gap> hom:=ActionHomomorphism(SymmetricGroup(4),rc,OnRight);
<action homomorphism>
gap> Image(hom);
Group([ (1,3), (2,3) ])
```

`CosetDecomposition(G,S)`: devuelve una partición de G en clases laterales derechas de S. La primera componente consta de los elementos de S, las restantes se devuelven de forma ordenada como producto $s \cdot rep$ para $s \in S$.

```
gap> CosetDecomposition(SymmetricGroup(4),s);
[ [ (),(3,4),(1,2),(1,2)(3,4),(1,3)(2,4),(1,3,2,4),(1,4,2,3),(1,4)(2,3) ],
  [ (2,3),(2,3,4),(1,3,2),(1,3,4,2),(1,2,4,3),(1,2,4),(1,4,3),(1,4) ],
  [ (2,4,3),(2,4),(1,4,3,2),(1,4,2),(1,2,3),(1,2,3,4),(1,3),(1,3,4) ] ]
```

`RightTransversal(G,S)` devuelve una lista de representantes de todas las clases laterales.

```
gap> rt:=RightTransversal(SymmetricGroup(4),s);
RightTransversal(Sym( [ 1 .. 4 ] ),Group([ (1,2), (3,4), (1,3)(2,4) ]))
gap> Elements(rt);
[ (), (2,3), (2,4,3) ]
gap> hom:=ActionHomomorphism(SymmetricGroup(4),rt,OnRight);
<action homomorphism>
gap> Image(hom);
Group([ (1,3), (2,3) ])
```

4.11. Grupos cociente

La forma "estándar" en GAP para la creación de grupos cocientes es el uso de `NaturalHomomorphismByNormalSubgroup(G,N)` que crea un homomorfismo $G \to G/N$. Alternati-

vamente, se puede utilizar `FactorGroup(G,N)` para crear el grupo cociente con el homomorfismo almacenado en el parámetro `NaturalHomomorphism` del grupo cociente.

```
gap> g:=SymmetricGroup(4);
Sym( [ 1 .. 4 ] )
gap> n:=Subgroup(g,[(1,2)(3,4),(1,3)(2,4)]);
Group([ (1,2)(3,4), (1,3)(2,4) ])
gap> nat:=NaturalHomomorphismByNormalSubgroup(g,n);
[ (1,2,3,4), (1,2) ] -> [ f1*f2, f1 ]
gap> f:=FactorGroup(g,n);
Group([ f1, f2 ])
gap> NaturalHomomorphism(f);
[ (1,2,3,4), (1,2) ] -> [ f1*f2, f1 ]
```

Se advierte que GAP trabaja duro en un intento de encontrar una manera eficiente (en sentido computacional) para representar a G/N que a menudo no tiene relación obvia con la representación de G ó N, pues simplemente se trata de un grupo que es isomorfo a G/N.

Por suerte, GAP ofrece una función `FactorGroupAsCosets` que crea un grupo que consiste en las clases laterales del grupo cociente, tal como se define. Esta funcionalidad está disponible para este grupo, tal y como se expone en el siguiente ejemplo.

```
gap> f:=FactorGroupAsCosets(g,n);
<group of size 6 with 2 generators>
gap> Elements(f);
[ RightCoset(Group( [ (1,2)(3,4), (1,3)(2,4) ] ),()),
  RightCoset(Group( [ (1,2)(3,4), (1,3)(2,4) ] ),(1,2)),
  RightCoset(Group( [ (1,2)(3,4), (1,3)(2,4) ] ),(1,2,4,3)),
  RightCoset(Group( [ (1,2)(3,4), (1,3)(2,4) ] ),(2,3,4)),
  RightCoset(Group( [ (1,2)(3,4), (1,3)(2,4) ] ),(1,3,4)),
  RightCoset(Group( [ (1,2)(3,4), (1,3)(2,4) ] ),(1,2,3,4)) ]
gap> hom:=NaturalHomomorphism(f);
MappingByFunction( Sym( [ 1 .. 4 ] ), <group of size 6 with
2 generators>, function( x ) ... end )
```

4.12. Buscando simetrías

Esta sección se trata la creación de grupos simétricos. Encontrar las simetrías de un objeto dado en general, no es tarea fácil, debido a la dificultad potencial de representar las simetrías. Si el objeto es geométrico sobre en un espacio lineal, se puede representar por medio de matrices. Para esto, es necesario definir una base y determinar la imágenes de los vectores de la base bajo simetrías.

Un método genérico, que en principio funciona para cualquier objeto "finito", es etiquetar las partes del objeto con números (por ejemplo caras o las esquinas de un cubo, los vértices y los bordes de un grafo). A veces se puede simplemente escribir permutaciones para algunas simetrías

y comprobar el orden del grupo generado por ellas, para asegurar de no cometer errores –el orden puede indicar que no se obtuvieron todas simetrías–. Por ejemplo, si tomamos un cubo, se etiquetan sus caras de forma estándar a como se etiquetan los dados, se pueden etiquetar las caras con los números del 1 al 6. La rotación alrededor de la cara 1 es $(2,3,5,4)$, la rotación alrededor de la cara 2 es $(1,3,6,4)$. El grupo generado por estos dos elementos tiene orden 24 y por lo tanto es el grupo de todas las rotaciones.

```
gap> H:=Group((2,3,5,4),(1,3,6,4));;
gap> Size(H);
24
```

También se puede representar relaciones entre objetos (que deben ser regidas por las simetrías) como conjuntos, por lo general de cardinalidad 2.

En el ejemplo de un dado, se podría tomar la relación "vecino" que daría subconjuntos (para evitar distinguir $\{1,2\}$ y $\{2,1\}$).

$$\{1,2\},\{1,3\},\{1,4\},\{1,5\},\{2,3\},\{2,4\},\{2,6\},\{3,5\},\{3,6\},\{4,5\},\{4,6\},\{5,6\}$$

Alternativamente, y más corto, se puede indicar la relación "no vecino":

$$\{1,6\},\{2,5\},\{3,4\}.$$

Consideremos ahora el grupo simétrico $G = S_n$. (Si los números representan dos clases distintas de objetos, puede considerarse el producto directo $S_a \times S_b$ con $1,\ldots,a$ que representa la primera clase de objetos y $1,\ldots,b$ la otra clase.)

Sea $\varphi\colon G \to S_{\binom{n}{2}}$ el homomorfismo que refleja la acción de G en **todos** los 2-conjuntos. A continuación, la relación se convierte en un subconjunto A de $\left\{1,\ldots,\binom{n}{2}\right\}$. Sea T ser el estabilizador de este conjunto en G^φ, la preimagen T bajo φ es un subgrupo de G que contiene todas las simetrías, y –si las relaciones fueron lo suficientemente restrictivas– será en realidad el grupo de todas las simetrías.

En el ejemplo del dado, tomaríamos todos los 2-subconjuntos de $\{1,\ldots,6\}$ y actuar sobre ellos con S_6:

```
gap> conjuntos:=Combinations([1..6],2);
[ [ 1, 2 ], [ 1, 3 ], [ 1, 4 ], [ 1, 5 ], [ 1, 6 ], [ 2, 3 ], [ 2, 4 ],
  [ 2, 5 ], [ 2, 6 ], [ 3, 4 ], [ 3, 5 ], [ 3, 6 ], [ 4, 5 ], [ 4, 6 ],
  [ 5, 6 ] ]
gap> G:=SymmetricGroup(6);
Sym( [ 1 .. 6 ] )
gap> phi:=ActionHomomorphism(G,conjuntos,OnSets);
<action homomorphism>
gap> img:=Image(phi,G);
Group([ (1,6,10,13,15,5)(2,7,11,14,4,9)(3,8,12), (2,6)(3,7)(4,8)(5,9) ])
```

Los conjuntos dados por la relación "no vecino" están en posiciones 5, 8, y 10, estas posiciones corresponden a la acción de permutación dada por *phi*, así que podemos calcular T como el conjunto estabilizador. (GAP utiliza un algoritmo especial para calcular estabilizadores de grupos de permutaciones.)

```
gap> Position(conjuntos,[1,6]);
5
gap> Position(conjuntos,[2,5]);
8
gap> Position(conjuntos,[3,4]);
10
gap> T:=Stabilizer(img,[5,8,10],OnSets);
Group([ (1,9)(2,12)(3,14)(4,15), (1,15)(2,14)(3,12)(4,9)(6,13)(7,11),
  (1,15)(2,12)(3,14)(4,9)(6,11)(7,13), (1,14)(2,15)(3,9)(4,12)(6,13)(8,10),
  (1,13,2,15,6,14)(3,4,11,12,9,7)(5,8,10) ])
gap> H:=PreImage(phi,T);
Group([ (1,6), (1,6)(2,5)(3,4), (1,6)(2,5), (1,6)(2,4)(3,5), (1,5,3,6,2,4) ])
```

El estabilizador resultante $H \leq G$ resulta ser el grupo de todas las simetrías rotacionales y reflectivas que actúa sobre las caras de un dado.

4.13. Aplicaciones

Permutaciones

Una *permutación* de grado n es una función de $\{1, \ldots, n\}$ en sí mismo, que es biyectiva. Podemos describir permutaciones especificando la imagen de cada punto, por ejemplo, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 6 & 4 & 1 & 2 \end{pmatrix}$. En la práctica, sin embargo, vamos a escribir las permutaciones en notación ciclo, es decir, $(1,5)(2,3,6)$ para la permutación anterior. En la notación de ciclo cada punto aparece como máximo una vez. La imagen de un punto a es:

- b si la ocurrencia de a se encuentra en un ciclo $(\ldots, a, b, \ldots)$
- c si la ocurrencia de a se encuentra en un ciclo $(c, \ldots, a)$ (es decir a está en el extremo de un de ciclo)
- a si a no aparece, esto es, se omite escribir el ciclo (a).

Para escribir una permutación $p = \begin{pmatrix} 1 & 2 & \ldots & n \\ p_1 & p_2 & \ldots & p_n \end{pmatrix}$ (es decir p mapea i en p_i) en forma de ciclo se recomienda utilizar el siguiente procedimiento:

Mientras hay puntos que no son procesados

Sea a un punto que no ha procesado.

Escribir "(a"

Sea $i := p_a$ (es decir, la imagen de a bajo p).

Mientras $i \neq a$

Escribir "$, i$"

Sea $i = p_i$

terminar Mientras

Escribir ")"

Si el ciclo que acaba de finalizar tiene longitud 1, elimínelo.

terminar Mientras

Por ejemplo, para la permutación inicial, empezamos por escoger $a = 1$, obteniendo $i = p_1 = 5$. Escribimos "(1," como $1 \neq 5$ seguimos "$(1, 5$" y obtenemos $i = p_5 = 1$. Esto cierra el ciclo y cerramos el ciclo "$(1, 5)$". A continuación escogemos $a = 2$, escribiendo "$(1, 5)(2$", entonces $i = p_2 = 3$ y escribimos "$(1, 5)(2, 3$", seguimos $i = p_3 = 6$ y escribimos "$(1, 5)(2, 3, 6$", como $i = p_6 = 2$ cerramos el ciclo "$(1, 5)(2, 3, 6)$". Finalmente recogemos $a = 4$, tenemos que $i = p_4 = 4$ el ciclo se cierra inmediatamente: "$(1, 5)(2, 3, 6)(4)$", que tiene longitud uno, por lo que lo eliminamos, obteniendo el resultado "$(1, 5)(2, 3, 6)$".

Es recomendable escoger a lo más pequeño posible como primer paso, lo que resulta en ciclos que comienzan con los elementos más pequeños, aunque es posible escribir cada ciclo de manera diferente, por ejemplo, $(1, 5)(2, 3, 6) = (5, 1)(3, 6, 2)$.

Observación importante: los diferentes ciclos de una permutación nunca compartiran números.

Aritmética de la notación de ciclo: La imagen de un punto bajo una permutación es su *sucesor* en el ciclo, la imagen bajo la permutación inversa es el *predecesor*. Así, podemos invertir una permutación simplemente revirtiendo todos sus ciclos (posiblemente girando cada ciclo y después de mover el número más pequeño al comienzo del ciclo): $(1, 5)(2, 3, 6)^{-1} = (5, 1)(6, 3, 2) = (1, 5)(2, 6, 3)$, $(1, 2, 3, 4, 5)^{-1} = (5, 4, 3, 2, 1) = (1, 5, 4, 3, 2)$.

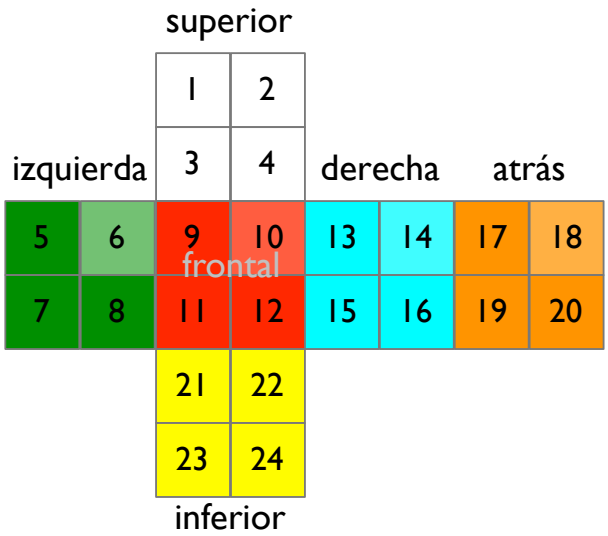
Para multiplicar permutaciones, debe rastrearse a través de cada ciclo las imágenes de cada puntos, y construir una nueva permutación con las imágenes. Por ejemplo, supongamos que queremos multiplicar $(1, 5)(2, 3, 6) \cdot (1, 6, 4)(3, 5)$. La imagen de 1 es 5 bajo la primera, y la imagen de 5 es 3 bajo la segunda permutación. El resultado se iniciará "$(1, 3 \ldots$", 3 asigna a 6 y 6 a 4, así "$(1, 3, 4 \ldots$", 4 queda fijo por la primera permutación y bajo la segunda permutación se asigna a 1. Así que el primer ciclo del resultado es "$(1, 3, 4)$". Tomamos el siguiente número, 2 se asigna a 3 y 3 a 5, por lo que tenemos "$(1, 3, 4)(2, 5 \ldots$", 5 se asigna a 1 y 1 a 6 y (ya que no hay puntos a la izquierda) hemos terminado: $(1, 5)(2, 3, 6) \cdot (1, 6, 4)(3, 5) = (1, 3, 4)(2, 5, 6)$.

Permutaciones en GAP**:** En GAP pueden escribirse las permutaciones en forma de ciclo y multiplicarlas (o invertirlas). El orden de la multiplicación es el mismo que se utiliza normalmente:

```
gap> (1,2,3)*(2,3);
(1,3)
gap> (2,3)*(1,2,3);
(1,2)
gap> a:=(1,2,3,4)(6,5,7);
(1,2,3,4)(5,7,6)
gap> a^2;
(1,3)(2,4)(5,6,7)
gap> a^-1;
(1,4,3,2)(5,6,7)
gap> b:=(1,3,5,7)(2,6,8);
(1,3,5,7)(2,6,8)
gap> a*b;
(1,6,7,8,2,5)(3,4)
gap> a*b*a^-1;
(1,7,8)(2,6,5,4)
```

Puzzles (Rompecabezas). Muchos rompecabezas se pueden describir de esta manera: Cada estado del rompecabezas corresponde a una permutación, la tarea de resolver el puzzle a continuación, corresponde a expresar la permutación como producto de generadores.

Resolviendo en GAP **el Cubo** $2 \times 2 \times 2$ **de Rubik.** A modo de ejemplo resolveremos el cubo de Rubik de dimensiones $2 \times 2 \times 2$. Se etiquetan las caras del cubo de la siguiente manera:



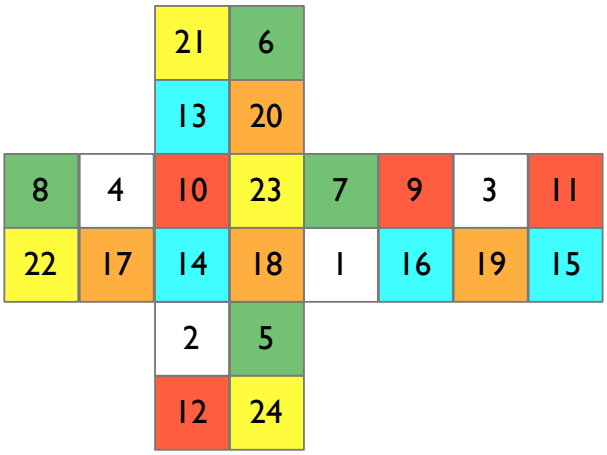
Para realizar las rotaciones a cada cara fijaremos cualquiera de las esquinas, digamos que fijamos la esquina inferior derecha (es decir, la esquina marcada con 16/19/24) en el espacio –esto es para orientar las rotaciones de todo el cubo en el espacio–. Por lo tanto, necesitamos considerar sólo tres rotaciones, frontal, superior e izquierda. Las permutaciones correspondientes son (rotaciones en el sentido de las agujas del reloj cuando se observa de frente a cada cara):

```
gap> superior:=(1,2,4,3)(5,17,13,9)(6,18,14,10);;
gap> izquierda:=(1,9,21,20)(5,6,8,7)(3,11,23,18);;
gap> frontal:=(3,13,22,8)(4,15,21,6)(9,10,12,11);;
gap> cubo:=Group(superior,izquierda,frontal);
Group([(1,2,4,3)(5,17,13,9)(6,18,14,10),(1,9,21,20)(3,11,23,18)(5,6,8,7),
  (3,13,22,8)(4,15,21,6)(9,10,12,11) ])
gap> Order(cubo);
3674160
```

Mediante la definición de una asignación adecuada, (que por el momento se considerará esta asignación como una caja negra) primero podemos elegir nombres adecuados –S, I y F– para los generadores:

```
gap> map:=EpimorphismFromFreeGroup(cubo:names:=["S","I","F"]);
[ S, I, F ] -> [ (1,2,4,3)(5,17,13,9)(6,18,14,10),
  (1,9,21,20)(3,11,23,18)(5,6,8,7), (3,13,22,8)(4,15,21,6)(9,10,12,11) ]
```

Ahora podemos usar el comando `Factorization` para expresar permutaciones del grupo en su palabra de generadores. El proceso aplicar la secuencia de operaciones inversas en *reversa* girará el cubo de nuevo a su forma original. Por ejemplo, supongamos que el cubo tiene el siguiente aspecto:



Esto corresponde a la permutación

```
gap> movimiento:=(1,15,20,4,6,2,21)(3,17,8,5,22,7,13)(9,14,11,18,12,23,10)
```

(1 ha ido en la posición en la que 15 era, 2 ha pasado en la posición de 21, etcétera). Expresamos esta permutación como palabra de generadores:

```
gap> Factorization(cubo, movimiento);
S*F*I*S*F*S
```

Podemos llevar el cubo a su posición original girando en sentido antihorario las capas superior, frontal, superior, izquierda, frontal, superior.

Rompecabezas más grandes. Si queremos hacer algo similar para rompecabezas más grandes, por ejemplo, el cubo de Rubik de dimensiones $3 \times 3 \times 3$, el algoritmo utilizado por `Factorization` se queda sin memoria. En su lugar, tendría que usar un algoritmo diferente, que puede ser seleccionado mediante el mapeo que hemos utilizado para definir el nombre. El algoritmo utilizado entonces no garantiza (por motivos de tiempo) que la palabra sea la más corta en longitud, en nuestro ejemplo:

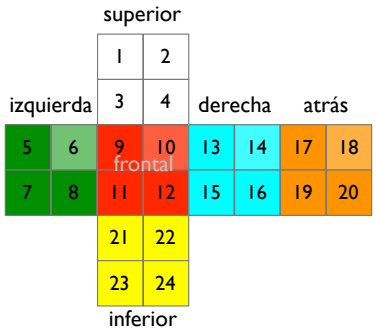
```
gap> PreImagesRepresentative(map,movimiento);
S*I^-2*S^-1*I*S*I^-2*S^-2*F*S*F^-1*I^-1*F*S^-1*F^-1*I*S*I*
S^-2*F*S*F^-1*S*F*S^-1*F^-2*I^-1*F^2*I
```

Resolviendo el cubo de Rubik manualmente

En esta nota, nos interesamos en determinar una estrategia para resolver el cubo de Rubik de $2 \times 2 \times 2$ manualmente (de nuevo, enfoques similares funcionan para otros rompecabezas, este es justamente un buen ejemplo para desarrollarse de forma rápida, clara y precisa, además que deja entre ver la aplicación de los conceptos matemáticos).

Recuerde que etiquetamos las caras del cubo como se muestra en la figura y fijamos la pieza (16/19/24) en el espacio. El grupo de simetrías es el siguiente:

La idea básica es ahora colocar las piezas en la posición correcta (en las "caras" del cubo) y a continuación, seguir con los movimientos que dejan fijas las piezas ya colocadas correctamente. Mover las primeras piezas suele ser fácil; lo complicado es encontrar los elementos adecuados en el estabilizador que permitan colocar las otras piezas en los lugares correctos dejando fijas las que ya se encuentran en sus posiciones correctas.



$$G = \langle \quad \text{superior} = (1,2,4,3)(5,17,13,9)(6,18,14,10),$$
$$\text{izquierda} = (1,9,21,20)(5,6,8,7)(3,11,23,18),$$
$$\text{frontal} = (3,13,22,8)(4,15,21,6)(9,10,12,11) \quad \rangle$$

Vamos a elegir las posiciones que cubriremos de forma que garanticemos que algunos de los generadores originales fijen las posiciones elegidas. Esto hará que de forma automática algunos generadores del estabilizador están representados por palabras cortas. En concreto, vamos a llenar las posiciones de partida en el orden (23, 22, 21) y luego trabajar en la capa superior.

Empezamos por calcular la órbita de 23. Esto se hace de una manera similar a como se enumeran los elementos de un grupo: calculamos la imagen de todos los puntos procesados bajo todos los generadores, hasta que no surgan nuevas imágenes. También mantenemos un registro de los elementos del grupo que hacen corresponder a 23 las posibles imágenes.

Es posible hacer estos cálculos ligeramente tediosos de forma más cómoda con GAP. La siguiente secuencia de comandos calcula la órbita y realiza un seguimiento de las palabras que producen la misma imagen. (Trabajamos con palabras de generadores, ya que son más fáciles de leer que las imágenes.)

```
map:=EpimorphismFromFreeGroup(cubo:names:=["S","I","F"]);
gen:=GeneratorsOfGroup(cubo);
letras:=GeneratorsOfGroup(Source(map)); # letras correspondientes
orb:=[23]; # la órbita que se está construyendo
palabras:=[One(letras[1])]; # palabras que producen las imágenes correctas
for x in orb do
  for i in [1..Length(gen)] do
    img:=x^gen[i];
    if not img in orb then
      Add(orb,img);
      p:=Position(orb,x);
      Add(palabras,palabras[p]*letras[i]);
    fi;
  od;
od;
```

Como resultado se obtiene la siguiente órbita y representantes:

Órbita	23	18	14	3	10	1	11	13	6	12	2
Rep	e	I	IS	I^2	IS^2	I^2S	I^3	I^2F	IS^3	IS^2F	I^2S^2

Órbita	9	22	8	4	5	21	7	15	17	20
Rep	I^2SI	I^2F^2	IS^3I	IS^3F	I^2SIS	I^2SI^2	IS^3I^2	IS^3F^2	I^2SIS^2	I^2SI^3

La idea fundamental de los elementos del estabilizador (aparte de los obvios, como la rotación de la parte superior) ahora es la siguiente: Supongamos que la imagen de la órbita del elemento x bajo un generador g da un elemento y *anterior* de la órbita. Entonces $\mathrm{Rep}_x \cdot g \cdot \mathrm{Rep}_y^{-1}$ mueve el elemento inicial (en este caso 23) a sí mismo y por lo tanto se encuentra en el estabilizador. (Puede demostrarse[1] que todos estos elementos generan el estabilizador).

En nuestro ejemplo, encontramos que $23^S = 23$, esto es que $e \cdot S \cdot e^{-1} = S$ está en el estabilizador. Similarmente $11^F = 9$, esto es que $I^3 \cdot F \cdot (I^2SI)$ también está en el estabilizador, y así sucesivamente.

Mediante cálculos sobre el orden del grupo, encontramos que sólo tenemos unos pocos elementos como generadores, es decir,

$$C_1 := Est_G(23) = \left\langle S, F, I^{-1}SI \right\rangle$$

(Vale la pena notar que el proceso de la construcción tiende a producir elementos de la forma ABA^{-1}. Si usted consulta cualquier estrategia de solución notará que este hecho es común.)

[1] Este resultado es llamado LEMA DE SCHREIER, para ampliar este resultado puede consultarse HOLT: Handbook of Computational Group Theory.

Por lo que se refiere a la solución del cubo, es muy fácil de conseguir algunas posiciones iniciales corectas. Por tanto, no aspiramos a una estrategia sistemática todavía, pero mantenemos los generadores estabilizador para el siguiente nivel.

En la siguiente posición con que trabajaremos es 22, el proceso es similar (de nuevo, no es un cálculo fácil el involucrado en demostrar que estos tres elementos son suficientes para generar el estabilizador, si se toma sólo unos pocos elementos aleatorios no hay ninguna garantía a priori que lo harían), obtenemos:

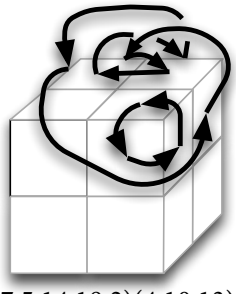
$$C_2 := Est_G(22, 23) = \left\langle S, I^{-1}SI, FSF^{-1} \right\rangle$$

A continuación (completando la capa inferior), vamos a trabajar con 21. Aquí es donde el estabilizador se vuelve interesante, en la medida de como continuar en lo que se refiere para resolver el cubo. Una aplicación repetida consigue

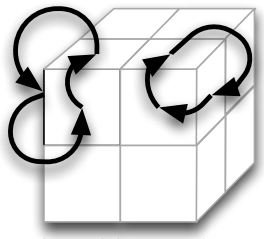
$$C_3 := Est_G(21, 22, 23) = \left\langle S, IS^{-1}I^{-1}S^{-1}F^{-1}IF \right\rangle$$

El segundo generador es escogido entre muchas otras posibilidades como ser de más corta longitud posible. Su acción sobre el cubo es la permutación $(1, 17, 5, 14, 18, 2)(4, 10, 13)$, es decir, dos piezas están intercambiados y una pieza está arriba. Si sólo tenemos en cuenta las posiciones (sin rotaciones) de los cuatro pedazos, no es difícil ver que, junto con la rotación de la parte superior esta nos permitirá poner cada pieza en su posición mediante rotaciones. (Es decir, estamos estabilizando los *conjuntos* $\{1, 5, 18\}$, $\{2, 14, 17\}$, $\{3, 6, 9\}$ y $\{4, 10, 13\}$) formalmente estamos considerando aquí una acción de grupo diferente, es decir, sobre las esquinas superiores del cubo.

Lo que queda ahora es orientar las 4 piezas adecuadamente. Mirando a través de los generadores del estabilizador encontramos el elemento $I^{-1}FI^{-1}FS^{-1}I^{-1}S^2F^2IS$ con la permutación $(3, 6, 9)(4, 13, 10)$. Giramos las dos esquinas delanteras superiores del cubo en direcciones opuestas. Es evidente movimientos similares sirven para mover las otras dos esquinas superiores del cubo. Mediante la aplicación de estos movimientos para el frente, izquierda y atrás, podemos determinar la ubicación de cualesquiera de las tres esquinas superiores.


(1,17,5,14,18,2)(4,10,13)

Afirmamos que esto resolverá el cubo completo. Sabemos que $[G : C_1] = \texttt{Ord}(\text{orb}_G(23)) = 24 - 3 = 21$ (en todo el cubo, la pieza en la posición 23 puede moverse a todas las posiciones, teniendo los tres fijos). Similarmente, cuando estabilizamos la posición 23, podemos (esto se puede comprobar fácilmente al probar los movimientos permitidos en C_1) mover la pieza en la posición 22 a todos los demás lugares, pero hay tres lugares fijos (16/19/24) y los tres que tienen adyacente una cara con 23 (7/20/23), entonces $[C_1 : C_2] = 18$. Un argumento similar comprueba que $[C_2 : C_3] = 15$.


(3,6,9)(4,13,10)

Bajo el estabilizador C_3 hemos visto que podemos colocar correctamente las cuatro caras en todas las permutaciones posibles, por lo tanto el grupo estabilizador de las posiciones de las caras tiene índice 24 en C_3. Usando que $\texttt{Ord}(G) = 3674160$, así conseguimos el grupo que sólo gira (pero

no permuta) las caras superiores, y deja fija a la capa inferior, tiene orden:

$$\frac{3674160}{21 \cdot 18 \cdot 15 \cdot 24} = 27 = 3^3.$$

Pero esto significa que girando sólo tres caras correctamente también debe colocarse la cuarta cara en la posición correcta.

Apéndice A

Lista de grupos de orden menor o igual a 100

Son muy pocos los grupos que los matemáticos y físicos estudiaron, razón por la que pocos de estos grupos carecen de nombres específicos. Algunos de los grupos estudiamos son los grupos cíclicos C_n, los grupos simétricos S_n, y los grupos alternantes A_n y los grupos diédricos D_n. La gran mayoría se describe por su estructura y una "prescripción" de cómo armar estas piezas para formar otro grupo. En el apéndice B esbozamos los conceptos que son cruciales para la descripción de los grupos: el producto directo, el producto semidirecto y sucesiones exactas.

Notación y convenios

Denotamos el producto directo con "$\times$" y el semidirecto por $N \rtimes_\varphi K$ donde N es un grupo normal. Es de considerar que esta convención no es única y que el símbolo "$\rtimes_\varphi$" puede apuntar hacia otro lado. Al escribir sucesiones exactas como $\mathbf{1} \to N \to G \to Q \to \mathbf{1}$, vamos a omitir los grupos triviales al inicio y fin con la finalidad de hacer que nuestra notación más ligera.

Denotamos el grupo diédrico de un n-ágono regular por D_n, y *no* por D_{2n}, como prerfieren algunos autores. Por C_n o $\mathbb{Z}_n$ denotaremos al grupo cíclico de orden n. Y por S_n y A_n al grupo simétrico y alternante, respectivamente. Q_4 y Q_8 son los grupo de los cuaterniones y octoniones, respectivamente. $\mathrm{SL}(n,p)$ es el grupo especial lineal sobre un campo finito, esto es, el conjunto de todas las matrices de orden $n \times n$ con determinante uno y valores en las entradas de un campo de orden p.

Algunos grupos que consideraremos no tienen nombres específicos, y nos referimos a ellos por medio de `GAPID`, $\mathfrak{G}(m,n)$ denotará el grupo que es generado en `GAP` por el comando `SmallGroup(`m`,`n`)`.

Generando grupos

El siguiente algoritmo genera la lista de todos los grupos de orden ≤ 100 usando la librería SmallGroups de `GAP`:

```
groups := AllSmallGroups([1..100]);;
for g in groups do
  Display(IdGroup(g));
  Display(StructureDescription(g));
```

```
  for i in [1..Size(chartab)] do
    Print(chartab[i][1], " ");
    od;
    Print("\n");
  od;
time;
```

Este algoritmo puede ejecutarse en GAP digitando directamente las líneas de código en la ventana principal de GAP. En lo que sigue se supone que las líneas anteriores se han guardado en un archivo llamado grupos.gap que luego es cargado y ejecutado automáticamente como se muestra a continuación:

```
gap> Read("grupos.gap");
```

Esta sección se incluye con el objetivo de brindar al lector el resultado de la ejecución del algoritmo, ahorrando el trabajo en la ejecución del algoritmo y el tiempo de espera para la ejecución del mismo.

En la Tabla A.1, listamos los 1048 grupos esencialmente diferentes (salvo isomorfismo) de orden ≤ 100. La primer columna GAPID etiqueta a cada grupo de forma única dentro de GAP. El primer número entre corchetes es el orden del grupo, y el segundo número simplemente numera cada diferente grupo del mismo orden.

La segunda columna es el nombre del grupo. Si dos o más grupos tienen el mismo nombre, estos son isomorfos. Para interpretar los nombres de cada grupo se hace necesario recurrir a la teoría expuesta en el apéndice B.

Cuadro A.1: Tabla

GAPID	Grupo
[1, 1]	1
[2, 1]	C_2
[3, 1]	C_3
[4, 1]	C_4
[4, 2]	$C_2 \times C_2$
[5, 1]	C_5
[6, 1]	S_3
[6, 2]	C_6
[7, 1]	C_7
[8, 1]	C_8
[8, 2]	$C_4 \times C_2$
[8, 3]	D_4
[8, 4]	Q_8
[8, 5]	$C_2 \times C_2 \times C_2$
[9, 1]	C_9
[9, 2]	$C_3 \times C_3$
[10, 1]	D_5
[10, 2]	C_{10}

Continúa en la página siguiente...

GAPID	Grupo
[11, 1]	C_{11}
[12, 1]	$C_3 \times_\rho C_4$
[12, 2]	C_{12}
[12, 3]	A_4
[12, 4]	D_6
[12, 5]	$C_6 \times C_2$
[13, 1]	C_{13}
[14, 1]	D_7
[14, 2]	C_{14}
[15, 1]	C_{15}
[16, 1]	C_{16}
[16, 2]	$C_4 \times C_4$
[16, 3]	$(C_4 \times C_2) \times_\rho C_2$
[16, 4]	$C_4 \times_\rho C_4$
[16, 5]	$C_8 \times C_2$
[16, 6]	$C_8 \times_\rho C_2$
[16, 7]	D_8
[16, 8]	QD_8
[16, 9]	Q_{16}
[16, 10]	$C_4 \times C_2 \times C_2$
[16, 11]	$C_2 \times D_4$
[16, 12]	$C_2 \times Q_8$
[16, 13]	$(C_4 \times C_2) \times_\rho C_2$
[16, 14]	$C_2 \times C_2 \times C_2 \times C_2$
[17, 1]	C_{17}
[18, 1]	D_9
[18, 2]	C_{18}
[18, 3]	$C_3 \times S_3$
[18, 4]	$(C_3 \times C_3) \times_\rho C_2$
[18, 5]	$C_6 \times C_3$
[19, 1]	C_{19}
[20, 1]	$C_5 \times_\rho C_4$
[20, 2]	C_{20}
[20, 3]	$C_5 \times_\rho C_4$
[20, 4]	D_{10}
[20, 5]	$C_{10} \times C_2$
[21, 1]	$C_7 \times_\rho C_3$
[21, 2]	C_{21}
[22, 1]	D_{11}
[22, 2]	C_{22}
[23, 1]	C_{23}
[24, 1]	$C_3 \times_\rho C_8$
[24, 2]	C_{24}
[24, 3]	$SL(2, 3)$
[24, 4]	$C_3 \times_\rho Q_8$
[24, 5]	$C_4 \times S_3$
[24, 6]	D_{12}
[24, 7]	$C_2 \times (C_3 \times_\rho C_4)$
[24, 8]	$(C_6 \times C_2) \times_\rho C_2$
[24, 9]	$C_{12} \times C_2$
[24, 10]	$C_3 \times D_4$
[24, 11]	$C_3 \times Q_8$
[24, 12]	S_4
[24, 13]	$C_2 \times A_4$
[24, 14]	$C_2 \times C_2 \times S_3$

Continúa en la página siguiente...

GAPID	Grupo
[24, 15]	$C_6 \times C_2 \times C_2$
[25, 1]	C_{25}
[25, 2]	$C_5 \times C_5$
[26, 1]	D_{13}
[26, 2]	C_{26}
[27, 1]	C_{27}
[27, 2]	$C_9 \times C_3$
[27, 3]	$(C_3 \times C_3) \times_\rho C_3$
[27, 4]	$C_9 \times_\rho C_3$
[27, 5]	$C_3 \times C_3 \times C_3$
[28, 1]	$C_7 \times_\rho C_4$
[28, 2]	C_{28}
[28, 3]	D_{14}
[28, 4]	$C_{14} \times C_2$
[29, 1]	C_{29}
[30, 1]	$C_5 \times S_3$
[30, 2]	$C_3 \times D_5$
[30, 3]	D_{15}
[30, 4]	C_{30}
[31, 1]	C_{31}
[32, 1]	C_{32}
[32, 2]	$(C_4 \times C_2) \times_\rho C_4$
[32, 3]	$C_8 \times C_4$
[32, 4]	$C_8 \times_\rho C_4$
[32, 5]	$(C_8 \times C_2) \times_\rho C_2$
[32, 6]	$((C_4 \times C_2) \times_\rho C_2) \times_\rho C_2$
[32, 7]	$(C_8 \times_\rho C_2) \times_\rho C_2$
[32, 8]	$(C_2 \times C_2) \to G \to (C_4 \times C_2)$
[32, 9]	$(C_8 \times C_2) \times_\rho C_2$
[32, 10]	$Q_8 \times_\rho C_4$
[32, 11]	$(C_4 \times C_4) \times_\rho C_2$
[32, 12]	$C_4 \times_\rho C_8$
[32, 13]	$C_8 \times_\rho C_4$
[32, 14]	$C_8 \times_\rho C_4$
[32, 15]	$C_4 \to G \to (C_4 \times C_2)$
[32, 16]	$C_{16} \times C_2$
[32, 17]	$C_{16} \times_\rho C_2$
[32, 18]	D_{16}
[32, 19]	QD_{16}
[32, 20]	Q_{32}
[32, 21]	$C_4 \times C_4 \times C_2$
[32, 22]	$C_2 \times ((C_4 \times C_2) \times_\rho C_2)$
[32, 23]	$C_2 \times (C_4 \times_\rho C_4)$
[32, 24]	$(C_4 \times C_4) \times_\rho C_2$
[32, 25]	$C_4 \times D_4$
[32, 26]	$C_4 \times Q_8$
[32, 27]	$(C_2 \times C_2 \times C_2 \times C_2) \times_\rho C_2$
[32, 28]	$(C_4 \times C_2 \times C_2) \times_\rho C_2$
[32, 29]	$(C_2 \times Q_8) \times_\rho C_2$
[32, 30]	$(C_4 \times C_2 \times C_2) \times_\rho C_2$
[32, 31]	$(C_4 \times C_4) \times_\rho C_2$
[32, 32]	$(C_2 \times C_2) \to G \to (C_2 \times C_2 \times C_2)$
[32, 33]	$(C_4 \times C_4) \times_\rho C_2$
[32, 34]	$(C_4 \times C_4) \times_\rho C_2$
[32, 35]	$C_4 \times_\rho Q_8$

Continúa en la página siguiente...

GAPID	Grupo
[32, 36]	$C_8 \times C_2 \times C_2$
[32, 37]	$C_2 \times (C_8 \times_\rho C_2)$
[32, 38]	$(C_8 \times C_2) \times_\rho C_2$
[32, 39]	$C_2 \times D_8$
[32, 40]	$C_2 \times \mathrm{QD}_8$
[32, 41]	$C_2 \times Q_{16}$
[32, 42]	$(C_8 \times C_2) \times_\rho C_2$
[32, 43]	$(C_2 \times D_4) \times_\rho C_2$
[32, 44]	$(C_2 \times Q_8) \times_\rho C_2$
[32, 45]	$C_4 \times C_2 \times C_2 \times C_2$
[32, 46]	$C_2 \times C_2 \times D_4$
[32, 47]	$C_2 \times C_2 \times Q_8$
[32, 48]	$C_2 \times ((C_4 \times C_2) \times_\rho C_2)$
[32, 49]	$(C_2 \times D_4) \times_\rho C_2$
[32, 50]	$(C_2 \times Q_8) \times_\rho C_2$
[32, 51]	$C_2 \times C_2 \times C_2 \times C_2 \times C_2$
[33, 1]	C_{33}
[34, 1]	D_{17}
[34, 2]	C_{34}
[35, 1]	C_{35}
[36, 1]	$C_9 \times_\rho C_4$
[36, 2]	C_{36}
[36, 3]	$(C_2 \times C_2) \times_\rho C_9$
[36, 4]	D_{18}
[36, 5]	$C_{18} \times C_2$
[36, 6]	$C_3 \times (C_3 \times_\rho C_4)$
[36, 7]	$(C_3 \times C_3) \times_\rho C_4$
[36, 8]	$C_{12} \times C_3$
[36, 9]	$(C_3 \times C_3) \times_\rho C_4$
[36, 10]	$S_3 \times S_3$
[36, 11]	$C_3 \times A_4$
[36, 12]	$C_6 \times S_3$
[36, 13]	$C_2 \times ((C_3 \times C_3) \times_\rho C_2)$
[36, 14]	$C_6 \times C_6$
[37, 1]	C_{37}
[38, 1]	D_{19}
[38, 2]	C_{38}
[39, 1]	$C_{13} \times_\rho C_3$
[39, 2]	C_{39}
[40, 1]	$C_5 \times_\rho C_8$
[40, 2]	C_{40}
[40, 3]	$C_5 \times_\rho C_8$
[40, 4]	$C_5 \times_\rho Q_8$
[40, 5]	$C_4 \times D_5$
[40, 6]	D_{20}
[40, 7]	$C_2 \times (C_5 \times_\rho C_4)$
[40, 8]	$(C_{10} \times C_2) \times_\rho C_2$
[40, 9]	$C_{20} \times C_2$
[40, 10]	$C_5 \times D_4$
[40, 11]	$C_5 \times Q_8$
[40, 12]	$C_2 \times (C_5 \times_\rho C_4)$
[40, 13]	$C_2 \times C_2 \times D_5$
[40, 14]	$C_{10} \times C_2 \times C_2$
[41, 1]	C_{41}
[42, 1]	$(C_7 \times_\rho C_3) \times_\rho C_2$

Continúa en la página siguiente...

GAPID	Grupo
[42, 2]	$C_2 \times (C_7 \times_\rho C_3)$
[42, 3]	$C_7 \times S_3$
[42, 4]	$C_3 \times D_7$
[42, 5]	D_{21}
[42, 6]	C_{42}
[43, 1]	C_{43}
[44, 1]	$C_{11} \times_\rho C_4$
[44, 2]	C_{44}
[44, 3]	D_{22}
[44, 4]	$C_{22} \times C_2$
[45, 1]	C_{45}
[45, 2]	$C_{15} \times C_3$
[46, 1]	D_{23}
[46, 2]	C_{46}
[47, 1]	C_{47}
[48, 1]	$C_3 \times_\rho C_{16}$
[48, 2]	C_{48}
[48, 3]	$(C_4 \times C_4) \times_\rho C_3$
[48, 4]	$C_8 \times S_3$
[48, 5]	$C_{24} \times_\rho C_2$
[48, 6]	$C_{24} \times_\rho C_2$
[48, 7]	D_{24}
[48, 8]	$C_3 \times_\rho Q_{16}$
[48, 9]	$C_2 \times (C_3 \times_\rho C_8)$
[48, 10]	$(C_3 \times_\rho C_8) \times_\rho C_2$
[48, 11]	$C_4 \times (C_3 \times_\rho C_4)$
[48, 12]	$(C_3 \times_\rho C_4) \times_\rho C_4$
[48, 13]	$C_{12} \times_\rho C_4$
[48, 14]	$(C_{12} \times C_2) \times_\rho C_2$
[48, 15]	$(C_3 \times D_4) \times_\rho C_2$
[48, 16]	$(C_3 \times_\rho C_8) \times_\rho C_2$
[48, 17]	$(C_3 \times Q_8) \times_\rho C_2$
[48, 18]	$C_3 \times_\rho Q_{16}$
[48, 19]	$(C_2 \times (C_3 \times_\rho C_4)) \times_\rho C_2$
[48, 20]	$C_{12} \times C_4$
[48, 21]	$C_3 \times ((C_4 \times C_2) \times_\rho C_2)$
[48, 22]	$C_3 \times (C_4 \times_\rho C_4)$
[48, 23]	$C_{24} \times C_2$
[48, 24]	$C_3 \times (C_8 \times_\rho C_2)$
[48, 25]	$C_3 \times D_8$
[48, 26]	$C_3 \times \mathrm{QD}_8$
[48, 27]	$C_3 \times Q_{16}$
[48, 28]	$\mathrm{SL}(2,3) \to G \to C_2$
[48, 29]	$\mathrm{GL}(2,3)$
[48, 30]	$A_4 \times_\rho C_4$
[48, 31]	$C_4 \times A_4$
[48, 32]	$C_2 \times \mathrm{SL}(2,3)$
[48, 33]	$\mathrm{SL}(2,3) \times_\rho C_2$
[48, 34]	$C_2 \times (C_3 \times_\rho Q_8)$
[48, 35]	$C_2 \times C_4 \times S_3$
[48, 36]	$C_2 \times D_{12}$
[48, 37]	$(C_{12} \times C_2) \times_\rho C_2$
[48, 38]	$D_4 \times S_3$
[48, 39]	$(C_2 \times (C_3 \times_\rho C_4)) \times_\rho C_2$
[48, 40]	$Q_8 \times S_3$

Continúa en la página siguiente...

GAPID	Grupo
[48, 41]	$(C_4 \times S_3) \times_\rho C_2$
[48, 42]	$C_2 \times C_2 \times (C_3 \times_\rho C_4)$
[48, 43]	$C_2 \times ((C_6 \times C_2) \times_\rho C_2)$
[48, 44]	$C_{12} \times C_2 \times C_2$
[48, 45]	$C_6 \times D_4$
[48, 46]	$C_6 \times Q_8$
[48, 47]	$C_3 \times ((C_4 \times C_2) \times_\rho C_2)$
[48, 48]	$C_2 \times S_4$
[48, 49]	$C_2 \times C_2 \times A_4$
[48, 50]	$(C_2 \times C_2 \times C_2 \times C_2) \times_\rho C_3$
[48, 51]	$C_2 \times C_2 \times C_2 \times S_3$
[48, 52]	$C_6 \times C_2 \times C_2 \times C_2$
[49, 1]	C_{49}
[49, 2]	$C_7 \times C_7$
[50, 1]	D_{25}
[50, 2]	C_{50}
[50, 3]	$C_5 \times D_5$
[50, 4]	$(C_5 \times C_5) \times_\rho C_2$
[50, 5]	$C_{10} \times C_5$
[51, 1]	C_{51}
[52, 1]	$C_{13} \times_\rho C_4$
[52, 2]	C_{52}
[52, 3]	$C_{13} \times_\rho C_4$
[52, 4]	D_{26}
[52, 5]	$C_{26} \times C_2$
[53, 1]	C_{53}
[54, 1]	D_{27}
[54, 2]	C_{54}
[54, 3]	$C_3 \times D_9$
[54, 4]	$C_9 \times S_3$
[54, 5]	$((C_3 \times C_3) \times_\rho C_3) \times_\rho C_2$
[54, 6]	$(C_9 \times_\rho C_3) \times_\rho C_2$
[54, 7]	$(C_9 \times C_3) \times_\rho C_2$
[54, 8]	$((C_3 \times C_3) \times_\rho C_3) \times_\rho C_2$
[54, 9]	$C_{18} \times C_3$
[54, 10]	$C_2 \times ((C_3 \times C_3) \times_\rho C_3)$
[54, 11]	$C_2 \times (C_9 \times_\rho C_3)$
[54, 12]	$C_3 \times C_3 \times S_3$
[54, 13]	$C_3 \times ((C_3 \times C_3) \times_\rho C_2)$
[54, 14]	$(C_3 \times C_3 \times C_3) \times_\rho C_2$
[54, 15]	$C_6 \times C_3 \times C_3$
[55, 1]	$C_{11} \times_\rho C_5$
[55, 2]	C_{55}
[56, 1]	$C_7 \times_\rho C_8$
[56, 2]	C_{56}
[56, 3]	$C_7 \times_\rho Q_8$
[56, 4]	$C_4 \times D_7$
[56, 5]	D_{28}
[56, 6]	$C_2 \times (C_7 \times_\rho C_4)$
[56, 7]	$(C_{14} \times C_2) \times_\rho C_2$
[56, 8]	$C_{28} \times C_2$
[56, 9]	$C_7 \times D_4$
[56, 10]	$C_7 \times Q_8$
[56, 11]	$(C_2 \times C_2 \times C_2) \times_\rho C_7$
[56, 12]	$C_2 \times C_2 \times D_7$

Continúa en la página siguiente...

GAPID	Grupo
[56, 13]	$C_{14} \times C_2 \times C_2$
[57, 1]	$C_{19} \times_\rho C_3$
[57, 2]	C_{57}
[58, 1]	D_{29}
[58, 2]	C_{58}
[59, 1]	C_{59}
[60, 1]	$C_5 \times (C_3 \times_\rho C_4)$
[60, 2]	$C_3 \times (C_5 \times_\rho C_4)$
[60, 3]	$C_{15} \times_\rho C_4$
[60, 4]	C_{60}
[60, 5]	A_5
[60, 6]	$C_3 \times (C_5 \times_\rho C_4)$
[60, 7]	$C_{15} \times_\rho C_4$
[60, 8]	$S_3 \times D_5$
[60, 9]	$C_5 \times A_4$
[60, 10]	$C_6 \times D_5$
[60, 11]	$C_{10} \times S_3$
[60, 12]	D_{30}
[60, 13]	$C_{30} \times C_2$
[61, 1]	C_{61}
[62, 1]	D_{31}
[62, 2]	C_{62}
[63, 1]	$C_7 \times_\rho C_9$
[63, 2]	C_{63}
[63, 3]	$C_3 \times (C_7 \times_\rho C_3)$
[63, 4]	$C_{21} \times C_3$
[64, 1]	C_{64}
[64, 2]	$C_8 \times C_8$
[64, 3]	$C_8 \times_\rho C_8$
[64, 4]	$((C_8 \times C_2) \times_\rho C_2) \times_\rho C_2$
[64, 5]	$(C_4 \times C_2) \times_\rho C_8$
[64, 6]	$(C_8 \times C_4) \times_\rho C_2$
[64, 7]	$Q_8 \times_\rho C_8$
[64, 8]	$((C_8 \times C_2) \times_\rho C_2) \times_\rho C_2$
[64, 9]	$(C_2 \times Q_8) \times_\rho C_4$
[64, 10]	$(C_8 \times_\rho C_4) \times_\rho C_2$
[64, 11]	$(C_4 \times C_2) \to G \to (C_4 \times C_2)$
[64, 12]	$(C_4 \times_\rho C_8) \times_\rho C_2$
[64, 13]	$(C_4 \times C_2) \to G \to (C_4 \times C_2)$
[64, 14]	$(C_4 \times C_2) \to G \to (C_4 \times C_2)$
[64, 15]	$C_8 \times_\rho C_8$
[64, 16]	$C_8 \times_\rho C_8$
[64, 17]	$(C_8 \times C_2) \times_\rho C_4$
[64, 18]	$(C_8 \times C_2) \times_\rho C_4$
[64, 19]	$C_4 \to G \to (C_4 \times C_4)$
[64, 20]	$(C_4 \times C_4) \times_\rho C_4$
[64, 21]	$(C_8 \times C_2) \times_\rho C_4$
[64, 22]	$C_4 \to G \to (C_4 \times C_4)$
[64, 23]	$(C_4 \times C_2 \times C_2) \times_\rho C_4$
[64, 24]	$(C_8 \times_\rho C_2) \times_\rho C_4$
[64, 25]	$(C_8 \times C_2) \times_\rho C_4$
[64, 26]	$C_{16} \times C_4$
[64, 27]	$C_{16} \times_\rho C_4$
[64, 28]	$C_{16} \times_\rho C_4$
[64, 29]	$(C_{16} \times C_2) \times_\rho C_2$

Continúa en la página siguiente...

GAPID	Grupo
[64, 30]	$(C_{16} \times_\rho C_2) \times_\rho C_2$
[64, 31]	$(C_{16} \times C_2) \times_\rho C_2$
[64, 32]	$((C_8 \times_\rho C_2) \times_\rho C_2) \times_\rho C_2$
[64, 33]	$(C_4 \times C_2 \times C_2) \times_\rho C_4$
[64, 34]	$(((C_4 \times C_2) \times_\rho C_2) \times_\rho C_2) \times_\rho C_2$
[64, 35]	$(C_4 \times C_4) \times_\rho C_4$
[64, 36]	$(C_2 \times C_2) \to G \to (C_4 \times C_2)) \times_\rho C_2$
[64, 37]	$(C_4 \times C_2) \to G \to (C_4 \times C_2)$
[64, 38]	$(C_{16} \times C_2) \times_\rho C_2$
[64, 39]	$Q_{16} \times_\rho C_4$
[64, 40]	$(C_{16} \times C_2) \times_\rho C_2$
[64, 41]	$(C_{16} \times_\rho C_2) \times_\rho C_2$
[64, 42]	$(C_{16} \times_\rho C_2) \times_\rho C_2$
[64, 43]	$C_8 \to G \to (C_4 \times C_2)$
[64, 44]	$C_4 \times_\rho C_{16}$
[64, 45]	$C_4 \to G \to (C_8 \times C_2)$
[64, 46]	$C_{16} \times_\rho C_4$
[64, 47]	$C_{16} \times_\rho C_4$
[64, 48]	$C_{16} \times_\rho C_4$
[64, 49]	$C_8 \to G \to (C_4 \times C_2)$
[64, 50]	$C_{32} \times C_2$
[64, 51]	$C_{32} \times_\rho C_2$
[64, 52]	D_{32}
[64, 53]	QD_{32}
[64, 54]	Q_{64}
[64, 55]	$C_4 \times C_4 \times C_4$
[64, 56]	$C_2 \times ((C_4 \times C_2) \times_\rho C_4)$
[64, 57]	$(C_4 \times C_4) \times_\rho C_4$
[64, 58]	$C_4 \times ((C_4 \times C_2) \times_\rho C_2)$
[64, 59]	$C_4 \times (C_4 \times_\rho C_4)$
[64, 60]	$(C_2 \times ((C_4 \times C_2) \times_\rho C_2)) \times_\rho C_2$
[64, 61]	$(C_2 \times (C_4 \times_\rho C_4)) \times_\rho C_2$
[64, 62]	$((C_4 \times C_2) \times_\rho C_4) \times_\rho C_2$
[64, 63]	$(C_4 \times C_4) \times_\rho C_4$
[64, 64]	$(C_4 \times C_4) \times_\rho C_4$
[64, 65]	$(C_4 \times C_4) \times_\rho C_4$
[64, 66]	$(C_2 \times (C_4 \times_\rho C_4)) \times_\rho C_2$
[64, 67]	$(C_4 \times C_2 \times C_2 \times C_2) \times_\rho C_2$
[64, 68]	$(C_4 \times_\rho C_4) \times_\rho C_4$
[64, 69]	$(C_4 \times C_4 \times C_2) \times_\rho C_2$
[64, 70]	$(C_4 \times_\rho C_4) \times_\rho C_4$
[64, 71]	$(C_4 \times C_4 \times C_2) \times_\rho C_2$
[64, 72]	$(C_2 \times Q_8) \times_\rho C_4$
[64, 73]	$(C_2 \times C_2 \times D_4) \times_\rho C_2$
[64, 74]	$(C_2 \times C_2 \times Q_8) \times_\rho C_2$
[64, 75]	$(C_2 \times ((C_4 \times C_2) \times_\rho C_2)) \times_\rho C_2$
[64, 76]	$(C_4 \times C_2) \times_\rho Q_8$
[64, 77]	$(C_2 \times (C_4 \times_\rho C_4)) \times_\rho C_2$
[64, 78]	$(C_2 \times (C_4 \times_\rho C_4)) \times_\rho C_2$
[64, 79]	$(C_2 \times C_2 \times C_2) \to G \to (C_2 \times C_2 \times C_2)$
[64, 80]	$(C_2 \times (C_4 \times_\rho C_4)) \times_\rho C_2$
[64, 81]	$(C_2 \times C_2 \times C_2) \to G \to (C_2 \times C_2 \times C_2)$
[64, 82]	$(C_2 \times C_2 \times C_2) \to G \to (C_2 \times C_2 \times C_2)$
[64, 83]	$C_8 \times C_4 \times C_2$
[64, 84]	$C_2 \times (C_8 \times_\rho C_4)$

Continúa en la página siguiente...

GAPID	Grupo
[64, 85]	$C_4 \times (C_8 \times_\rho C_2)$
[64, 86]	$(C_8 \times C_4) \times_\rho C_2$
[64, 87]	$C_2 \times ((C_8 \times C_2) \times_\rho C_2)$
[64, 88]	$(C_2 \times (C_8 \times_\rho C_2)) \times_\rho C_2$
[64, 89]	$(C_8 \times C_2 \times C_2) \times_\rho C_2$
[64, 90]	$C_2 \times (((C_4 \times C_2) \times_\rho C_2) \times_\rho C_2)$
[64, 91]	$(((C_4 \times C_2) \times_\rho C_2) \times_\rho C_2) \times_\rho C_2$
[64, 92]	$C_2 \times ((C_8 \times_\rho C_2) \times_\rho C_2)$
[64, 93]	$(C_2 \times C_2) \to G \to (C_4 \times C_2))$
[64, 94]	$(C_2 \times (C_8 \times_\rho C_2)) \times_\rho C_2$
[64, 95]	$C_2 \times ((C_8 \times C_2) \times_\rho C_2)$
[64, 96]	$C_2 \times (Q_8 \times_\rho C_4)$
[64, 97]	$(C_8 \times C_2 \times C_2) \times_\rho C_2$
[64, 98]	$(C_2 \times (C_8 \times_\rho C_2)) \times_\rho C_2$
[64, 99]	$(C_2 \times (C_8 \times_\rho C_2)) \times_\rho C_2$
[64, 100]	$(Q_8 \times_\rho C_4) \times_\rho C_2$
[64, 101]	$C_2 \times ((C_4 \times C_4) \times_\rho C_2)$
[64, 102]	$(C_2 \times (C_8 \times_\rho C_2)) \times_\rho C_2$
[64, 103]	$C_2 \times (C_4 \times_\rho C_8)$
[64, 104]	$(C_4 \times_\rho C_8) \times_\rho C_2$
[64, 105]	$(C_4 \times_\rho C_8) \times_\rho C_2$
[64, 106]	$C_2 \times (C_8 \times_\rho C_4)$
[64, 107]	$C_2 \times (C_8 \times_\rho C_4)$
[64, 108]	$(C_8 \times_\rho C_4) \times_\rho C_2$
[64, 109]	$(C_8 \times_\rho C_4) \times_\rho C_2$
[64, 110]	$C_4 \to G \to (C_4 \times C_2))$
[64, 111]	$C_4 \to G \to (C_4 \times C_2)) \times_\rho C_2$
[64, 112]	$(C_8 \times C_4) \times_\rho C_2$
[64, 113]	$(C_4 \times_\rho C_8) \times_\rho C_2$
[64, 114]	$(C_8 \times C_4) \times_\rho C_2$
[64, 115]	$C_8 \times D_4$
[64, 116]	$(C_8 \times C_2 \times C_2) \times_\rho C_2$
[64, 117]	$(C_8 \times C_4) \times_\rho C_2$
[64, 118]	$C_4 \times D_8$
[64, 119]	$C_4 \times \mathrm{QD}_8$
[64, 120]	$C_4 \times Q_{16}$
[64, 121]	$(C_4 \times Q_8) \times_\rho C_2$
[64, 122]	$Q_{16} \times_\rho C_4$
[64, 123]	$(C_4 \times D_4) \times_\rho C_2$
[64, 124]	$(C_8 \times C_4) \times_\rho C_2$
[64, 125]	$((C_4 \times C_4) \times_\rho C_2) \times_\rho C_2$
[64, 126]	$C_8 \times Q_8$
[64, 127]	$C_8 \times_\rho Q_8$
[64, 128]	$(C_2 \times C_2 \times D_4) \times_\rho C_2$
[64, 129]	$(C_2 \times C_2 \times Q_8) \times_\rho C_2$
[64, 130]	$(C_2 \times D_8) \times_\rho C_2$
[64, 131]	$(C_2 \times \mathrm{QD}_8) \times_\rho C_2$
[64, 132]	$(C_2 \times Q_{16}) \times_\rho C_2$
[64, 133]	$(C_2 \times Q_{16}) \times_\rho C_2$
[64, 134]	$((C_4 \times C_4) \times_\rho C_2) \times_\rho C_2$
[64, 135]	$((C_4 \times C_4) \times_\rho C_2) \times_\rho C_2$
[64, 136]	$((C_4 \times C_4) \times_\rho C_2) \times_\rho C_2$
[64, 137]	$((C_4 \times C_4) \times_\rho C_2) \times_\rho C_2$
[64, 138]	$(((C_4 \times C_2) \times_\rho C_2) \times_\rho C_2) \times_\rho C_2$
[64, 139]	$(((C_4 \times C_2) \times_\rho C_2) \times_\rho C_2) \times_\rho C_2$

Continúa en la página siguiente...

GAPID	Grupo
[64, 140]	$(C_4 \times D_4) \times_\rho C_2$
[64, 141]	$(C_2 \times \mathrm{QD}_8) \times_\rho C_2$
[64, 142]	$(Q_8 \times_\rho C_4) \times_\rho C_2$
[64, 143]	$C_4 \times_\rho Q_{16}$
[64, 144]	$(C_4 \times D_4) \times_\rho C_2$
[64, 145]	$(C_2 \times Q_{16}) \times_\rho C_2$
[64, 146]	$(C_8 \times C_2 \times C_2) \times_\rho C_2$
[64, 147]	$(C_8 \times C_2 \times C_2) \times_\rho C_2$
[64, 148]	$(C_2 \times Q_{16}) \times_\rho C_2$
[64, 149]	$(C_2 \times (C_8 \times_\rho C_2)) \times_\rho C_2$
[64, 150]	$(C_2 \times (C_8 \times_\rho C_2)) \times_\rho C_2$
[64, 151]	$(C_2 \times Q_{16}) \times_\rho C_2$
[64, 152]	$(C_2 \times \mathrm{QD}_8) \times_\rho C_2$
[64, 153]	$(C_2 \times D_8) \times_\rho C_2$
[64, 154]	$(C_2 \times Q_{16}) \times_\rho C_2$
[64, 155]	$(C_8 \times_\rho C_4) \times_\rho C_2$
[64, 156]	$Q_8 \times_\rho Q_8$
[64, 157]	$(C_8 \times_\rho C_4) \times_\rho C_2$
[64, 158]	$Q_8 \times_\rho Q_8$
[64, 159]	$(C_8 \times_\rho C_4) \times_\rho C_2$
[64, 160]	$(C_4 \times C_2) \to G \to (C_2 \times C_2 \times C_2)$
[64, 161]	$(C_2 \times (C_4 \times_\rho C_4)) \times_\rho C_2$
[64, 162]	$(C_2 \times (C_4 \times_\rho C_4)) \times_\rho C_2$
[64, 163]	$((C_8 \times C_2) \times_\rho C_2) \times_\rho C_2$
[64, 164]	$(Q_8 \times_\rho C_4) \times_\rho C_2$
[64, 165]	$(Q_8 \times_\rho C_4) \times_\rho C_2$
[64, 166]	$(C_8 \times_\rho C_4) \times_\rho C_2$
[64, 167]	$(C_8 \times C_4) \times_\rho C_2$
[64, 168]	$(C_4 \times C_2) \to G \to (C_2 \times C_2 \times C_2)$
[64, 169]	$(C_8 \times C_4) \times_\rho C_2$
[64, 170]	$(Q_8 \times_\rho C_4) \times_\rho C_2$
[64, 171]	$((C_8 \times C_2) \times_\rho C_2) \times_\rho C_2$
[64, 172]	$(C_4 \times C_2) \to G \to (C_2 \times C_2 \times C_2)$
[64, 173]	$(C_8 \times C_4) \times_\rho C_2$
[64, 174]	$(C_8 \times C_4) \times_\rho C_2$
[64, 175]	$C_4 \times_\rho Q_{16}$
[64, 176]	$(C_8 \times C_4) \times_\rho C_2$
[64, 177]	$(C_2 \times D_8) \times_\rho C_2$
[64, 178]	$(C_2 \times Q_{16}) \times_\rho C_2$
[64, 179]	$C_8 \times_\rho Q_8$
[64, 180]	$(C_4 \times C_2) \to G \to (C_2 \times C_2 \times C_2)$
[64, 181]	$C_8 \times_\rho Q_8$
[64, 182]	$C_8 \times_\rho Q_8$
[64, 183]	$C_{16} \times C_2 \times C_2$
[64, 184]	$C_2 \times (C_{16} \times_\rho C_2)$
[64, 185]	$(C_{16} \times C_2) \times_\rho C_2$
[64, 186]	$C_2 \times D_{16}$
[64, 187]	$C_2 \times \mathrm{QD}_{16}$
[64, 188]	$C_2 \times Q_{32}$
[64, 189]	$(C_{16} \times C_2) \times_\rho C_2$
[64, 190]	$(C_2 \times D_8) \times_\rho C_2$
[64, 191]	$(C_2 \times Q_{16}) \times_\rho C_2$
[64, 192]	$C_4 \times C_4 \times C_2 \times C_2$
[64, 193]	$C_2 \times C_2 \times ((C_4 \times C_2) \times_\rho C_2)$
[64, 194]	$C_2 \times C_2 \times (C_4 \times_\rho C_4)$

Continúa en la página siguiente...

GAPID	Grupo
[64, 195]	$C_2 \times ((C_4 \times C_4) \times_\rho C_2)$
[64, 196]	$C_2 \times C_4 \times D_4$
[64, 197]	$C_2 \times C_4 \times Q_8$
[64, 198]	$C_4 \times ((C_4 \times C_2) \times_\rho C_2)$
[64, 199]	$(C_4 \times D_4) \times_\rho C_2$
[64, 200]	$(C_4 \times Q_8) \times_\rho C_2$
[64, 201]	$(C_4 \times Q_8) \times_\rho C_2$
[64, 202]	$C_2 \times ((C_2 \times C_2 \times C_2 \times C_2) \times_\rho C_2)$
[64, 203]	$C_2 \times ((C_4 \times C_2 \times C_2) \times_\rho C_2)$
[64, 204]	$C_2 \times ((C_2 \times Q_8) \times_\rho C_2)$
[64, 205]	$C_2 \times ((C_4 \times C_2 \times C_2) \times_\rho C_2)$
[64, 206]	$(C_4 \times C_2 \times C_2 \times C_2) \times_\rho C_2$
[64, 207]	$C_2 \times ((C_4 \times C_4) \times_\rho C_2)$
[64, 208]	$C_2 \times ((C_2 \times C_2) \to G \to (C_2 \times C_2 \times C_2))$
[64, 209]	$C_2 \times ((C_4 \times C_4) \times_\rho C_2)$
[64, 210]	$(C_4 \times C_4 \times C_2) \times_\rho C_2$
[64, 211]	$C_2 \times ((C_4 \times C_4) \times_\rho C_2)$
[64, 212]	$C_2 \times (C_4 \times_\rho Q_8)$
[64, 213]	$(C_4 \times C_4 \times C_2) \times_\rho C_2$
[64, 214]	$(C_4 \times Q_8) \times_\rho C_2$
[64, 215]	$(C_2 \times C_2 \times D_4) \times_\rho C_2$
[64, 216]	$(C_2 \times C_2 \times D_4) \times_\rho C_2$
[64, 217]	$(C_2 \times C_2 \times Q_8) \times_\rho C_2$
[64, 218]	$(C_2 \times ((C_4 \times C_2) \times_\rho C_2)) \times_\rho C_2$
[64, 219]	$(C_4 \times D_4) \times_\rho C_2$
[64, 220]	$(C_4 \times D_4) \times_\rho C_2$
[64, 221]	$(C_4 \times D_4) \times_\rho C_2$
[64, 222]	$(C_4 \times Q_8) \times_\rho C_2$
[64, 223]	$(C_4 \times Q_8) \times_\rho C_2$
[64, 224]	$((C_2 \times Q_8) \times_\rho C_2) \times_\rho C_2$
[64, 225]	$(C_4 \times_\rho Q_8) \times_\rho C_2$
[64, 226]	$D_4 \times D_4$
[64, 227]	$(C_2 \times C_2 \times D_4) \times_\rho C_2$
[64, 228]	$(C_4 \times D_4) \times_\rho C_2$
[64, 229]	$(C_2 \times C_2 \times Q_8) \times_\rho C_2$
[64, 230]	$Q_8 \times D_4$
[64, 231]	$(C_4 \times D_4) \times_\rho C_2$
[64, 232]	$(C_4 \times D_4) \times_\rho C_2$
[64, 233]	$(C_4 \times Q_8) \times_\rho C_2$
[64, 234]	$(C_4 \times D_4) \times_\rho C_2$
[64, 235]	$(C_4 \times Q_8) \times_\rho C_2$
[64, 236]	$(C_4 \times D_4) \times_\rho C_2$
[64, 237]	$(C_4 \times Q_8) \times_\rho C_2$
[64, 238]	$Q_8 \times_\rho Q_8$
[64, 239]	$Q_8 \times Q_8$
[64, 240]	$(C_4 \times D_4) \times_\rho C_2$
[64, 241]	$((C_4 \times C_2 \times C_2) \times_\rho C_2) \times_\rho C_2$
[64, 242]	$((C_4 \times C_4) \times_\rho C_2) \times_\rho C_2$
[64, 243]	$((C_2 \times C_2) \to G \to (C_2 \times C_2 \times C_2)) \times_\rho C_2$
[64, 244]	$((C_4 \times C_4) \times_\rho C_2) \times_\rho C_2$
[64, 245]	$(C_2 \times C_2) \to G \to (C_2 \times C_2 \times C_2 \times C_2)$
[64, 246]	$C_8 \times C_2 \times C_2 \times C_2$
[64, 247]	$C_2 \times C_2 \times (C_8 \times_\rho C_2)$
[64, 248]	$C_2 \times ((C_8 \times C_2) \times_\rho C_2)$
[64, 249]	$(C_2 \times (C_8 \times_\rho C_2)) \times_\rho C_2$

Continúa en la página siguiente...

GAPID	Grupo
[64, 250]	$C_2 \times C_2 \times D_8$
[64, 251]	$C_2 \times C_2 \times \mathrm{QD}_8$
[64, 252]	$C_2 \times C_2 \times Q_{16}$
[64, 253]	$C_2 \times ((C_8 \times C_2) \times_\rho C_2)$
[64, 254]	$C_2 \times ((C_2 \times D_4) \times_\rho C_2)$
[64, 255]	$C_2 \times ((C_2 \times Q_8) \times_\rho C_2)$
[64, 256]	$(C_2 \times (C_8 \times_\rho C_2)) \times_\rho C_2$
[64, 257]	$(C_2 \times D_8) \times_\rho C_2$
[64, 258]	$(C_2 \times \mathrm{QD}_8) \times_\rho C_2$
[64, 259]	$(C_2 \times Q_{16}) \times_\rho C_2$
[64, 260]	$C_4 \times C_2 \times C_2 \times C_2 \times C_2$
[64, 261]	$C_2 \times C_2 \times C_2 \times D_4$
[64, 262]	$C_2 \times C_2 \times C_2 \times Q_8$
[64, 263]	$C_2 \times C_2 \times ((C_4 \times C_2) \times_\rho C_2)$
[64, 264]	$C_2 \times ((C_2 \times D_4) \times_\rho C_2)$
[64, 265]	$C_2 \times ((C_2 \times Q_8) \times_\rho C_2)$
[64, 266]	$(C_2 \times ((C_4 \times C_2) \times_\rho C_2)) \times_\rho C_2$
[64, 267]	$C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2$
[65, 1]	C_{65}
[66, 1]	$C_{11} \times S_3$
[66, 2]	$C_3 \times D_{11}$
[66, 3]	D_{33}
[66, 4]	C_{66}
[67, 1]	C_{67}
[68, 1]	$C_{17} \times_\rho C_4$
[68, 2]	C_{68}
[68, 3]	$C_{17} \times_\rho C_4$
[68, 4]	D_{34}
[68, 5]	$C_{34} \times C_2$
[69, 1]	C_{69}
[70, 1]	$C_7 \times D_5$
[70, 2]	$C_5 \times D_7$
[70, 3]	D_{35}
[70, 4]	C_{70}
[71, 1]	C_{71}
[72, 1]	$C_9 \times_\rho C_8$
[72, 2]	C_{72}
[72, 3]	$Q_8 \times_\rho C_9$
[72, 4]	$C_9 \times_\rho Q_8$
[72, 5]	$C_4 \times D_9$
[72, 6]	D_{36}
[72, 7]	$C_2 \times (C_9 \times_\rho C_4)$
[72, 8]	$(C_{18} \times C_2) \times_\rho C_2$
[72, 9]	$C_{36} \times C_2$
[72, 10]	$C_9 \times D_4$
[72, 11]	$C_9 \times Q_8$
[72, 12]	$C_3 \times (C_3 \times_\rho C_8)$
[72, 13]	$(C_3 \times C_3) \times_\rho C_8$
[72, 14]	$C_{24} \times C_3$
[72, 15]	$((C_2 \times C_2) \times_\rho C_9) \times_\rho C_2$
[72, 16]	$C_2 \times ((C_2 \times C_2) \times_\rho C_9)$
[72, 17]	$C_2 \times C_2 \times D_9$
[72, 18]	$C_{18} \times C_2 \times C_2$
[72, 19]	$(C_3 \times C_3) \times_\rho C_8$
[72, 20]	$(C_3 \times_\rho C_4) \times S_3$

Continúa en la página siguiente...

GAPID	Grupo
[72, 21]	$(C_3 \times (C_3 \times_\rho C_4)) \times_\rho C_2$
[72, 22]	$(C_6 \times S_3) \times_\rho C_2$
[72, 23]	$(C_6 \times S_3) \times_\rho C_2$
[72, 24]	$(C_3 \times C_3) \times_\rho Q_8$
[72, 25]	$C_3 \times \mathrm{SL}(2,3)$
[72, 26]	$C_3 \times (C_3 \times_\rho Q_8)$
[72, 27]	$C_{12} \times S_3$
[72, 28]	$C_3 \times D_{12}$
[72, 29]	$C_6 \times (C_3 \times_\rho C_4)$
[72, 30]	$C_3 \times ((C_6 \times C_2) \times_\rho C_2)$
[72, 31]	$(C_3 \times C_3) \times_\rho Q_8$
[72, 32]	$C_4 \times ((C_3 \times C_3) \times_\rho C_2)$
[72, 33]	$(C_{12} \times C_3) \times_\rho C_2$
[72, 34]	$C_2 \times ((C_3 \times C_3) \times_\rho C_4)$
[72, 35]	$(C_6 \times C_6) \times_\rho C_2$
[72, 36]	$C_{12} \times C_6$
[72, 37]	$C_3 \times C_3 \times D_4$
[72, 38]	$C_3 \times C_3 \times Q_8$
[72, 39]	$(C_3 \times C_3) \times_\rho C_8$
[72, 40]	$(S_3 \times S_3) \times_\rho C_2$
[72, 41]	$(C_3 \times C_3) \times_\rho Q_8$
[72, 42]	$C_3 \times S_4$
[72, 43]	$(C_3 \times A_4) \times_\rho C_2$
[72, 44]	$A_4 \times S_3$
[72, 45]	$C_2 \times ((C_3 \times C_3) \times_\rho C_4)$
[72, 46]	$C_2 \times S_3 \times S_3$
[72, 47]	$C_6 \times A_4$
[72, 48]	$C_2 \times C_6 \times S_3$
[72, 49]	$C_2 \times C_2 \times ((C_3 \times C_3) \times_\rho C_2)$
[72, 50]	$C_6 \times C_6 \times C_2$
[73, 1]	C_{73}
[74, 1]	D_{37}
[74, 2]	C_{74}
[75, 1]	C_{75}
[75, 2]	$(C_5 \times C_5) \times_\rho C_3$
[75, 3]	$C_{15} \times C_5$
[76, 1]	$C_{19} \times_\rho C_4$
[76, 2]	C_{76}
[76, 3]	D_{38}
[76, 4]	$C_{38} \times C_2$
[77, 1]	C_{77}
[78, 1]	$(C_{13} \times_\rho C_3) \times_\rho C_2$
[78, 2]	$C_2 \times (C_{13} \times_\rho C_3)$
[78, 3]	$C_{13} \times S_3$
[78, 4]	$C_3 \times D_{13}$
[78, 5]	D_{39}
[78, 6]	C_{78}
[79, 1]	C_{79}
[80, 1]	$C_5 \times_\rho C_{16}$
[80, 2]	C_{80}
[80, 3]	$C_5 \times_\rho C_{16}$
[80, 4]	$C_8 \times D_5$
[80, 5]	$C_{40} \times_\rho C_2$
[80, 6]	$C_{40} \times_\rho C_2$
[80, 7]	D_{40}

Continúa en la página siguiente...

GAPID	Grupo
[80, 8]	$C_5 \times_\rho Q_{16}$
[80, 9]	$C_2 \times (C_5 \times_\rho C_8)$
[80, 10]	$(C_5 \times_\rho C_8) \times_\rho C_2$
[80, 11]	$C_4 \times (C_5 \times_\rho C_4)$
[80, 12]	$(C_5 \times_\rho C_4) \times_\rho C_4$
[80, 13]	$C_{20} \times_\rho C_4$
[80, 14]	$(C_{20} \times C_2) \times_\rho C_2$
[80, 15]	$(C_5 \times D_4) \times_\rho C_2$
[80, 16]	$(C_5 \times_\rho C_8) \times_\rho C_2$
[80, 17]	$(C_5 \times Q_8) \times_\rho C_2$
[80, 18]	$C_5 \times_\rho Q_{16}$
[80, 19]	$(C_2 \times (C_5 \times_\rho C_4)) \times_\rho C_2$
[80, 20]	$C_{20} \times C_4$
[80, 21]	$C_5 \times ((C_4 \times C_2) \times_\rho C_2)$
[80, 22]	$C_5 \times (C_4 \times_\rho C_4)$
[80, 23]	$C_{40} \times C_2$
[80, 24]	$C_5 \times (C_8 \times_\rho C_2)$
[80, 25]	$C_5 \times D_8$
[80, 26]	$C_5 \times \mathrm{QD}_8$
[80, 27]	$C_5 \times Q_{16}$
[80, 28]	$(C_5 \times_\rho C_8) \times_\rho C_2$
[80, 29]	$(C_5 \times_\rho C_8) \times_\rho C_2$
[80, 30]	$C_4 \times (C_5 \times_\rho C_4)$
[80, 31]	$C_{20} \times_\rho C_4$
[80, 32]	$C_2 \times (C_5 \times_\rho C_8)$
[80, 33]	$(C_5 \times_\rho C_8) \times_\rho C_2$
[80, 34]	$(C_2 \times (C_5 \times_\rho C_4)) \times_\rho C_2$
[80, 35]	$C_2 \times (C_5 \times_\rho Q_8)$
[80, 36]	$C_2 \times C_4 \times D_5$
[80, 37]	$C_2 \times D_{20}$
[80, 38]	$(C_{20} \times C_2) \times_\rho C_2$
[80, 39]	$D_4 \times D_5$
[80, 40]	$(C_2 \times (C_5 \times_\rho C_4)) \times_\rho C_2$
[80, 41]	$Q_8 \times D_5$
[80, 42]	$(C_4 \times D_5) \times_\rho C_2$
[80, 43]	$C_2 \times C_2 \times (C_5 \times_\rho C_4)$
[80, 44]	$C_2 \times ((C_{10} \times C_2) \times_\rho C_2)$
[80, 45]	$C_{20} \times C_2 \times C_2$
[80, 46]	$C_{10} \times D_4$
[80, 47]	$C_{10} \times Q_8$
[80, 48]	$C_5 \times ((C_4 \times C_2) \times_\rho C_2)$
[80, 49]	$(C_2 \times C_2 \times C_2 \times C_2) \times_\rho C_5$
[80, 50]	$C_2 \times C_2 \times (C_5 \times_\rho C_4)$
[80, 51]	$C_2 \times C_2 \times C_2 \times D_5$
[80, 52]	$C_{10} \times C_2 \times C_2 \times C_2$
[81, 1]	C_{81}
[81, 2]	$C_9 \times C_9$
[81, 3]	$(C_9 \times C_3) \times_\rho C_3$
[81, 4]	$C_9 \times_\rho C_9$
[81, 5]	$C_{27} \times C_3$
[81, 6]	$C_{27} \times_\rho C_3$
[81, 7]	$(C_3 \times C_3 \times C_3) \times_\rho C_3$
[81, 8]	$(C_9 \times C_3) \times_\rho C_3$
[81, 9]	$(C_9 \times C_3) \times_\rho C_3$
[81, 10]	$(C_3 \times C_3) \to G \to (C_3 \times C_3)$

Continúa en la página siguiente...

GAPID	Grupo
[81, 11]	$C_9 \times C_3 \times C_3$
[81, 12]	$C_3 \times ((C_3 \times C_3) \times_\rho C_3)$
[81, 13]	$C_3 \times (C_9 \times_\rho C_3)$
[81, 14]	$(C_9 \times C_3) \times_\rho C_3$
[81, 15]	$C_3 \times C_3 \times C_3 \times C_3$
[82, 1]	D_{41}
[82, 2]	C_{82}
[83, 1]	C_{83}
[84, 1]	$(C_7 \times_\rho C_4) \times_\rho C_3$
[84, 2]	$C_4 \times (C_7 \times_\rho C_3)$
[84, 3]	$C_7 \times (C_3 \times_\rho C_4)$
[84, 4]	$C_3 \times (C_7 \times_\rho C_4)$
[84, 5]	$C_{21} \times_\rho C_4$
[84, 6]	C_{84}
[84, 7]	$C_2 \times ((C_7 \times_\rho C_3) \times_\rho C_2)$
[84, 8]	$S_3 \times D_7$
[84, 9]	$C_2 \times C_2 \times (C_7 \times_\rho C_3)$
[84, 10]	$C_7 \times A_4$
[84, 11]	$(C_{14} \times C_2) \times_\rho C_3$
[84, 12]	$C_6 \times D_7$
[84, 13]	$C_{14} \times S_3$
[84, 14]	D_{42}
[84, 15]	$C_{42} \times C_2$
[85, 1]	C_{85}
[86, 1]	D_{43}
[86, 2]	C_{86}
[87, 1]	C_{87}
[88, 1]	$C_{11} \times_\rho C_8$
[88, 2]	C_{88}
[88, 3]	$C_{11} \times_\rho Q_8$
[88, 4]	$C_4 \times D_{11}$
[88, 5]	D_{44}
[88, 6]	$C_2 \times (C_{11} \times_\rho C_4)$
[88, 7]	$(C_{22} \times C_2) \times_\rho C_2$
[88, 8]	$C_{44} \times C_2$
[88, 9]	$C_{11} \times D_4$
[88, 10]	$C_{11} \times Q_8$
[88, 11]	$C_2 \times C_2 \times D_{11}$
[88, 12]	$C_{22} \times C_2 \times C_2$
[89, 1]	C_{89}
[90, 1]	$C_5 \times D_9$
[90, 2]	$C_9 \times D_5$
[90, 3]	D_{45}
[90, 4]	C_{90}
[90, 5]	$C_3 \times C_3 \times D_5$
[90, 6]	$C_{15} \times S_3$
[90, 7]	$C_3 \times D_{15}$
[90, 8]	$C_5 \times ((C_3 \times C_3) \times_\rho C_2)$
[90, 9]	$(C_{15} \times C_3) \times_\rho C_2$
[90, 10]	$C_{30} \times C_3$
[91, 1]	C_{91}
[92, 1]	$C_{23} \times_\rho C_4$
[92, 2]	C_{92}
[92, 3]	D_{46}
[92, 4]	$C_{46} \times C_2$

Continúa en la página siguiente...

GAPID	Grupo
[93, 1]	$C_{31} \times_\rho C_3$
[93, 2]	C_{93}
[94, 1]	D_{47}
[94, 2]	C_{94}
[95, 1]	C_{95}
[96, 1]	$C_3 \times_\rho C_{32}$
[96, 2]	C_{96}
[96, 3]	$((C_4 \times C_2) \times_\rho C_4) \times_\rho C_3$
[96, 4]	$C_{16} \times S_3$
[96, 5]	$C_{48} \times_\rho C_2$
[96, 6]	D_{48}
[96, 7]	$C_{48} \times_\rho C_2$
[96, 8]	$C_3 \times_\rho Q_{32}$
[96, 9]	$C_4 \times (C_3 \times_\rho C_8)$
[96, 10]	$(C_3 \times_\rho C_8) \times_\rho C_4$
[96, 11]	$C_{12} \times_\rho C_8$
[96, 12]	$(C_{12} \times C_4) \times_\rho C_2$
[96, 13]	$(C_3 \times ((C_4 \times C_2) \times_\rho C_2)) \times_\rho C_2$
[96, 14]	$(C_3 \times_\rho C_8) \times_\rho C_4$
[96, 15]	$(C_3 \times_\rho C_8) \times_\rho C_4$
[96, 16]	$(C_2 \times (C_3 \times_\rho C_8)) \times_\rho C_2$
[96, 17]	$(C_3 \times_\rho Q_8) \times_\rho C_4$
[96, 18]	$C_2 \times (C_3 \times_\rho C_{16})$
[96, 19]	$(C_3 \times_\rho C_{16}) \times_\rho C_2$
[96, 20]	$C_8 \times (C_3 \times_\rho C_4)$
[96, 21]	$(C_3 \times_\rho C_4) \times_\rho C_8$
[96, 22]	$C_{24} \times_\rho C_4$
[96, 23]	$(C_3 \times_\rho Q_8) \times_\rho C_4$
[96, 24]	$C_{24} \times_\rho C_4$
[96, 25]	$C_{24} \times_\rho C_4$
[96, 26]	$C_4 \to G \to (C_4 \times C_2))$
[96, 27]	$(C_{24} \times C_2) \times_\rho C_2$
[96, 28]	$(C_{24} \times C_2) \times_\rho C_2$
[96, 29]	$C_4 \to G \to (C_4 \times C_2))$
[96, 30]	$(C_3 \times (C_8 \times_\rho C_2)) \times_\rho C_2$
[96, 31]	$(C_2 \times C_2) \to G \to (C_4 \times C_2))$
[96, 32]	$(C_3 \times (C_8 \times_\rho C_2)) \times_\rho C_2$
[96, 33]	$(C_3 \times D_8) \times_\rho C_2$
[96, 34]	$(C_3 \times_\rho C_{16}) \times_\rho C_2$
[96, 35]	$(C_3 \times Q_{16}) \times_\rho C_2$
[96, 36]	$C_3 \times_\rho Q_{32}$
[96, 37]	$(C_2 \times (C_3 \times_\rho C_8)) \times_\rho C_2$
[96, 38]	$(C_{12} \times C_2) \times_\rho C_4$
[96, 39]	$(C_2 \times (C_3 \times_\rho C_8)) \times_\rho C_2$
[96, 40]	$((C_3 \times_\rho C_8) \times_\rho C_2) \times_\rho C_2$
[96, 41]	$((C_2 \times (C_3 \times_\rho C_4)) \times_\rho C_2) \times_\rho C_2$
[96, 42]	$(C_3 \times Q_8) \times_\rho C_4$
[96, 43]	$(C_2 \times C_2) \to G \to (C_4 \times C_2))$
[96, 44]	$(C_4 \times (C_3 \times_\rho C_4)) \times_\rho C_2$
[96, 45]	$C_3 \times ((C_4 \times C_2) \times_\rho C_4)$
[96, 46]	$C_{24} \times C_4$
[96, 47]	$C_3 \times (C_8 \times_\rho C_4)$
[96, 48]	$C_3 \times ((C_8 \times C_2) \times_\rho C_2)$
[96, 49]	$C_3 \times (((C_4 \times C_2) \times_\rho C_2) \times_\rho C_2)$
[96, 50]	$C_3 \times ((C_8 \times_\rho C_2) \times_\rho C_2)$

Continúa en la página siguiente...

GAPID	Grupo
[96, 51]	$(C_2 \times C_2) \to G \to (C_4 \times C_2))$
[96, 52]	$C_3 \times ((C_8 \times C_2) \times_\rho C_2)$
[96, 53]	$C_3 \times (Q_8 \times_\rho C_4)$
[96, 54]	$C_3 \times ((C_4 \times C_4) \times_\rho C_2)$
[96, 55]	$C_3 \times (C_4 \times_\rho C_8)$
[96, 56]	$C_3 \times (C_8 \times_\rho C_4)$
[96, 57]	$C_3 \times (C_8 \times_\rho C_4)$
[96, 58]	$C_4 \to G \to (C_4 \times C_2))$
[96, 59]	$C_{48} \times C_2$
[96, 60]	$C_3 \times (C_{16} \times_\rho C_2)$
[96, 61]	$C_3 \times D_{16}$
[96, 62]	$C_3 \times \mathrm{QD}_{16}$
[96, 63]	$C_3 \times Q_{32}$
[96, 64]	$((C_4 \times C_4) \times_\rho C_3) \times_\rho C_2$
[96, 65]	$A_4 \times_\rho C_8$
[96, 66]	$\mathrm{SL}(2,3) \times_\rho C_4$
[96, 67]	$\mathrm{SL}(2,3) \times_\rho C_4$
[96, 68]	$C_2 \times ((C_4 \times C_4) \times_\rho C_3)$
[96, 69]	$C_4 \times \mathrm{SL}(2,3)$
[96, 70]	$((C_2 \times C_2 \times C_2 \times C_2) \times_\rho C_3) \times_\rho C_2$
[96, 71]	$((C_4 \times C_4) \times_\rho C_3) \times_\rho C_2$
[96, 72]	$((C_4 \times C_4) \times_\rho C_3) \times_\rho C_2$
[96, 73]	$C_8 \times A_4$
[96, 74]	$((C_8 \times C_2) \times_\rho C_2) \times_\rho C_3$
[96, 75]	$C_4 \times (C_3 \times_\rho Q_8)$
[96, 76]	$C_{12} \times_\rho Q_8$
[96, 77]	$C_3 \times_\rho ((C_2 \times C_2) \to G \to (C_2 \times C_2 \times C_2))$
[96, 78]	$C_4 \times C_4 \times S_3$
[96, 79]	$(C_{12} \times C_4) \times_\rho C_2$
[96, 80]	$C_4 \times D_{12}$
[96, 81]	$(C_{12} \times C_4) \times_\rho C_2$
[96, 82]	$(C_{12} \times C_4) \times_\rho C_2$
[96, 83]	$(C_{12} \times C_4) \times_\rho C_2$
[96, 84]	$(C_4 \times (C_3 \times_\rho C_4)) \times_\rho C_2$
[96, 85]	$(C_2 \times (C_3 \times_\rho Q_8)) \times_\rho C_2$
[96, 86]	$(C_4 \times (C_3 \times_\rho C_4)) \times_\rho C_2$
[96, 87]	$((C_4 \times C_2) \times_\rho C_2) \times S_3$
[96, 88]	$(C_2 \times C_4 \times S_3) \times_\rho C_2$
[96, 89]	$(C_2 \times C_2 \times C_2 \times S_3) \times_\rho C_2$
[96, 90]	$(C_2 \times C_4 \times S_3) \times_\rho C_2$
[96, 91]	$(C_2 \times C_4 \times S_3) \times_\rho C_2$
[96, 92]	$(C_2 \times (C_3 \times_\rho Q_8)) \times_\rho C_2$
[96, 93]	$(C_2 \times C_2 \times (C_3 \times_\rho C_4)) \times_\rho C_2$
[96, 94]	$(C_3 \times_\rho Q_8) \times_\rho C_4$
[96, 95]	$C_{12} \times_\rho Q_8$
[96, 96]	$C_3 \times_\rho ((C_2 \times C_2) \to G \to (C_2 \times C_2 \times C))$
[96, 97]	$C_3 \times_\rho ((C_2 \times C_2) \to G \to (C_2 \times C_2 \times C))$
[96, 98]	$(C_4 \times_\rho C_4) \times S_3$
[96, 99]	$(C_4 \times (C_3 \times_\rho C_4)) \times_\rho C_2$
[96, 100]	$(C_2 \times C_4 \times S_3) \times_\rho C_2$
[96, 101]	$(C_2 \times C_4 \times S_3) \times_\rho C_2$
[96, 102]	$(C_2 \times C_4 \times S_3) \times_\rho C_2$
[96, 103]	$(C_2 \times (C_3 \times_\rho Q_8)) \times_\rho C_2$
[96, 104]	$(C_3 \times (C_4 \times_\rho C_4)) \times_\rho C_2$
[96, 105]	$(C_3 \times (C_4 \times_\rho C_4)) \times_\rho C_2$

Continúa en la página siguiente...

GAPID	Grupo
[96, 106]	$C_2 \times C_8 \times S_3$
[96, 107]	$C_2 \times (C_{24} \times_\rho C_2)$
[96, 108]	$(C_{24} \times C_2) \times_\rho C_2$
[96, 109]	$C_2 \times (C_{24} \times_\rho C_2)$
[96, 110]	$C_2 \times D_{24}$
[96, 111]	$(C_{24} \times C_2) \times_\rho C_2$
[96, 112]	$C_2 \times (C_3 \times_\rho Q_{16})$
[96, 113]	$(C_8 \times_\rho C_2) \times S_3$
[96, 114]	$(C_8 \times S_3) \times_\rho C_2$
[96, 115]	$(C_2 \times D_{12}) \times_\rho C_2$
[96, 116]	$(C_3 \times (C_8 \times_\rho C_2)) \times_\rho C_2$
[96, 117]	$D_8 \times S_3$
[96, 118]	$(D_4 \times S_3) \times_\rho C_2$
[96, 119]	$(C_8 \times S_3) \times_\rho C_2$
[96, 120]	$\mathrm{QD}_8 \times S_3$
[96, 121]	$(D_4 \times S_3) \times_\rho C_2$
[96, 122]	$(Q_8 \times S_3) \times_\rho C_2$
[96, 123]	$(C_8 \times S_3) \times_\rho C_2$
[96, 124]	$Q_{16} \times S_3$
[96, 125]	$(C_3 \times Q_{16}) \times_\rho C_2$
[96, 126]	$(C_8 \times S_3) \times_\rho C_2$
[96, 127]	$C_2 \times C_2 \times (C_3 \times_\rho C_8)$
[96, 128]	$C_2 \times ((C_3 \times_\rho C_8) \times_\rho C_2)$
[96, 129]	$C_2 \times C_4 \times (C_3 \times_\rho C_4)$
[96, 130]	$C_2 \times ((C_3 \times_\rho C_4) \times_\rho C_4)$
[96, 131]	$(C_2 \times (C_3 \times_\rho Q_8)) \times_\rho C_2$
[96, 132]	$C_2 \times (C_{12} \times_\rho C_4)$
[96, 133]	$(C_4 \times (C_3 \times_\rho C_4)) \times_\rho C_2$
[96, 134]	$C_2 \times ((C_{12} \times C_2) \times_\rho C_2)$
[96, 135]	$C_4 \times ((C_6 \times C_2) \times_\rho C_2)$
[96, 136]	$(C_{12} \times C_2 \times C_2) \times_\rho C_2$
[96, 137]	$(C_{12} \times C_2 \times C_2) \times_\rho C_2$
[96, 138]	$C_2 \times ((C_3 \times D_4) \times_\rho C_2)$
[96, 139]	$(C_6 \times D_4) \times_\rho C_2$
[96, 140]	$C_2 \times ((C_3 \times_\rho C_8) \times_\rho C_2)$
[96, 141]	$D_4 \times (C_3 \times_\rho C_4)$
[96, 142]	$(C_2 \times C_2 \times (C_3 \times_\rho C_4)) \times_\rho C_2$
[96, 143]	$(C_2 \times (C_3 \times_\rho Q_8)) \times_\rho C_2$
[96, 144]	$(C_2 \times C_2 \times C_2 \times S_3) \times_\rho C_2$
[96, 145]	$(C_6 \times D_4) \times_\rho C_2$
[96, 146]	$(C_2 \times C_2 \times (C_3 \times_\rho C_4)) \times_\rho C_2$
[96, 147]	$(C_6 \times D_4) \times_\rho C_2$
[96, 148]	$C_2 \times ((C_3 \times Q_8) \times_\rho C_2)$
[96, 149]	$(C_6 \times Q_8) \times_\rho C_2$
[96, 150]	$C_2 \times (C_3 \times_\rho Q_{16})$
[96, 151]	$(C_3 \times_\rho C_4) \times_\rho Q_8$
[96, 152]	$Q_8 \times (C_3 \times_\rho C_4)$
[96, 153]	$(C_6 \times Q_8) \times_\rho C_2$
[96, 154]	$(C_6 \times Q_8) \times_\rho C_2$
[96, 155]	$(C_2 \times (C_3 \times_\rho C_8)) \times_\rho C_2$
[96, 156]	$(C_2 \times D_{12}) \times_\rho C_2$
[96, 157]	$(C_2 \times (C_3 \times_\rho C_8)) \times_\rho C_2$
[96, 158]	$(C_2 \times (C_3 \times_\rho Q_8)) \times_\rho C_2$
[96, 159]	$C_2 \times ((C_2 \times (C_3 \times_\rho C_4)) \times_\rho C_2)$
[96, 160]	$(C_6 \times C_2 \times C_2 \times C_2) \times_\rho C_2$

Continúa en la página siguiente...

GAPID	Grupo
[96, 161]	$C_{12} \times C_4 \times C_2$
[96, 162]	$C_6 \times ((C_4 \times C_2) \times_\rho C_2)$
[96, 163]	$C_6 \times (C_4 \times_\rho C_4)$
[96, 164]	$C_3 \times ((C_4 \times C_4) \times_\rho C_2)$
[96, 165]	$C_{12} \times D_4$
[96, 166]	$C_{12} \times Q_8$
[96, 167]	$C_3 \times ((C_2 \times C_2 \times C_2 \times C_2) \times_\rho C_2)$
[96, 168]	$C_3 \times ((C_4 \times C_2 \times C_2) \times_\rho C_2)$
[96, 169]	$C_3 \times ((C_2 \times Q_8) \times_\rho C_2)$
[96, 170]	$C_3 \times ((C_4 \times C_2 \times C_2) \times_\rho C_2)$
[96, 171]	$C_3 \times ((C_4 \times C_4) \times_\rho C_2)$
[96, 172]	$C_3 \times ((C_2 \times C_2) \to G \to (C_2 \times C_2 \times C_2))$
[96, 173]	$C_3 \times ((C_4 \times C_4) \times_\rho C_2)$
[96, 174]	$C_3 \times ((C_4 \times C_4) \times_\rho C_2)$
[96, 175]	$C_3 \times (C_4 \times_\rho Q_8)$
[96, 176]	$C_{24} \times C_2 \times C_2$
[96, 177]	$C_6 \times (C_8 \times_\rho C_2)$
[96, 178]	$C_3 \times ((C_8 \times C_2) \times_\rho C_2)$
[96, 179]	$C_6 \times D_8$
[96, 180]	$C_6 \times \mathrm{QD}_8$
[96, 181]	$C_6 \times Q_{16}$
[96, 182]	$C_3 \times ((C_8 \times C_2) \times_\rho C_2)$
[96, 183]	$C_3 \times ((C_2 \times D_4) \times_\rho C_2)$
[96, 184]	$C_3 \times ((C_2 \times Q_8) \times_\rho C_2)$
[96, 185]	$A_4 \times_\rho Q_8$
[96, 186]	$C_4 \times S_4$
[96, 187]	$(C_2 \times S_4) \times_\rho C_2$
[96, 188]	$\mathrm{SL}(2,3) \to G \to C_2)$
[96, 189]	$C_2 \times \mathrm{GL}(2,3)$
[96, 190]	$(C_2 \times \mathrm{SL}(2,3)) \times_\rho C_2$
[96, 191]	$\mathrm{SL}(2,3) \to G \to C_2) \times_\rho C_2$
[96, 192]	$\mathrm{SL}(2,3) \to G \to C_2) \times_\rho C_2$
[96, 193]	$(\mathrm{SL}(2,3) \times_\rho C_2) \times_\rho C_2$
[96, 194]	$C_2 \times (A_4 \times_\rho C_4)$
[96, 195]	$(C_2 \times C_2 \times A_4) \times_\rho C_2$
[96, 196]	$C_2 \times C_4 \times A_4$
[96, 197]	$D_4 \times A_4$
[96, 198]	$C_2 \times C_2 \times \mathrm{SL}(2,3)$
[96, 199]	$Q_8 \times A_4$
[96, 200]	$C_2 \times (\mathrm{SL}(2,3) \times_\rho C_2)$
[96, 201]	$(\mathrm{SL}(2,3) \times_\rho C_2) \times_\rho C_2$
[96, 202]	$(C_2 \times \mathrm{SL}(2,3)) \times_\rho C_2$
[96, 203]	$(C_2 \times C_2 \times Q_8) \times_\rho C_3$
[96, 204]	$((C_2 \times D_4) \times_\rho C_2) \times_\rho C_3$
[96, 205]	$C_2 \times C_2 \times (C_3 \times_\rho Q_8)$
[96, 206]	$C_2 \times C_2 \times C_4 \times S_3$
[96, 207]	$C_2 \times C_2 \times D_{12}$
[96, 208]	$C_2 \times ((C_{12} \times C_2) \times_\rho C_2)$
[96, 209]	$C_2 \times D_4 \times S_3$
[96, 210]	$C_2 \times ((C_2 \times (C_3 \times_\rho C_4)) \times_\rho C_2)$
[96, 211]	$(C_6 \times D_4) \times_\rho C_2$
[96, 212]	$C_2 \times Q_8 \times S_3$
[96, 213]	$C_2 \times ((C_4 \times S_3) \times_\rho C_2)$
[96, 214]	$(C_6 \times Q_8) \times_\rho C_2$
[96, 215]	$((C_4 \times C_2) \times_\rho C_2) \times S_3$

Continúa en la página siguiente...

GAPID	Grupo
[96, 216]	$(D_4 \times S_3) \times_\rho C_2$
[96, 217]	$(Q_8 \times S_3) \times_\rho C_2$
[96, 218]	$C_2 \times C_2 \times C_2 \times (C_3 \times_\rho C_4)$
[96, 219]	$C_2 \times C_2 \times ((C_6 \times C_2) \times_\rho C_2)$
[96, 220]	$C_{12} \times C_2 \times C_2 \times C_2$
[96, 221]	$C_2 \times C_6 \times D_4$
[96, 222]	$C_2 \times C_6 \times Q_8$
[96, 223]	$C_6 \times ((C_4 \times C_2) \times_\rho C_2)$
[96, 224]	$C_3 \times ((C_2 \times D_4) \times_\rho C_2)$
[96, 225]	$C_3 \times ((C_2 \times Q_8) \times_\rho C_2)$
[96, 226]	$C_2 \times C_2 \times S_4$
[96, 227]	$((C_2 \times C_2 \times C_2 \times C_2) \times_\rho C_3) \times_\rho C_2$
[96, 228]	$C_2 \times C_2 \times C_2 \times A_4$
[96, 229]	$C_2 \times ((C_2 \times C_2 \times C_2 \times C_2) \times_\rho C_3)$
[96, 230]	$C_2 \times C_2 \times C_2 \times C_2 \times S_3$
[96, 231]	$C_6 \times C_2 \times C_2 \times C_2 \times C_2$
[97, 1]	C_{97}
[98, 1]	D_{49}
[98, 2]	C_{98}
[98, 3]	$C_7 \times D_7$
[98, 4]	$(C_7 \times C_7) \times_\rho C_2$
[98, 5]	$C_{14} \times C_7$
[99, 1]	C_{99}
[99, 2]	$C_{33} \times C_3$
[100, 1]	$C_{25} \times_\rho C_4$
[100, 2]	C_{100}
[100, 3]	$C_{25} \times_\rho C_4$
[100, 4]	D_{50}
[100, 5]	$C_{50} \times C_2$
[100, 6]	$C_5 \times (C_5 \times_\rho C_4)$
[100, 7]	$(C_5 \times C_5) \times_\rho C_4$
[100, 8]	$C_{20} \times C_5$
[100, 9]	$C_5 \times (C_5 \times_\rho C_4)$
[100, 10]	$(C_5 \times C_5) \times_\rho C_4$
[100, 11]	$(C_5 \times C_5) \times_\rho C_4$
[100, 12]	$(C_5 \times C_5) \times_\rho C_4$
[100, 13]	$D_5 \times D_5$
[100, 14]	$C_{10} \times D_5$
[100, 15]	$C_2 \times ((C_5 \times C_5) \times_\rho C_2)$
[100, 16]	$C_{10} \times C_{10}$

Apéndice B

Tópicos en Teoría de Grupos Finitos

En este apéndice se resumen algunas de las definiciones más importantes y teoremas de la teoría de grupos finitos que son necesarios para interpretar la A.1, este apartado está para ser un recurso bibliográfico inmediato sin tener que recurrir a toda la teoría expuesta en los capítulos de este ejemplar. Para leer este apéndice se hacen necesarios conocimientos básicos de Teoría de Grupos, puede encontrarse una exposición básica de esta teoría en los dos primeros capítulos.

Producto directo

Dado dos grupos A, B definimos su *producto directo* $A \times B$ como el conjunto de todos los pares (a, b) con $a \in A$ y $b \in B$, donde la operación del grupo se define por la multiplicación de elementos en cada coordenada:

$$(a_1, b_1) \cdot (a_2, b_2) \equiv (a_1 \cdot a_2, b_1 \cdot b_2) \tag{B.1}$$

Recíprocamente, cuando tenemos un grupo G, podemos preguntarnos cuando puede ser escrito como producto directo de dos subgrupos, digamos A y B. De la definición anterior, está claro que deben cumplirse dos condiciones: En primer lugar, cada elemento $g \in G$ debe ser expresable como un producto $g = a \cdot b$ con $a \in A$ y $b \in B$. Si A y B no tienen elementos en común distintos del elemento identidad de G, es claro que utilizando las condiciones y propiedades de grupo, esta descomposición es única, esto es, tenemos una correspondencia uno a uno $a \cdot b \leftrightarrow (a, b)$. Segundo, todos los elementos de A deben conmutar con los elementos de B para que pueda obtener parecido con el producto B.1:

$$g_1 \cdot g_2 = (a_1 \cdot b_1) \cdot (a_2 \cdot b_2) = a_1 \cdot b_1 \cdot a_2 \cdot b_2 = a_1 \cdot a_2 \cdot b_1 \cdot b_2 = (a_1 \cdot a_2) \cdot (b_1 \cdot b_2) \tag{B.2}$$

Con la identificación $a \cdot b \leftrightarrow (a, b)$, lo anterior lo interpretamos:

$$g_1 \cdot g_2 = (a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2) \tag{B.3}$$

Hay una correspondecia uno a uno $a \cdot b \leftrightarrow (a, b)$ entre los elementos G y $A \times B$ que es compatible con la operación del grupo, es decir, los dos grupos son *isomorfos*. Para propósitos prácticos, diremos que estos dos grupos son iguales y escribiremos $G = A \times B$.

Subgrupos normales

Un subgrupo $N \subset G$ es llamado *normal*, si para cualquier $n \in N$ se tiene que $gng^{-1} \in N$ para todo $g \in G$, esto es la conjugación bajo cualquier elemento de G de N se queda en N. Se escribe

$N \lhd G$. Este concepto es importante en el contexto en que nos encontramos, porque ambos A y B son subgrupos normales de $G = A \times B$:

$$ga'g^{-1} = (ab)a'(ab)^{-1} = aba'b^{-1}a^{-1} = abb^{-1}a'a^{-1} = aa'a^{-1} \in A \tag{B.4}$$

La demostración para B es análoga. Si N es normal en G, las clases laterales de G con respecto a N de un grupo, llamado el grupo cociente y se denota por G/N. Dividir por N quiere decir diferenciar todos los elementos diferentes bajo la multiplicación por $n \in N$, esto es, $g_1 \sim g_2$, si y sólo si $g_1 = ng_2$. En este sentido es claro que $(A \times B)/B$ es el conjunto de todos loes elemenos de la forma $(a, \mathbf{1})$, que es isomorfo a A, porque $(a, \mathbf{1}) \sim a \cdot \mathbf{1} = a$. Un argumento análogo cuenta para B.

Producto semidirectos

El producto semidirecto es una generalización natural del producto directo para el caso de que A y B no conmutan. Repitamos el cálculo de B.2:

$$g_1 \cdot g_2 = (a_1 \cdot b_1) \cdot (a_2 \cdot b_2) = a_1 \cdot b_1 \cdot a_2 \cdot b_2 = a_1 \cdot a_2 \cdot a_2^{-1} \cdot b_1 \cdot a_2 \cdot b_2 = a_1 \cdot a_2 \cdot (a_2^{-1} \cdot b_1 \cdot a_2) \cdot b_2 \tag{B.5}$$

Primero, si queremos tener alguna posibilidad de escribir $g_1 \cdot g_2$ como producto $\tilde{a} \cdot \tilde{b}$ con $\tilde{a} \in A$ y $\tilde{b} \in B$, debemos asumir que $a_2^{-1} \cdot b_1 \cdot a_2 \in B$. La relación anterior debe ser para todo $a_2 \in A$ (y además se satisface para $b \in B$), esto es equivalente a necesitar que B sea un subgrupo normal. Segundo, necesitamos conocer la acción de A en B por medio de la conjutación que denotaremos por ρ_a:

$$\rho_a : B \to B, \qquad \rho_a(b) = a^{-1} \cdot b \cdot a \tag{B.6}$$

Note que $\rho_a : b \mapsto a^{-1} \cdot b \cdot a$ es un automorfismo de B, y $\rho : a \mapsto \rho_a$ es un homomorfismo de A en $\mathrm{Aut}(B)$, el grupo de automormisfos de B.

$$g_1 \cdot g_2 = (a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2,\ \rho_{a_2}(b_1) \cdot b_2), \tag{B.7}$$

en analogía a B.1, y la única diferencia es que la regla de la multiplicación queda ligeramente modificada. Si A y B son dos subgrupos de G, y la regla de multiplicación entre elementos de A y B es conocida, y si es posible calcular manualmente el segundo término en B.6. Sin embargo, tenemos dos subgrupos A y Bque no guardan relación uno con el otro, debemos *escoger* ρ_a del conjunto de todos los automorfismos de B, y esto *sirve como la definición* de conjugación. En este sentido, el producto semidirecto no es único, pues depende de la elección de ρ.

En resumen, el *producto semidirecto* de A y B con respecto a ρ es el conjunto de todos los pares (a, b) con $a \in A$ y $b \in B$, donde la operación del grupo se define por B.7 y $\rho : a \mapsto \rho_a$ es un homomorfismo de A en $\mathrm{Aut}(B)$. Usaremos la notación $G \equiv B \rtimes_\rho A$ para el producto semidirecto. Entonces,

- $B \lhd G$, esto es B es un subgrupo normal de G,
- A actúa en B por conjugación, y
- el grupo cociente G/B es isomorfo a A. Es importante destacar que el orden de los factores es relevante.

El producto semidirecto no es único, sino que depende de la elección de ρ. Si ρ_a es el homomorfismo identidad para todo a, el producto semidirecto se reduce al producto directo.

Sucesiones exactas cortas

La forma más general para describir un grupo es por medio de sucesiones exactas cortas, como se amplía acontinuación. Una *sucesión exacta* es una colección de homomorfismos de grupos

$$G_1 \xrightarrow{\rho_1} G_2 \xrightarrow{\rho_2} G_3 \xrightarrow{\rho_3} \cdots \xrightarrow{\rho_{n-1}} G_n \tag{B.8}$$

tales que la imagen de cada homomorfismo es igual al kernel de la la siguiente, esto es $\mathrm{Im}(\rho_k) = \mathrm{Ker}(\rho_{k+1})$. Una *sucesión exacta corta* es una sucesión exacta de la forma

$$\mathbf{1} \xrightarrow{\rho_0} G_1 \xrightarrow{\rho_1} G_2 \xrightarrow{\rho_2} G_3 \xrightarrow{\rho_3} \mathbf{1}, \tag{B.9}$$

donde $\mathbf{1}$ denota el grupo trivial. Un homomorfismo de grupo siempre mapea el elemento identidad en el elemento identidad, entonces $\mathrm{Im}(\rho_0) = \mathbf{1}$. Porque la sucesión es exacta, tenemos $\mathrm{Ker}(\rho_1) = \mathrm{Im}(\rho_0) = \mathbf{1}$, esto es ρ_1 es inyectivo, desde ρ_3 mapea a todo G_3 en $\mathbf{1}$, su kernel es G_3, y por el mismo argumento concluimos que $\mathrm{Im}(\rho_2) = \mathrm{Ker}(\rho_3) = G_3$, esto es ρ_2 es sobreyectivo.

Los teoremas de isomorfismos se satisfacen para cualquier homomorfismo $\rho : A \to B$,

$$\mathrm{Im}(\rho) = A/\mathrm{Ker}(\rho). \tag{B.10}$$

Es fácil ver porque esto se satisface: ρ es inyectivo, además $\mathrm{Im}(\rho) \subset B$, y $\rho : A \to \mathrm{Im}(\rho)$ es sobreyectivo. El kernel $\mathrm{Ker}(\rho) \subset A$ es en general no trivial, por lo que ρ no es inyectiva. Dividiendo A por el kernel (que es siempre un subconjunto normal) identificamos todos los elementos en $\mathrm{Ker}(\rho)$ con $\mathbf{1}$, entonces $\rho : A/\mathrm{Ker}(\rho) \to \mathrm{Im}(\rho)$ es inyectivo. Esto concluye una justificación para la B.10.

Aplicando este resultado en nuestro caso, obtenemos:

$$\mathrm{Im}(\rho_2) = G_2/\mathrm{Ker}(\rho_2) \quad \leftrightarrow \quad G_3 = G_2/\mathrm{Im}(\rho_1) \quad \leftrightarrow \quad G_3 = G_2/G_1. \tag{B.11}$$

Para la última equivalencia se ha utilizado el hecho de que ρ_1 es inyectivo, y por lo tanto establece un isomorfismo entre G_1 y $\mathrm{Im}(\rho_1)$. De nuevo, el kernel de un homomorfismo siempre es normal, $G_1 \simeq \mathrm{Im}(\rho_1) = \mathrm{Ker}(\rho_2)$ es un subgrupo normal de G_2.

Escribimos B.11 usando la siguiente notación:

$$\mathbf{1} \to N \xrightarrow{\rho} G \xrightarrow{\psi} Q \to \mathbf{1} \qquad \Rightarrow \qquad N \lhd G \quad \text{y} \quad Q = G/N \tag{B.12}$$

La ecuación B.12 da una descripción de G en términos de un subgrupo normal N y el grupo cociente G/N y decimos que G es una extensión de Q por N.

Conclusiones y Recomendaciones

En base a la teoría expuesta en la investigación desarrollada, puede concluirse que:

- Se lograron los objetivos planteados al inicio: Definir los elementos básicos de la teoría de grupos finitos, enunciar y demostrar detalladamente las demostraciones de los principales teoremas y clasificar los grupos finitos de orden menor que cien en forma teórica o computacional.
- Exponer la ventaja de contar con recursos computacionales que permiten trabajar con estructuras algebraicas abstractas, el uso y aplicaciones del programa GAP a la solución de problemas, mediantes cálculos directos o ejecución de algoritmos.
- Haber elaborado un recurso bibliográfico de apoyo y consulta disponible a todos los estudiantes al cual puedan recurrir y extraer información que consideren pertinente según sus necesidades académicas.

En esta obra se expuso la aplicación principal de los teoremas de Sylow: demostrar que para un grupo dado 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 más fino.

Se ha estudiado y clasificado de forma teórica la cantidad de grupos finitos distintos (salvo isomorfismo), que tienen como orden un número primo, o bien el producto de dos números primos iguales o distintos. Para esto se utilizaron métodos elementales basados en la acción de los automorfismos internos sobre el propio grupo. Con esta finalidad se hizo que el grupo G actuara sobre sí mismo mediante los automorfismos internos, y posteriormentente estudiando las órbitas de conjugación de cada elemento.

También se hacen las siguientes recomendaciones y consideraciones:

- Se recomienda al lector interesado en esta investigación comprender cada uno de los resultados y técnicas expuestas, pues éstas mismas pueden aplicarse a los grupos no estudiados en esta obra, con un poco de dedicación al respecto, es posible extender y aplicar la teoría desarrollada.
- Seguir estudiando esta línea de trabajo y dar continuidad a esta investigación: por ejemplo extender el estudio hecho a otros casos de ordenes de grupo o bien interesarse en exponer de forma explícita la regla de asignación de los homomorfismos de definición del producto semidirecto.

Bibliografía

[1] R. Bourgne and J.-P Azra. *Ecrits et Mémoires Mathématiques d'Évariste Galois*. Gauthier-Villars, Paris, France, 1962.

[2] H. Wussing. *The Genesis of the Abstract Group Concept*. The MIT Press Cambridge, Massachusetts, London England, first edition, 1984.

[3] G. Mazzola. *The Topos of Music. Birkhäuser*, Germany, first edition, 2002.

[4] Alperin, J. L., *Centralizers of abelian normal subgroups of p-groups*, Jour. Alg., 1 (1964), 110-113.

[5] Bender, H., *A group theoretic proof of Burnside' s p^aq^b- theorem*, Math. Z.126 (1972), 327-338.

[6] Burnside, W., *Theory of Groups of Finite Order*, 2nd edition, Dover, New York, 1955.

[7] Robinson, Derek J. S., *A Course in the Theory of Groups*, Springer, New York, 1995.

[8] Fraleigh, J. B., *Álgebra Abstracta*, Addison-Wesley Iberoamericana, 1987.

[9] Gorenstein, D. *Finite Groups*, Chelsea, New York, 1980.

[10] Jacobson, N. *Basic Algebra*, 2nd edition. Freeman and Company, New York, 1985.

[11] Kerber, A. *Aplied Finite Group Actions*, 2nd edition, Springer 1999.

[12] Kurosh, A., *Group Theory*, Chelsea, New York, 1979.

[13] Joseph Gallian, Contemporary abstract algebra, 5 ed., Houghton Mifflin, 2002