Teoría de Grupos, un primer curso

Emilio Lluis-Puebla
Universidad Nacional Autónoma de México

Publicaciones Electrónicas
Sociedad Matemática Mexicana

Índice General

.

Prefacio

El éxito de la Teoría de Grupos es impresionante y extraordinario. Es quizás, la rama más poderosa e influyente de toda la Matemática. Influye en casi todas las disciplinas científicas, artísticas y en la propia Matemática de una manera fundamental. Lo que realmente se ha hecho en la Teoría de Grupos, es extraer lo esencial de diversas situaciones donde ocurre. Dado un conjunto no vacío, definimos una operación binaria en él, tal que cumpla ciertas axiomas, es decir, que posea una estructura, (la estructura de grupo). El concepto de estructura y los relacionados con éste, como el de isomorfismo, juegan un papel decisivo en la Matemática actual.

La teoría general de las estructuras es una herramienta muy poderosa. Siempre que alguien pruebe que sus objetos de estudio satisfacen los axiomas de cierta estructura, obtiene, de inmediato para sus objetos, todos los resultados válidos para esa teoría. Ya no tiene que comprobar cada uno de ellos particularmente. Actualmente, podría decirse que las estructuras permiten clasificar las diversas ramas de la Matemática.

Este texto contiene el trabajo escrito a lo largo de varios años del material correspondiente a mi curso sobre la materia que he impartido en la Facultad de Ciencias de la Universidad Nacional Autónoma de México. Después de haber ofrecido el curso con excelentes textos, algunos citados en la Bibliografía, decidí escribir uno que siga el enfoque de mis propios libros [Ll1] y [Ll2]. Es decir, escogí una presentación moderna donde introduzco el lenguaje de diagramas conmutativos y propiedades universales, tan requerido en la matemática actual así como en la Física y en la Ciencia de la Computación, entre otras disciplinas.

El texto consta de tres capítulos con cuatro secciones cada uno. Cada sección contiene una serie de problemas que se resuelven con creatividad utilizando el material expuesto, mismos que constituyen una parte fundamental del texto. Tienen también como finalidad, la de permitirle al estudiante redactar matemática. El libro está diseñado para un primer curso sobre la Teoría de Grupos el cual se cubre en su totalidad en cuarenta horas de clase.

Deseo agradecer a mis alumnos, a los árbitros revisores y muy en especial a mi estimado colega, el Dr. Juan Morales Rodríguez el haber hecho oportunas y acertadas sugerencias para mejorar este texto. Cualquier falta u omisión que aún permanezca es de mi exclusiva responsabilidad.

Finalmente, comento que he decidido incluir este texto dentro de las Publicaciones Electrónicas de la Sociedad Matemática Mexicana con el ánimo de predicar con el ejemplo y mostrar (como matemático y Editor Ejecutivo) la confianza en este tipo de publicación.

Ciudad Universitaria.
Abril de 2006.
.

Introducción

La Matemática existe desde que existe el ser humano. Prácticamente todo ser humano es un matemático en algún sentido. Desde los que utilizan la Matemática hasta los que la crean. También todos son hasta cierto punto filósofos de la Matemática. Efectivamente, todos los que miden, reconocen personas o cosas, cuentan o dicen que “tan claro como que dos y dos son cuatro” son matemáticos o filósofos de la Matemática. Sin embargo, hay un número muy reducido de personas que se dedican a crear, enseñar, cultivar o divulgar la Matemática.

La Matemática es pilar y cimiento de nuestra civilización. Desde la primera mitad del siglo XIX, debido al progreso en diversas ramas se le dio unidad a la Ciencia Matemática y justificaron el nombre en singular. Según me comentó mi querido amigo, Arrigo Coen, Mathema significa erudición, manthánein el infinitivo de aprender, el radical mendh significa en pasivo, ciencia, saber. Luego, es lo relativo al aprendizaje. Así que en sentido implícito, Matemática significa: “lo digno de ser aprendido”. También se dice que Matemática significa “ciencia por excelencia”.

Sin embargo, de muy pocas personas podría decirse que poseen información correcta y actualizada sobre alguna de sus ramas o subramas. Los niños y jóvenes de nuestros días pueden poseer una imagen bastante aproximada de electrones, galaxias, agujeros negros, código genético, etc. Sin embargo, difícilmente encontrarán durante sus estudios, conceptos matemáticos creados más allá de la primera mitad del siglo XIX. Esto es debido a la naturaleza de los conceptos de la Matemática.

Es muy común la creencia de que un matemático es una persona que se dedica a realizar enormes sumas de números naturales durante todos los días de su vida. También, la gente supone que un matemático sabe sumar y multiplicar los números naturales muy rápidamente. Si pensamos un poco acerca de este concepto que la mayoría tiene acerca de los matemáticos, podríamos concluir que no se requieren matemáticos ya que una calculadora de bolsillo realiza este trabajo.

También, cuando uno pregunta ¿cuál es la diferencia entre un matemático y un contador? la consideran una pregunta equivalente a ¿cuál es la diferencia entre x y x? Es decir, suponen que hacen lo mismo. Si uno dice que un matemático rara vez tiene que realizar sumas o multiplicaciones, les resulta increíble. También les resulta increíble el que los libros de Matemática rara vez utilizan números mayores que 10, exceptuando quizás los números de las páginas.

Durante muchos años, a los niños se les ha hecho énfasis en el aprendizaje de las tablas de multiplicar, en el cálculo de enormes sumas, restas, multiplicaciones, divisiones y raíces cuadradas a lápiz pero de números muy pequeños (para los números grandes, la mayoría de las personas tiene poca idea de su magnitud). Después, cuando jóvenes, aquellos que sumaban y multiplicaban polinomios eran considerados por sus compañeros como genios poseedores de un gran talento matemático y posteriormente a éstos, si tenían suerte, se les enseñaba a sumar y multiplicar números complejos.

Pareciera ser, entonces, que el matemático es aquel ser que se pasa la vida haciendo sumas y multiplicaciones (de números pequeños), algo así como un encargado de la caja de un negocio. Esta impresión subsiste en una gran mayoría de las personas. Nada más lejos de esto. Los matemáticos no son los que calculan o hacen cuentas sino los que inventan cómo calcular o hacer cuentas. Hacer Matemática es imaginar, crear, razonar.

Para contar fue necesario representar los números de alguna forma, por ejemplo, los dedos de la mano. Después, el ábaco constituyó un paso todavía ligado a contar con los dedos, el cual todavía se utiliza en algunas partes del planeta. Posteriormente la máquina aritmética de Pascal inventada en 1642 permitía efectuar sumas y restas mediante un sistema muy ingenioso de engranes. En la actualidad, las calculadoras de bolsillo permiten realizar, en segundos, cálculos que antes podrían haber llevado años enteros y también le permitieron a uno deshacerse de las famosas tablas de logaritmos y de la regla de cálculo.

Sin embargo, en general, los alumnos de cualquier carrera y los egresados de ellas a los cuales se les pregunta, -¿qué es la suma? o mejor dicho, ¿qué es la adición?- simplemente encogen los hombros, a pesar de que han pasado más de doce años sumando y de que la suma es un concepto muy primitivo. También suele suceder que cuando un niño o un joven o un adulto profesionista se enfrenta a un problema, no sabe si debe sumar, restar, multiplicar o llorar.

El concepto de operación binaria o ley de composición es uno de los más antiguos de la Matemática y se remonta a los antiguos egipcios y babilonios quienes ya poseían métodos para calcular sumas y multiplicaciones de números naturales positivos y de números racionales positivos (téngase en cuenta que no poseían el sistema de numeración que nosotros usamos). Sin embargo, al paso del tiempo, los matemáticos se dieron cuenta que lo importante no eran las tablas de sumar o multiplicar de ciertos "números" sino el conjunto y su operación binaria definida en él. Esto, junto con ciertas propiedades que satisfacían dieron lugar al concepto fundamental llamado grupo.

Históricamente, el concepto de operación binaria o ley de composición fue extendido de dos maneras donde solamente se tiene una resemblanza con los casos numéricos de los babilonios y los egipcios. La primera fue por Gauss, al estudiar formas cuadráticas con coeficientes enteros, donde vio que la ley de composición era compatible con ciertas clases de equivalencia. La segunda culminó con el concepto de grupo en la Teoría de Sustituciones, (mediante el desarrollo de las ideas de Lagrange, Vandermonde y Gauss en la solución de ecuaciones algebraicas). Sin embargo, éstas ideas permanecieron superficiales, siendo Galois el verdadero iniciador de la Teoría de Grupos al reducir el estudio de las ecuaciones algebraicas al de grupos de permutaciones asociados a ellas.

Fueron los matemáticos ingleses de la primera mitad del siglo XIX los que aislaron el concepto de ley de composición y ampliaron el campo del Álgebra aplicándola a la Lógica (Boole), a vectores y cuaternios (Hamilton), y a matrices (Cayley). Para finales del siglo XIX, el Álgebra se orientó al estudio de las estructuras algebraicas dejando atrás el interés por las aplicaciones de las soluciones de ecuaciones numéricas. Ésta orientación dio lugar a tres principales corrientes:

(i) la Teoría de Números que surgió de los matemáticos alemanes Dirichlet, Kummer, Kronecker, Dedekind y Hilbert, basados en los estudios de Gauss. El concepto de campo fue fundamental.

(ii) la creación del Álgebra Lineal en Inglaterra por Sylvester, Clifford; en Estados Unidos por Pierce, Dickson, Wedderburn; y en Alemania y Francia por Weirstrass, Dedekind, Frobenius, Molien, Laguerre, Cartan.

(iii) la Teoría de Grupos que al principio se concentró en el estudio de grupos de permutaciones. Fue Jordan quien desarrolló en gran forma el trabajo de Galois, Serret y otros de sus predecesores. Él introdujo el concepto de homomorfismo y fue el primero en estudiar grupos infinitos. Más tarde, Lie, Klein y Poincaré desarrollaron este estudio considerablemente. Finalmente se hizo patente que la idea fundamental y esencial de grupo era su ley de composición u operación binaria y no la naturaleza de sus objetos.

El éxito de la Teoría de Grupos es impresionante y extraordinario. Basta nombrar su influencia en casi toda la Matemática y otras disciplinas del conocimiento. Los ejemplos escritos en 1.1 podrían dejar perplejo al no ilustrado en matemática con un pensamiento acerca de los pasatiempos que los matemáticos inventan combinando "números" de una manera perversa. Sin embargo ahí hemos considerado ejemplos vitales para la Teoría de los Números (se podría reemplazar el número 3 por cualquier número natural n (si $n = 12$ obtenemos los números de los relojes) o por un número primo p obteniendo conceptos y resultados importantes) y para la propia Teoría de Grupos (grupo diédrico y simétrico). Al observar esto, lo que realmente se ha hecho en la Teoría de Grupos, es extraer lo esencial de ellos, a saber, dado un conjunto no vacío, definimos una operación binaria en él, tal que cumpla ciertas axiomas, postulados o propiedades, es decir, que posea una estructura, (la estructura de grupo). Existen varios conceptos ligados al de estructura, uno de los más importantes es el de isomorfismo.

El concepto de estructura y de los relacionados con éste, como el de isomorfismo, juegan un papel decisivo en la Matemática actual. Las teorías generales de las estructuras importantes son herramientas muy poderosas. Siempre que alguien pruebe que sus objetos de estudio satisfacen los axiomas de cierta estructura, obtiene, de inmediato, todos los resultados válidos para esa teoría en sus objetos. Ya no tiene que comprobar cada uno de ellos particularmente. Un uso actual en la Matemática, de las estructuras y los isomorfismos, es el de clasificar las diversas ramas de ella (no es importante la naturaleza de los objetos pero sí lo es el de sus relaciones).

En la Edad Media la clasificación en ramas de la Matemática estaba dada por la de Aritmética, Música, Geometría y Astronomía las que constituyeron el Cuadrivium. Después y hasta la mitad del siglo XIX, las ramas de la Matemática se distinguían por los objetos que estudiaban, por ejemplo, Aritmética, Álgebra, Geometría Analítica, Análisis, todas con algunas subdivisiones. Algo así como si dijéramos que puesto que los murciélagos y las águilas vuelan entonces pertenecen a las aves. Lo que se nos presenta ahora es el ver más allá y extraer de las apariencias las estructuras subyacentes. Actualmente existen 63 ramas de la Matemática con más de 5000 subclasificaciones. Entre ellas se encuentran la Topología Algebraica (estructuras mixtas), el Álgebra Homológica (la purificación de la interacción entre el Álgebra y la Topología, creada en los años cincuenta del siglo pasado), y la K-Teoría Algebraica (una de las más recientes ramas, creada en los años setenta del siglo pasado).

Algunos piensan que la Matemática es un juego simple que sola y fríamente interesa al intelecto. Esto sería el olvidar, asienta Poincaré, la sensación de la belleza matemática, de la armonía de los números y las formas, así como de la elegancia geométrica. Esta es ciertamente una sensación de placer estético que todo verdadero matemático ha sentido y por supuesto que pertenece al campo de la emoción sensible. La belleza y la elegancia matemática consisten de todos los elementos dispuestos armónicamente tales que nuestra mente pueda abarcarlos totalmente sin esfuerzo y a la vez mantener sus detalles.

Esta armonía, continúa Poincaré, es, de inmediato, una satisfacción de nuestras necesidades estéticas y una ayuda para la mente que sostiene y guía. Y al mismo tiempo, al poner bajo nuestra visión un todo bien ordenado, nos hace entrever una ley o verdad matemática. Esta es la sensibilidad estética que juega un papel de filtro delicado, la cual explica suficientemente el porqué el que carece de ella nunca será un verdadero creador, concluye Poincaré.

Para el autor de este texto, la Matemática es una de las Bellas Artes, la más pura de ellas, que tiene el don de ser la más precisa y la precisión de las Ciencias.

.

Capítulo I

I.1 Operaciones Binarias

En esta sección presentaremos uno de los conceptos más antiguos de la Matemática, la operación binaria o ley de composición. También veremos qué tan ciertos son unos "dichos populares" como son los de "tan claro como que dos y dos son cuatro" y "el orden de los factores no altera el producto".

Recordemos algunos conceptos elementales.

Primero, recuerde el conjunto de los números enteros

$$\mathbb{Z} = \{... - 5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, ...\}$$

Segundo, pregúntese: -¿cómo se relacionan dos conjuntos “adecuadamente”? Sean A y B dos conjuntos cualesquiera. Diremos que $f : A \to B$ es una **función** de A en B si a cada elemento de A le asociamos un elemento único de B.

Por ejemplo, si $A = \{a, b, c\}$ y $B = \{p, q, r, s\}$ entonces $f : A \to B$ dada por la siguiente asociación

$$\begin{array}{ccc} a & \longmapsto & p \\ b & \longmapsto & q \\ c & \longmapsto & r \end{array}$$

es una función, mientras que la asociación

$$\begin{array}{ccc} a & \longmapsto & p \\ a & \longmapsto & q \\ b & \longmapsto & q \\ c & \longmapsto & r \end{array}$$

no es una función, puesto que a un objeto de A no se le asocia un único elemento de B, (a a se le asocian p y q). Los conjuntos A y B se llaman **dominio** y **codominio**, respectivamente, de la función f.

El subconjunto del codominio que consiste de los elementos que son asociados a los del dominio se llama **imagen** de f. Así, en la función anterior, la imagen de f es el conjunto $\{p, q, r\}$; el elemento s de B no está en la imagen de f, es decir, no es imagen de ningún elemento de A bajo f.

Utilizamos la siguiente notación para denotar las imágenes de los elementos de A bajo f:

$$\begin{array}{rccc} f: & A & \longrightarrow & B \\ & a & \longmapsto & f(a)=p \\ & b & \longmapsto & f(b)=q \\ & c & \longmapsto & f(c)=r \end{array}$$

Tercero: considere el producto cartesiano de un conjunto A que se denota $A\times A$ y que consiste de todas las parejas ordenadas de elementos de A, es decir

$$A\times A=\{(a,b)|a,b\in A\}$$

Ahora ya podemos definir el importantísimo concepto de operación binaria o ley de composición. Sea G un conjunto no vacío. Una **operación binaria** o **ley de composición** en G es una función $f:G\times G\to G$ donde $(x,y)\longmapsto f(x,y)$.

Como es obvio, podemos denotar una función con cualquier símbolo, por ejemplo $f,g,h,\blacklozenge,\blacktriangle,\clubsuit,\heartsuit,\times,\otimes,*$, etc. Así, en $\mathbb{Z}$ podemos tener una operación binaria

$$\begin{array}{rccc} f: & \mathbb{Z}\times\mathbb{Z} & \rightarrow & \mathbb{Z} \\ & (x,y) & \longmapsto & f(x,y) \end{array}$$

y por abuso o conveniencia de notación denotamos $f(x,y)$ como xfy. Por ejemplo, $(3,2)\longmapsto f(3,2)=3f2$.

Si la operación binaria f la denotamos simplemente como $+$ (la suma usual en $\mathbb{Z}$) entonces $(3,2)\longmapsto +(3,2)=3+2$ que es igual a 5. Si la operación binaria f la denotamos como $\cdot$ (la multiplicación usual en $\mathbb{Z}$), entonces $(3,2)\longmapsto \cdot(3,2)=3\cdot 2$ que es igual a 6. Observe que una operación binaria se define en un conjunto no vacío G.

1.1 Ejemplo. Definamos un conjunto de la siguiente manera: considere tres cajas y reparta los números enteros en cada una de ellas de una manera ordenada como sigue:

$\vdots$	$\vdots$	$\vdots$
-6	-5	-4
-3	-2	-1
0	1	2
3	4	5
6	7	8
9	10	11
$\vdots$	$\vdots$	$\vdots$

[0]	[1]	[2]

Las cajas las denotaremos así: [0] por contener al cero, (o bien $0+3\mathbb{Z}$, es decir, los múltiplos de 3), [1] por contener al uno (o bien $1+3\mathbb{Z}$, es decir, los múltiplos de 3 mas 1), y caja [2] por contener al dos (o bien $2+3\mathbb{Z}$, es decir, los múltiplos de 3 mas 2). Asignémosle a la caja [0] el número 0, porque sus elementos dan residuo 0 al dividirlos entre 3; análogamente asignémosle a la caja [1] el número 1 y a la caja [2] el número 2, pues sus elementos dan residuo 1 y 2 respectivamente, al dividirlos entre 3. Consideremos el conjunto $\mathbb{Z}_3 = \{0, 1, 2\}$ llamado **juego completo de residuos módulo** 3, pues al dividir cualquier entero entre 3 da residuos $0, 1$ ó 2. Definamos en él una operación binaria que podríamos denotar con $f, g, h, \blacklozenge, \blacktriangle, \clubsuit, \heartsuit, \times, \otimes, *$, etc; escojamos $+$. Así

$$+ : \mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathbb{Z}_3$$

con

$$(1,1) \longmapsto +(1,1) = 1 + 1 = 2$$

$$(0,1) \longmapsto +(0,1) = 0 + 1 = 1$$

$$(1,0) \longmapsto +(1,0) = 1 + 0 = 1$$

$$(2,1) \longmapsto +(2,1) = 2 + 1 = 0$$

$$(2,2) \longmapsto +(2,2) = 2 + 2 = 1$$

Escribamos su tabla de sumar:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Veamos otro

1.2 Ejemplo. Consideremos el juego completo de residuos módulo 5, es decir, los posibles residuos que se obtienen al dividir cualquier número entero entre 5, el cual denotaremos con $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Dibuje usted las cajas. Definamos una operación binaria en $\mathbb{Z}_5$

$$\cdot : \mathbb{Z}_5 \times \mathbb{Z}_5 \to \mathbb{Z}_5$$

de la siguiente manera:

$$(2,2) \to \cdot(2,2) = 2 \cdot 2 = 4$$

$$(2,1) \to \cdot(2,1) = 2 \cdot 1 = 2$$

$$(2,3) \to \cdot(2,3) = 2 \cdot 3 = 1$$

$$(3,4) \to \cdot(3,4) = 3 \cdot 4 = 2$$

Es común oír el dicho "tan cierto como que dos y dos son cuatro". Sin embargo, como hemos visto en los ejemplos anteriores $2 + 2 = 1$, $2 + 1 = 0$, $2 \cdot 3 = 1$, $3 \cdot 4 = 2$, etc. y claramente $2 + 2 \neq 4$. En los ejemplos anteriores hemos considerado los conjuntos $\mathbb{Z}_3$ y $\mathbb{Z}_5$ a los cuales le hemos definido una "suma" u operación binaria. La suma usual en los números naturales y enteros es una operación binaria, lo mismo que la multiplicación definida en ellos. Estas son las operaciones binarias consideradas en el dicho. En los primeros años de escuela se pone un énfasis especial en uno de los muchos algoritmos para sumar y multiplicar números naturales (i.e. en el procedimiento o manera de sumarlos y multiplicarlos). Después de varios años se pone un especial énfasis en sumar y multiplicar números enteros y en multiplicar y dividir polinomios. En general, cuando se "suma" hay que especificar siempre el conjunto en el cual se define la operación binaria.

También es común oír el dicho "el orden de los factores no altera el producto". ¿Será esto siempre cierto?

1.3 Ejemplo. Consideremos el conjunto Δ_3 de los movimientos rígidos de un triángulo equilátero con vértices A, B, C, es decir, las rotaciones sobre el baricentro de $0°$, $120°$ y $240°$ y las reflexiones sobre las medianas. Denotemos éstos movimientos rígidos de la siguiente manera:

$$0 = [ABC/ABC], 1 = [ABC/BCA], 2 = [ABC/CAB]$$

$$3 = [ABC/ACB], 4 = [ABC/CBA], 5 = [ABC/BAC]$$

Los elementos $0, 1$ y 2 corresponden a las rotaciones. Los elementos $3, 4$ y 5 corresponden a las reflexiones. Definamos una operación binaria $\circ$ en Δ_3:

$$\circ : \Delta_3 \times \Delta_3 \to \Delta_3$$

$$(x, y) \to \circ\, (x, y) = x \circ y$$

Calculemos:

$$[ABC/BCA] \circ [ABC/BCA] = [ABC/CAB]$$

esto es

$$(1, 1) \to \circ (1, 1) = 1 \circ 1 = 2.$$

$$[ABC/CAB] \circ\ [ABC/ACB] = [ABC/BAC]$$

esto es

$$(2, 3) \to \circ\, (2, 3) = 2 \circ 3 = 5.$$

$$[ABC/ACB] \circ\ [ABC/CAB] = [ABC/CBA]$$

esto es

$$(3, 2) \to \circ\, (3, 2) = 3 \circ 2 = 4.$$

Observe que

$$2 \circ 3 \neq 3 \circ 2.$$

Ahora sí, ¿$2 + 2 = 4$ y $2 \circ 3 = 3 \circ 2$?

El concepto de operación binaria o ley de composición es uno de los más antiguos de la Matemática y se remonta a los antiguos egipcios y babilonios quienes ya poseían métodos para calcular sumas y multiplicaciones de números naturales positivos y de números racionales positivos (téngase en cuenta que no poseían el sistema de numeración que nosotros usamos). Sin embargo, al paso del tiempo, los matemáticos se dieron cuenta que lo importante no eran las tablas de sumar o multiplicar de ciertos "números" sino el conjunto y su operación binaria definida en él. Esto, junto con ciertas propiedades que satisfacían dieron lugar al concepto fundamental llamado grupo.

Es así que, de manera informal que posteriormente precisaremos, diremos que un **grupo** es un conjunto no vacío G junto con una operación binaria $f : G\times G\to G$, denotado (G, f) la cual cumple con ser asociativa, poseer elemento de identidad e inversos. La imagen de (x, y) en G la denotamos $(x, y) \longmapsto f(x, y)$. Por abuso o conveniencia de notación denotamos $f(x, y)$ como xfy y se llama **composición** de x y y.

Es fácil comprobar (ver los Problemas abajo) que los conjuntos $\mathbb{Z}_3$, $\mathbb{Z}_5$ y Δ_3 con su operacion binaria respectiva, poseen la estructura de grupo. Como se puede ver en el caso de $(\Delta_3, \circ)$, el concepto de grupo está estrechamente ligado con el concepto de simetría. Los ejemplos anteriores muestran algunos conjuntos que poseen una estructura de grupo y lo variantes estos pueden ser.

Podemos definir funciones $f : G \to G$, $g : G^2 = G\times G \to G$, $h : G\times G\times G \to G$ o bien $j : G^n = G \times ... \times G \to G$ dando así lugar a **operaciones unarias**, **binarias**, **ternarias** *o* **n arias**. La **operación nula** es una función $i : \{e\} \to G$.

Una **estructura algebraica** o **sistema algebraico** es un conjunto C junto con una o más operaciones n arias definidas en C las cuales podrían satisfacer ciertas axiomas o propiedades. En la siguiente sección definiremos algunas.

1.4 Definición. Considere H un subconjunto de un grupo $(G, \circ)$. Diremos que H es **estable** o **cerrado** con respecto a la operación binaria $\circ$ si $x \circ y \in H$, para cualesquiera elementos $x, y \in H$. Obsérvese que la restricción de $\circ$ a un subconjunto estable o cerrado H proporciona una operación binaria para H llamada **operación binaria inducida**.

Problemas

1.1 Haga una tabla que represente la multiplicación de todos los elementos de $\mathbb{Z}_3$.

1.2 Construya una tabla que represente la suma de todos los elementos de $\mathbb{Z}_5$.

1.3 Construya una tabla que represente la multiplicación de todos los elementos de $\mathbb{Z}_5$.

1.4 Compruebe que Δ_3 con la operación binaria definida en el Ejemplo 1.3 es un grupo.

1.5 Sea Σ_3 el conjunto de las permutaciones de $1, 2, 3$. Calcule el número de elementos de Σ_3. Defina una operación binaria en Σ_3 y construya su tabla.

1.6 Sea Σ_n el conjunto de las permutaciones de un conjunto con n elementos. Calcule el número de elementos de Σ_n.

1.7 Construya una tabla que represente la suma de todos los elementos de $\mathbb{Z}_6$ y compárela con las tablas de Σ_3 y Δ_3. Observe que las tablas de Σ_3 y Δ_3 son la misma salvo por el orden y el nombre de los elementos. Compruebe que éstos dos últimos son grupos y establezca una función biyectiva entre sus elementos. Observe que la tabla de $\mathbb{Z}_6$ le permite comprobar que es un grupo, pero que su tabla es totalmente diferente a las otras dos.

I.2 Estructuras Algebraicas

En esta sección definiremos varias estructuras algebraicas algunas de las cuales ya han sido implícitamente estudiadas. Tiene como finalidad la de **presentar un breve panorama** de algunas de las estructuras algebraicas (no el del estudio propio de la categoría de grupos) y así situar al lector en una mejor posición para comprender los objetos de estudio de la Teoría de Grupos. Supondremos que el lector ya conoce los fundamentos del Álgebra Lineal como en (Ll2) y utilizaremos la notación que ahí se expone.

Sea $(V, +, \mu)$ un espacio vectorial sobre un campo K tal como se definió en Álgebra Lineal. Si quitamos la multiplicación escalar μ nos quedaremos con un conjunto con una operación binaria $+$ que cumple las cuatro axiomas usuales. Entonces diremos que $(V, +)$ es un **grupo conmutativo bajo** $+$. Formalmente, **con esta notación y en este contexto** (en la próxima sección daremos otra versión de la definición de grupo más general) **repetimos,** para ligarla con el estudio de espacios vectoriales, la definición de grupo introducida en la sección anterior:

2.1 Definición. Un **grupo** es una pareja $(G, +)$ donde G es un conjunto no vacío y
$$+ \colon G \times G \to G$$
es una operación binaria
$$(u, v) \longmapsto +(u, v)$$
donde, por conveniencia o abuso de notación se escribe
$$+(u, v) = u + v$$
tal que
(i) $+(+(u, v), w) = +(u, +(v, w))$, es decir, $(u + v) + w = u + (v + w)$
(ii) existe un elemento $O \in G$, llamado **elemento de identidad**, tal que $+(v, O) = v + O = v$
(iii) para cada $v \in G$ existe un elemento, llamado **inverso**, denotado con $-v$, tal que $+(v, -v) = v + (-v) = O$.

Diremos que el grupo es **conmutativo** si además satisface
(iv) $+(u, v) = +(v, u)$ es decir, $u + v = v + u$.

Si en la definición anterior consideramos un conjunto E con una operación binaria $+$ sin que cumpla alguna condición, decimos que $(E, +)$ es un **magma** (o **grupoide**).

Si en la definición anterior consideramos un conjunto S con una operación binaria $+$ que cumpla (i) diremos que $(S, +)$ es un **semigrupo**.

También, si en la definición 2.1 consideramos un conjunto M con una operación binaria $+$ que cumpla (i) y (ii) diremos que $(M, +)$ es un **monoide**.

2.2 Ejemplo. El conjunto $\mathbb{N}$ de los números naturales con la suma usual es un semigrupo pero no un monoide pues no tiene elemento de identidad. $(\mathbb{Z}, +)$ y $(\mathbb{Z}_n, +)$ (con $n \in \mathbb{N}$) son monoides conmutativos bajo la "suma" y $(\mathbb{N}, \cdot), (\mathbb{Z}, \cdot)$y $(\mathbb{Z}_n, \cdot)$ son monoides "multiplicativos".

2.3 Ejemplo. El lector podrá comprobar que $(\mathbb{Z}, +)$, $(n\mathbb{Z}, +)$, $n \in \mathbb{Z}$, $(\mathbb{Q}, +)$, $(\mathbb{Q}^* = \mathbb{Q} - \{0\}, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R}^* = \mathbb{R} - \{0\}, \cdot)$, $(\mathbb{C}, +)$, $(\mathbb{C}^* = \mathbb{C} - \{0\}, \cdot)$, $(\mathbb{Z}_n, +)$, $(\Delta_3, \circ)$, $(\Sigma_3, \circ)$, $(\Sigma_n, \circ)$, $(M_nK, +)$, donde M_nK denota las matrices cuadradas de $n \times n$ con coeficientes en un campo K, $(GL_nK, +)$ y $(GL_nK, \cdot)$, donde GL_nK denota las matrices cuadradas invertibles de $n \times n$ $(n \in \mathbb{N})$ con coeficientes en un campo K, son grupos (con las operaciones binarias usuales en cada uno de ellos).

Recordemos que podemos denotar la operación binaria en un conjunto con cualquier símbolo, por ejemplo, $+, *, \circ, \diamond, \star, \theta, \bullet, \triangle$, etc.lo cual haremos en adelante. Diremos que el **orden** de un grupo $(G, \cdot)$ es el número de elementos del conjunto G y lo denotaremos con $o(G)$ o bien con $\mid G \mid$ indistintamente. Así, varias formas de escribir esto son: $(\mathbb{Z}_n, +)$ tiene orden n, $o(\Delta_3, \circ) = 6$, $\mid \Sigma_3 \mid = 6$, $o(\Sigma_n) = n!$. Si $\mid G \mid$ es infinito (finito) diremos que G es infinito (finito). Así, $\mathbb{Z}$ es (constituye un grupo) infinito (bajo la suma usual).

Para relacionar dos grupos es necesario definir una función que preserve la estructura de grupo.

2.4 Definición. Sean $(G, \diamond)$ y $(G', \star)$ dos grupos. Un **homomorfismo de grupos** es una función $f \colon G \to G'$ tal que $f(u \diamond v) = f(u) \star f(v)$.

Ahora, recordemos la definición de acción y definamos el concepto de grupo con operadores:

2.5 Definición. Sean Ω y A dos conjuntos. Una **acción** de Ω en A es una función de $\Omega \times A$ en el conjunto A.

2.6 Definición. Sea Ω un conjunto. Un grupo $(G, \cdot)$ junto con una acción de Ω en $(G, \cdot)$

$$\begin{array}{rcl} \circ : \Omega \times G & \longrightarrow & G \\ (\alpha, x) & \mapsto & \circ(\alpha, x) = \alpha \circ x = x^\alpha \end{array}$$

que sea distributiva con respecto a la ley de composición de $(G, \cdot)$ se llama **grupo con operadores** en Ω.

La ley distributiva puede expresarse como

$$(xy)^\alpha = x^\alpha y^\alpha$$

i.e.,

$$(\alpha, xy) \longmapsto \circ(\alpha, xy) = \alpha \circ (xy) = (\alpha \circ x)(\alpha \circ y).$$

2.7 Observación. En un grupo G con operadores en Ω, cada elemento de Ω (llamado **operador**) define un endomorfismo (i.e.un homomorfismo de $G \longrightarrow G$) del grupo G. Consideremos $\Omega = \mathbb{Z}$ y para $x \in G$, $n \in \mathbb{Z}$ definamos

$$\begin{array}{ccc} \circ : \mathbb{Z} \times G & \longrightarrow & G \\ (n, x) & \mapsto & n \circ x = x^n \end{array}$$

Si G es abeliano, tenemos que

$$n(xy) = (xy)^n = x^n y^n = (nx)(ny)$$

Luego, todo grupo abeliano G puede verse como un grupo con operadores en $\mathbb{Z}$.

2.8 Definición. Un **anillo** es una terna $(\Lambda, +, \cdot)$ donde Λ es un conjunto, $+$ y $\cdot$ son operaciones binarias tales que
(i) $(\Lambda, +)$ es un grupo conmutativo
(ii) $(\Lambda, \cdot)$ es un semigrupo
(iii) $u(v + w) = uv + uw$ y $(u + v)w = uw + vw$

El lector podrá comprobar que $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$,$(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(M_nK, +, \cdot)$, $(K, +, \cdot)$,$(K[x], +, \cdot)$, $(\mathbb{C}, +, \cdot)$ son anillos.

Si un anillo $(\Lambda, +, \cdot)$ satisface
(iv) $(\Lambda, \cdot)$ es un semigrupo conmutativo, entonces $(\Lambda, +, \cdot)$ se llamará **anillo conmutativo**.

Si $(\Lambda, \cdot)$ es un monoide, diremos que $(\Lambda, +, \cdot)$ es un **anillo con identidad** o **con uno**.

Recuerde que si el producto de dos elementos distintos de cero de un anillo Λ es el elemento cero del anillo, entonces esos dos elementos se dice que son **divisores de cero.** Si el anillo $(\Delta, +, \cdot)$ con $1 \neq 0$ no posee divisores de cero, se llamará **dominio entero**. Si un dominio entero posee un inverso multiplicativo para cada elemento no nulo, se dice que es un **anillo con división**.

Finalmente, un **campo** es un anillo conmutativo con división.

¿Cómo se relacionan dos anillos? Mediante funciones que preserven la estructura de anillos. Si $(\Lambda, \diamond, \star)$ y $(\Lambda', +, \cdot)$ son anillos, un **homomorfismo de anillos** es una función que es un homomorfismo del grupo conmutativo de Λ en el grupo conmutativo de Λ' y que también es un homomorfismo del semigrupo de Λ en el semigrupo de Λ', es decir,

$$f(u \diamond v) = f(u) + f(v) \text{ y } f(u \star v) = f(u) \cdot f(v).$$

Si en la definición de espacio vectorial consideramos un anillo $(\Lambda, +, \cdot)$ conmutativo con 1 en lugar de un campo K, obtendremos una estructura algebraica llamada **Λ-módulo (izquierdo)**. Entonces, como caso particular de los Λ-módulos están los K-módulos, i.e. los espacios vectoriales sobre un campo K.

Muchos de los resultados para los espacios vectoriales son válidos para los Λ-módulos, basta tomar $K = \Lambda$ un anillo conmutativo con 1. En particular, relacionamos dos Λ-módulos mediante un **homomorfismo de Λ-módulos**. Los Λ-módulos son generalizaciones de los conceptos de grupo conmutativo y de espacio vectorial, y son los objetos de estudio del Álgebra Homológica (véase Ll1). Imitando a los espacios vectoriales, si un Λ-módulo posee una *base*, lo llamaremos **Λ-módulo libre**. No todo Λ-módulo posee base, es decir, no todo Λ-módulo es libre, pero todo espacio vectorial o K-módulo es libre, es decir, sí posee una base. Diremos que un Λ-módulo es **proyectivo** si es sumando directo de un libre y que es **finitamente generado** si posee un conjunto finito de generadores.

Un **álgebra** sobre Λ (Λ un anillo conmutativo con uno) es un conjunto A que simultáneamente es un anillo y un Λ-módulo. Es decir, un álgebra $(A, +, \mu, \cdot)$ es un Λ-módulo con otra operación binaria, llamada **multiplicación** con una condición extra que hace compatibles las operaciones binarias y multiplicación escalar, la cual es la siguiente:

$(\lambda u + \lambda' v)w = \lambda(uw) + \lambda'(vw)$
$w(\lambda u + \lambda' v) = \lambda(wu) + \lambda'(wv) \quad$ para $\lambda, \lambda' \in \Lambda; u, v, w \in A$

En particular se tiene que $(\lambda u)v = \lambda(uv) = u(\lambda v)$ y por lo tanto λuv es un elemento bien definido de A. Dejamos al lector proporcionar la definición de homomorfismo de álgebras así como percatarse de varios ejemplos de álgebras ya conocidos introducidos implícitamente.

Si se imponen condiciones en la multiplicación de un álgebra se obtienen **álgebras conmutativas**, **álgebras asociativas**, **álgebras con uno**.

Un álgebra asociativa con uno tal que todo elemento diferente de cero sea invertible se llama **álgebra con división**.

2.9 Ejemplo. $(M_nK, +, \cdot, \mu)$, donde M_nK denota las matrices cuadradas de $n \times n$ con coeficientes en un campo K (μ denota la multiplicación escalar) es un álgebra al igual que $(K, +, \cdot, \mu)$ y $(K[x], +, \cdot, \mu)$.

Definimos un **álgebra graduada** como una sucesión $A = (A_0, A_1, A_2, ...)$ de álgebras A_i, una para cada índice $i \in N$.

Para quienes han estudiado, dentro de un curso elemental de Álgebra Lineal, el Álgebra Multilineal (como en Ll2), recordarán los siguientes conceptos que no son requisitos para este texto.

2.10 Ejemplo. Sea $T^k(V) = \otimes^k V = V \otimes_K \cdots \otimes_K V$ el producto tensorial de un espacio vectorial V sobre un campo K, k veces. Llamaremos a $T^k(V)$ **espacio tensorial de grado** k de V. Si definimos una multiplicación

$$\cdot : T^k V \times T^l V \to T^{k+l} V \text{ mediante}$$

$$(u_1 \otimes ... \otimes u_k) \cdot (v_1 \otimes ... \otimes v_l) = u_1 \otimes ... \otimes u_k \otimes v_1 \otimes ... \otimes v_l$$

tenemos un álgebra graduada (donde definimos $T^0 V = K$ y $T^1 V = V$) $TV = (K, V, T^2 V, T^3 V, T^4 V, \ldots)$ llamada **álgebra tensorial** de V.

2.11 Ejemplo. Sea $\bigwedge^k V = V \wedge ... \wedge V$ el producto exterior de un espacio vectorial V sobre un campo K, k veces. Consideremos la multiplicación exterior definida por

$$\wedge : \bigwedge^k V \times \bigwedge^l V \to \bigwedge^{k+l} V.$$

Entonces tenemos un álgebra graduada

$$\bigwedge V = (K, V, \bigwedge^2 V, \bigwedge^3 V, \ldots)$$

llamada **álgebra exterior** o **álgebra de Grassmann** de V.

Problemas

2.1 Compruebe que los conjuntos con sus operaciones binarias respectivas en el Ejemplo 2.2 son efectivamente monoides.

2.2 Compruebe que los conjuntos con sus operaciones binarias respectivas en el Ejemplo 2.3 son efectivamente grupos.

2.3 Compruebe que los conjuntos con sus operaciones binarias respectivas en el Ejemplo 2.9 son efectivamente álgebras.

2.4 Compruebe que los números complejos bajo la multiplicación forman un monoide.

I.3 Propiedades Elementales

En esta sección presentaremos algunas propiedades elementales de los grupos. Como se ha explicado anteriormente en general, ahora en particular aplicado a la Teoría de Grupos, siempre que se pruebe alguna propiedad para un conjunto con una operación binaria que satisfaga los axiomas de grupo, de inmediato, esa propiedad es válida para todos esos conjuntos que satisfagan las axiomas de grupo.

Consideremos un grupo $(G,\cdot)$. Si x y y son elementos de G, denotaremos $x\cdot y$ simplemente como xy para simplificar la notación. Sea e el elemento de identidad de G. Con esta notación, la definición generalizada de grupo que prometimos en la sección anterior es:

Un **grupo** es una pareja $(G,\cdot)$ donde G es un conjunto no vacío y

$$\cdot\colon G\times G\to G$$

es una operación binaria

$$(x,y)\longmapsto \cdot(x,y)$$

donde, por abuso o conveniencia de notación se escribe

$$\cdot(x,y)=x\cdot y=xy$$

tal que
(i) $(xy)z=x(yz)$; $x,y,z\in G$.
(ii) existe un elemento $e\in G$ tal que $ey=y$, para toda $y\in G$.
(iii) para cada $y\in G$ existe un elemento, denotado y^{-1}, tal que $(y^{-1})y=e$.

Diremos que el grupo es **conmutativo** o **abeliano** si además satisface
(iv) $xy=yx$, para toda $x,y\in G$, es decir, si su operación binaria es conmutativa.

Si el grupo es abeliano, se acostumbra denotar su operación binaria con el signo $+$.

Podemos ver el concepto de grupo como un caso especial del de grupos con operadores en $\varnothing$ (con acción, la única posible de $\varnothing$ en G).

El elemento e lo llamaremos **elemento de identidad izquierdo** o simplemente **identidad izquierda** de x y y^{-1}lo llamaremos **inverso izquierdo** de y.

De manera análoga se tiene el **elemento de identidad derecho** y el **inverso derecho**. Cuando es clara la notación de la operación binaria, con frecuencia se omite y simplemente se designa un grupo $(G, \cdot)$ con G.

Veamos a continuación que en nuestra definición de grupo, el pedir que se tenga elemento de identidad por la izquierda e inverso izquierdo implica que se tiene también identidad e inverso derechos.

3.1 Proposición. En un grupo $(G, \cdot)$, si un elemento es inverso izquierdo entonces es inverso derecho. Si e es identidad izquierda, entonces es identidad derecha.

Demostración. Considere $x^{-1}x = e$ para cualquier elemento $x \in G$. Considere el elemento inverso izquierdo del elemento x^{-1}, es decir $(x^{-1})^{-1}x^{-1} = e$. Luego

$$xx^{-1} = e(xx^{-1}) = ((x^{-1})^{-1}x^{-1})(xx^{-1}) = (x^{-1})^{-1}ex^{-1} = (x^{-1})^{-1}x^{-1} = e.$$

Así que x^{-1} es inverso derecho de x. Ahora, para cualquier elemento x, considere las igualdades

$$xe = x(x^{-1}x) = (xx^{-1})x = ex = x.$$

Luego e es identidad derecha.♦

Diremos que e es el **elemento de identidad** de un grupo G si e es elemento de identidad izquierdo o derecho y hablaremos del **inverso** de un elemento si existe su inverso izquierdo o derecho.

A continuación veamos algunas propiedades elementales:

3.2 Proposición. El elemento de identidad e de un grupo G es único.

Demostración. Sea e' otro elemento de identidad tal que $e'e = e$. Como e es también identidad, entonces $e'e = e'$. Luego $e = e'$.♦

3.3 Proposición. Si en un grupo G se tiene que $xy = xz$, entonces $y = z$. También, si $yx = zx$, entonces $y = z$.

Demostración. Si $xy = xz$, entonces $x^{-1}(xy) = x^{-1}(xz)$. Por la asociatividad, $(x^{-1}x)y = (x^{-1}x)z$. Luego, $ey = ez$ y finalmente $y = z$. De manera semejante se prueba que si $yx = zx$, entonces $y = z$.♦

3.4 Proposición. En un grupo cualquiera, el inverso de cualquier elemento de un grupo es único.

Demostración. Sea x' otro inverso del elemento x. Luego, $x'x = e$. También $x^{-1}x = e$. Luego, $x'x = x^{-1}x = e$. Por la proposición anterior, $x' = x^{-1}$.♦

3.5 Proposición. En un grupo cualquiera G, si $x, y \in G$, las ecuaciones $xa = y$ y $bx = y$ tienen solución única en G.

Demostración. Puesto que $x(x^{-1}y) = (xx^{-1})y = ey = y$. Luego, $a = x^{-1}y$ es una solución de $xa = y$. Supongamos que hay dos soluciones, $xa = y$ y $x\acute{a} = y$. Entonces $xa = x\acute{a}$, luego $a = \acute{a}$. Análogamente para el otro caso.♦

3.6 Proposición. En un grupo G, se tiene, para cualesquiera elementos x, y de G

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Demostración. Como

$$\begin{aligned} (xy)(y^{-1}x^{-1}) &= x(yy^{-1})x^{-1} = xx^{-1} = e \\ (y^{-1}x^{-1})(xy) &= y^{-1}(x^{-1}x)y = y^{-1}y = e \end{aligned}$$

luego, $(xy)^{-1} = y^{-1}x^{-1}$.♦

Recordemos la definición de homomorfismo de grupos de la sección anterior con la notación siguiente:. Sean $(G, +)$ y $(G', \cdot)$ dos grupos. Un **homomorfismo de grupos** es una función $f \colon G \to G'$ tal que $f(u + v) = f(u) \cdot f(v)$.

Veamos algunos ejemplos.

3.7 Ejemplo. Sea $G = \mathbb{R}^3$ y $G' = \mathbb{R}$ con la suma usual. Definamos $f : G \to G'$ mediante la regla $f(x, y, z) = 8x - 4y + 4z$. Veamos que f es un homomorfismo. Como

$$\begin{aligned} f((x_1, y_1, z_1) + (x_2, y_2, z_2)) &= f(x_1 + x_2, y_1 + y_2, z_1 + z_2) \\ &= 8(x_1 + x_2) - 4(y_1 + y_2) + 4(z_1 + z_2) \text{ y} \\ f(x_1, y_1, z_1) + f(x_2, y_2, z_2) &= (8x_1, -4y_1 + 4z_1) + (8x_2 - 4y_2 + 4z_2), \end{aligned}$$

f es un homomorfismo.

3.8 Proposición. Sea $f : G \to G'$ un homomorfismo de grupos. Si e es el elemento de identidad de G entonces $f(e) = e'$ es el elemento de identidad de G'.

Demostración. Considere $e'f(x) = f(x) = f(ex) = f(e)f(x)$. Multiplicando ambos lados por el inverso de $f(x)$obtenemos $e'f(x)f(x)^{-1} = f(e)f(x)f(x)^{-1}$. Luego $e' = e'e' = f(e)e' = f(e)$. Así que $e' = f(e)$.♦

3.9 Ejemplo. Sea $G = G' = \mathbb{R}^2$. Definamos $f : G \to G'$ mediante $f(x, y) = (x + 8, y + 2)$. Como $f(0, 0) = (8, 2) \neq (0, 0)$, f no es homomorfismo pues todo homomorfismo de grupos envía el elemento de identidad del dominio en el elemento de identidad del codominio.

3.10 Proposición. La composición de dos homomorfismos de grupos es un homomorfismo de grupos.

Demostración. Sean $f : G' \to G$ y $g : G \to G''$ homomorfismos de grupos. Luego $(g \circ f)(x + y) = g(f(x + y)) = g(f(x) + f(y)) = g(f(x)) + g(f(y)) = (g \circ f)(x) + (g \circ f)(y)$. Por lo tanto $(g \circ f)$ es un homomorfismo.♦

3.11 Definición. Sea $f : G \to G'$ un homomorfismo de grupos. Diremos que f es un **isomorfismo**, y escribiremos $f : G \overset{\cong}{\to} G'$ si existe un homomorfismo $g : G' \to G$ tal que $g \circ f = 1_G$ y $f \circ g = 1_{G'}$.

Es fácil comprobar (Problema 3.13) que, si g existe, está determinada en forma única; la denotaremos con f^{-1} y se llama **inverso** de f. Así, $f : G \to G'$ es isomorfismo si, y sólo si, es biyectiva. Diremos que dos grupos G y G' son **isomorfos** si existe un isomorfismo $f : G \overset{\cong}{\to} G'$ y escribiremos $G \cong G'$.

3.12 Definición. Sea $f : G \to G'$ un homomorfismo de grupos. El **núcleo** de f, denotado ker f, es el conjunto de todos los elementos $x \in G$ tales que $f(x) = e'$ donde e' denota la identidad de G'. La **imagen** de f, denotada $im\ f$, es el conjunto de $f(x)$ con $x \in G$.

Si en la definición de homomorfismo se tiene que ker $f = \{e\}$ diremos que f es un **monomorfismo** y lo denotamos $f : G \rightarrowtail G'$; si $im\ f = G'$ diremos que f es un **epimorfismo** y lo denotamos $f : G \twoheadrightarrow G'$ y si f es tal que $\ker f = \{e\}$ e $im\ f = G'$ entonces diremos que f es un **isomorfismo**. Dicho de otra manera, f es un monomorfismo cuando es inyectiva; es un epimorfismo cuando es suprayectiva y es un isomorfismo cuando es biyectiva (Problema 3.13). Llamaremos **endomorfismo** a un homomorfismo $f : G \to G$ y diremos que es **automorfismo** si dicha f es biyectiva.

3.13 Proposición. Sean $f \colon G' \to G$, $g \colon G \to G''$ dos homomorfismos de grupos y $h = g \circ f$ la composición. Entonces, (i) si h es monomorfismo, f es monomorfismo, y (ii) si h es epimorfismo, g es epimorfismo.

Demostración. (i) Supongamos que h es monomorfismo. Si $f(x) = f(y)$ luego $h(x) = g(f(x)) = g(f(y)) = h(y)$. Como h es monomorfismo, $x = y$. Por lo tanto, f es monomorfismo. (ii) Supongamos que h es epimorfismo. Entonces $h(G') = G''$. Luego, $G'' = h(G') = g(f(G')) \subset g(G) \subset G''$. Por lo tanto, $g(G) = G''$.♦

Diremos que un homomorfismo $f \colon G \to G'$ es **trivial** si $f(x) = e'$ para todo $x \in G$. Es decir, $im\ f = \{e'\}$. Si f es trivial, lo denotaremos con O (véase el Problema 3.9). Así que, $f = O$ si, y sólo si, $\ker f = G$.

A continuación nos preguntamos acerca de los subconjuntos de un grupo que son, a la vez, grupos.

3.14 Definición. Diremos que un subconjunto H de $(G, \cdot)$ es un **subrupo** de G si H es un grupo estable o cerrado bajo la operación binaria inducida. Lo denotaremos $H < G$.

Veamos un resultado que proporciona una manera de comprobar si un subconjunto de un grupo es un subgrupo de él.

3.15 Proposición. Un subconjunto H de $(G, \cdot)$ es un subrupo de G si, y sólo si, se satisfacen las siguientes tres condiciones:
(i) H es estable o cerrado bajo $\cdot$.
(ii) el elemento de identidad e de G está en H.
(iii) si $x \in H$, entonces $x^{-1} \in H$.
Demostración. Véase el Problema 3.4.♦

3.16 Ejemplo. $(\mathbb{Z}, +)$ es subgrupo de $(\mathbb{R}, +)$. $(\mathbb{Q}^+, \cdot)$ es un subgrupo de $(\mathbb{R}^+, \cdot)$. También, $(\mathbb{Q}, +)$ es un subgrupo de $(\mathbb{R}, +)$, $(\mathbb{R}, +)$ es un subgrupo de $(\mathbb{C}, +)$ y $(2\mathbb{Z}, +)$ es un subgrupo de $(\mathbb{Z}, +)$.

3.17 Ejemplo. Sea $(G, \cdot)$ un grupo. Tanto G como $\{e\}$ son subgrupos de $(G, \cdot)$, llamados **subgrupos impropios**. Los demás subgrupos se llaman **propios**. El subgrupo $\{e\}$ se llama **subgrupo trivial** y se acostumbra denotar, por abuso, simplemente como e donde e puede denotarse como 0 o 1 o cualquier otra notación que denota el elemento de identidad del grupo que se está considerando.

3.18 Proposición. La intersección de subgrupos de G es un subgrupo de G.

Demostración. Sea $\{H_i\}_{i \in I}$ una colección de subgrupos de G indizada por un conjunto de índices I. Tomemos $x, y \in \cap_i H_i$. Como $\cap_i H_i \subset H_i$ para cualquier i, tenemos que $x, y \in H_i$. Como H_i es subgrupo de G, $x + y \in H_i$, $e \in H_i$, $x^{-1} \in H_i$ para toda $i \in I$. Por lo tanto, $x + y \in \cap H_i, e \in \cap H_i, x^{-1} \in \cap H_i$.♦

3.19 Proposición. Sea $f : G \to G'$ un homomorfismo de grupos. Entonces, si H es un subgrupo de G, $f(H)$ es un subgrupo de G' y si H'es un subgrupo de G', $f^{-1}(H')$ es un subgrupo de G.

Demostración. Veamos que $f(H) = \{f(x) \mid x \in H\}$ es un subgrupo de G'. Sean $v, w \in f(H)$, luego, existen $x, y \in H$ tales que $f(x) = v$, $f(y) = w$. Como H es subgrupo de G, $x + y \in H$. Como f es homomorfismo, $f(e) = e' \in f(H)$, $v+w = f(x)+f(y) = f(x+y) \in f(H)$. Si $x \in H$ entonces $f(x) \in f(H)$. Por ser H subgrupo de G, $x^{-1} \in H$. Luego (Problema 3.18) $f(x^{-1}) = f(x)^{-1} \in f(H)$. Por lo tanto, $f(H)$ es un subgrupo de G'.

Ahora, veamos que $f^{-1}(H') = \{x \in G | f(x) \in H'\}$ es un subgrupo de G. Sean $x, y \in f^{-1}(H')$, entonces $f(x)$ y $f(y)$ están en H'. Como H' es un subgrupo de G' y f es homomorfismo, $f(x + y) = f(x) + f(y) \in H'$ y $f(e) = e' \in H'$. También, dado $f(x) \in H'$, como $f(x)^{-1} = f(x^{-1})$, $f(x)^{-1} \in H'$. Así $f^{-1}(H')$ es un subgrupo de G.♦

Observe que en la Proposición anterior, la imagen inversa es un subgrupo del dominio aunque no exista una función inversa f^{-1} para f. La imagen inversa de $\{e'\}$ es el núcleo de f y la imagen inversa de cualquier subgrupo contiene al núcleo de f.

3.20 Corolario. Sea $f : G \to G'$ un homomorfismo de grupos. Entonces *im* f es un subgrupo de G' y *ker* f es un subgrupo de G.

Demostración. Inmediata de la proposición anterior tomando $H = G$ y $H' = e'$.♦

Denotemos con $Hom(X,Y)$ el conjunto de homomorfismos del grupo abeliano X en el grupo abeliano Y. Sean $f, g\colon X \longrightarrow Y$ homomorfismos de grupos abelianos y definamos $f + g\colon X \longrightarrow Y$ mediante $(f+g)(x) = f(x) + g(x)$. Es fácil comprobar que esta definición hace de $Hom(X,Y)$ un grupo abeliano, (Problema 3.21).

Sea $\psi\colon Y' \longrightarrow Y$ un homomorfismo de grupos abelianos y $(X \xrightarrow{f} Y')$ un elemento de $Hom(X,Y')$. Asociemos a f un homomorfismo $(X \xrightarrow{g} Y) \in Hom(X,Y)$ mediante una función

$$\psi_* = Hom(X,\psi)\colon Hom(X,Y') \longrightarrow Hom(X,Y)$$

dada por $\psi_*(f) = \psi \circ f$. Entonces ψ_* es un homomorfismo de grupos abelianos (Problema 3.22), llamado **homomorfismo inducido por** ψ.

Sea $\varphi\colon X' \longrightarrow X$ un homomorfismo de grupos abelianos y $(X \xrightarrow{g} Y) \in Hom(X,Y)$. Asociemos a g un homomorfismo $(X' \xrightarrow{f} Y) \in Hom(X',Y)$ mediante una función

$$\varphi^* = Hom(\varphi,Y)\colon Hom(X,Y) \longrightarrow (X',Y)$$

dada por $\varphi^*(g) = g \circ \varphi$. Entonces φ^* es un homomorfismo de grupos abelianos (Problema 3.23), llamado **homomorfismo inducido por** φ.

Sean $\psi\colon Y' \longrightarrow Y$ y $\psi'\colon Y \longrightarrow Y''$ homomorfismos de grupos abelianos y X un grupo abeliano. Si $1_Y\colon Y \longrightarrow Y$ es la identidad, entonces $1_{Y_*}\colon Hom(X,Y) \longrightarrow Hom(X,Y)$ es la identidad de $Hom(X,Y)$, y $(\psi' \circ \psi)_* = \psi'_* \circ \psi_*$. (Problema 3.24). Esto lo podemos visualizar en el siguiente diagrama:

$$\begin{array}{ccccccc}
(X \xrightarrow{f} & Y') & & \in & Hom(X,Y') & & \\
\| & \downarrow \psi & 1_Y & & \downarrow \psi_* & 1_{Y_*} & \\
(X \xrightarrow{g} & Y) & & \in & Hom(X,Y) & & \psi'_* \circ \psi_* \\
\| & \downarrow \psi' & & & \downarrow \psi'_* & & \\
(X \xrightarrow{h} & Y'') & & \in & Hom(X,Y'') & &
\end{array}$$

Sean $\varphi\colon X' \longrightarrow X$ y $\varphi'\colon X \longrightarrow X''$ homomorfismos de grupos abelianos y Y un grupo abeliano. Si $1_X\colon X \longrightarrow X$ es la identidad, entonces $1^*_X\colon Hom(X,Y) \rightarrow Hom(X,Y)$ es la identidad de $Hom(X,Y)$, y $(\varphi' \circ \varphi)^* = \varphi^* \circ \varphi'^*$. (Problema 3.25). Esto lo podemos visualizar en el siguiente diagrama:

$$\begin{array}{cccccc}
(X' \xrightarrow{f} & Y) & \in & Hom(X',Y) & & \\
{}_{1_X} \downarrow \varphi & \| & & \uparrow \varphi^* & 1^*_X & \\
(X \xrightarrow{g} & Y) & \in & Hom(X,Y) & & (\varphi' \circ \varphi)^* \\
\downarrow \varphi' & \| & & \uparrow \varphi'^* & & \\
(X'' \xrightarrow{h} & Y) & \in & Hom(X'',Y) & &
\end{array}$$

Problemas.

3.1 Establezca la definición de grupo conmutativo escrito "aditivamente", así como las propiedades elementales arriba expuestas.

3.2 Pruebe que $(x^{-1})^{-1} = x$ y que $e^{-1} = e$.

3.3 Pruebe que si $xy = yx$ en un grupo G entonces $(xy)^n = x^n y^n$.

3.4 Pruebe la Proposición 3.15.

3.5 Muestre que hay dos grupos que tienen 4 elementos, escriba sus tablas, encuentre sus subgrupos y su red de subgrupos. Uno es $\mathbb{Z}_4$ y el otro se conoce como el **grupo** 4 **de Klein** denotado con la letra V.

3.6 Compruebe las afirmaciones del Ejemplo 3.16.

3.7 El grupo de simetrías de un polígono regular de n lados se llama grupo diedro de grado n, denotado D_n. Escriba las tablas de multiplicar de D_3 y D_4. Determine el orden de D_n.

3.8 Sea $G = G' = K^n$ donde K es denota un campo. Pruebe que $f\colon G \to G'$ dado por $f(u_1, \ldots, u_n) = (u_1, u_2, \ldots, u_{n-1}, 0)$ es un homomorfismo.

3.9 Sea G un grupo. Pruebe que la función $1_G\colon G \to G$ y la función $O_G\colon G \to G$ dadas por $1_G(x) = x$ y $O_G(x) = O$ para toda $x \in G$, son homomorfismos. 1_G se llama **homomorfismo identidad** de G y O_G se llama **homomorfismo trivial**.

3.10 Compruebe cuales funciones son homomorfismos y cuales no lo son:
(i) $f\colon K^n \to K^m$, $f(x) = Ax$ donde A es una matriz de $m \times n$ con elementos en el campo K.
(ii) $f\colon K^2 \to K^2$, $f(x, y) = (4y, 0)$
(iii) $f\colon K^3 \to K^3$, $f(x, y, z) = (-z, x, y)$
(iv) $f\colon K^2 \to K^2$, $f(x, y) = (x^2, 2y)$
(v) $f\colon K^5 \to K^4$, $f(u, v, x, y, z) = (2uy, 3xz, 0, 4u)$
(vi) $f\colon K^3 \to K^3$, $f(x, y, z) = (x + 2, y + 2, z + 2)$

3.11 Establezca, si es posible, homomorfismos no triviales en los siguientes casos:
(i) $1 \longrightarrow Z_2$
(ii) $Z_2 \xrightarrow{\times 2} Z_4$
(iii) $Z_4 \longrightarrow Z_2$
(iv) $Z_2 \longrightarrow 1$
(v) $Z_2 \longrightarrow Z_2 \times Z_2$

(vi) $Z_2 \times Z_2 \longrightarrow Z_2$
(vii) $Z_4 \longrightarrow Z_2 \times Z_2$

3.12 Denotemos con $Hom(G, G')$ el conjunto de homomorfismos del grupo G en el grupo abeliano G'. Defina $f+g\colon G \to G'$ mediante $(f+g)(x) = f(x)+g(x)$, $x \in G$. Pruebe que $(Hom(G, G'), +)$ es un grupo.

3.13 Pruebe que si $f : G \to G'$ es un isomorfismo de grupos como en la Definición 3.11, g está determinada en forma única y que f es isomorfismo si, y sólo si es biyectiva.

3.14 Sea $f : G \to G'$ un homomorfismo de grupos biyectivo. Pruebe que la función inversa $f^{-1} : G' \to G$ es también un homomorfismo.

3.15 Pruebe, sin utilizar la Proposición 3.19, la afirmación del Corolario 3.20.

3.16 Demuestre que un homomorfismo de grupos $f\colon G \to G'$ es inyectivo si, y sólo si, $\ker f = \{e\}$.

3.17 En un grupo G pruebe que si un elemento x es idempotente $(x \cdot x = x)$ entonces $x = e$, donde e es el elemento de identidad de G. Utilice esto para probar que bajo un homomorfismo de grupos, el elemento de identidad del dominio es enviado bajo el homomorfismo al elemento de identidad del codominio.

3.18 Sea $f : G \to G'$ un homomorfismo de grupos. Pruebe que si $x \in G$ entonces $f(x^{-1}) = f(x)^{-1}$.

3.19 Sean X, Y y G grupos abelianos. Diremos que $f\colon X \times Y \to G$ es una función biaditiva, si $f(x_1 + x_2, y) = f(x_1, y) + f(x_2, y)$ y $f(x, y_1 + y_2) = f(x, y_1) + f(x, y_2)$ para $x, x_1, x_2 \in X$, $y, y_1, y_2 \in Y$. Pruebe que
(i) $f(\lambda x, y) = \lambda f(x, y) = f(x, \lambda y)$ para toda $x \in X, y \in Y)$ y $\lambda \in \mathbb{Z}$.
(ii)f nunca es inyectiva a menos que $X = Y = 0$.

3.20 Pruebe que el grupo $(\mathbb{Z}[x], +)$ es isomorfo al grupo $(\mathbb{Q}^+, \cdot)$.

3.21 Considere $Hom(X, Y)$ el conjunto de homomorfismos del grupo abeliano X en el grupo abeliano Y. Sean $f, g\colon X \longrightarrow Y$ homomorfismos de grupos abelianos y definamos $f + g\colon X \longrightarrow Y$ mediante $(f + g)(x) = f(x) + g(x)$. Pruebe que esta definición hace de $Hom(X, Y)$ un grupo abeliano.

3.22 Sea $\psi\colon Y' \longrightarrow Y$ un homomorfismo de grupos abelianos y $(X \xrightarrow{f} Y')$ un elemento de $Hom(X, Y')$. Asociemos a f un homomorfismo $(X \xrightarrow{g} Y) \in Hom(X, Y)$ mediante una función

$$\psi_* = Hom(X, \psi)\colon Hom(X, Y') \longrightarrow Hom(X, Y)$$

dada por $\psi_*(f) = \psi \circ f$. Pruebe que ψ_* es un homomorfismo de grupos abelianos.

3.23 Sea $\varphi\colon X' \longrightarrow X$ un homomorfismo de grupos abelianos y $(X \xrightarrow{g} Y) \in Hom(X,Y)$. Asociemos a g un homomorfismo $(X' \xrightarrow{f} Y) \in Hom(X',Y)$ mediante una función

$$\varphi^* = Hom(\varphi, Y)\colon Hom(X,Y) \longrightarrow (X',Y)$$

dada por $\varphi^*(g) = g \circ \varphi$. Pruebe que φ^* es un homomorfismo de grupos abelianos.

3.24 Sean $\psi\colon Y' \longrightarrow Y$ y $\psi'\colon Y \longrightarrow Y''$ homomorfismos de grupos abelianos y X un grupo abeliano. Pruebe que si $1_Y\colon Y \longrightarrow Y$ es la identidad, entonces $1_{Y_*}\colon Hom(X,Y) \longrightarrow Hom(X,Y)$ es la identidad de $Hom(X,Y)$, y $(\psi' \circ \psi)_* = \psi'_* \circ \psi_*$.

3.25 Sean $\varphi\colon X' \longrightarrow X$ y $\varphi'\colon X \longrightarrow X''$ homomorfismos de grupos abelianos y Y un grupo abeliano. Pruebe que si $1_X\colon X \longrightarrow X$ es la identidad, entonces $1_X^*\colon Hom(X,Y) \longrightarrow Hom(X,Y)$ es la identidad de $Hom(X,Y)$, y $(\varphi' \circ \varphi)^* = \varphi^* \circ \varphi'^*$.

I.4 Grupos Cíclicos

Consideremos un grupo multiplicativo $(G, \cdot)$ y las potencias de un elemento fijo $x \in G$, es decir, $\{x^n \mid n \in \mathbb{Z}\}$ donde definimos $x^0 = e$.

4.1 Proposición. El conjunto $\{x^n \mid n \in \mathbb{Z}\}$ denotado (x) es un subgrupo de G.

Demostración. Como $x^i x^j = x^{i+j}$, el producto de dos elementos del conjunto está en el conjunto y por lo tanto (x) es cerrado. Como $x^0 = e$, $e \in (x)$. Finalmente, para x^n, consideremos x^{-n}. Luego, $x^n x^{-n} = e$.♦

4.2 Definición. El subgrupo (x) lo llamaremos **subgrupo cíclico** de G generado por uno de sus elementos x y diremos que x es un **generador** de (x). Si $(x) = G$ diremos que G es un **grupo cíclico generado por** x.

Si para el subgrupo (x) no existe un número natural n tal que $x^n = e$ decimos que (x) es **cíclico infinito**. Si n es el natural más pequeño tal que $x^n = e$, entonces (x) consiste de los elementos $x^{n-1}, ...x^1, e = x^n$ y en este caso decimos que (x) es un **grupo cíclico de orden** n.

4.3 Ejemplo. $\mathbb{Z}$ y $\mathbb{Z}_n$ son grupos cíclicos, el primero infinito, y el segundo finito. También, $3\mathbb{Z} = (3)$ y en general, $n\mathbb{Z} = (n)$ son grupos cíclicos infinitos $n \in \mathbb{N}$. Observe que $(8) = 8\mathbb{Z} < (4) = 4\mathbb{Z} < (2) = 2\mathbb{Z}$.

4.4 Ejemplo. $(1) = (3) = \mathbb{Z}_4$, $(1) = (-1) = \mathbb{Z}$.

4.5 Proposición. Si G es un grupo cíclico, entonces es conmutativo o abeliano.

Demostración. Sea $(x) = G$. Entonces $x^m x^r = x^{m+r} = x^{r+m} = x^r x^m$. Luego, G es conmutativo o abeliano.♦

4.6 Definición. Sea G cualquier grupo y x un elemento de G. Sea r el número natural más pequeño tal que $x^r = e$, entonces decimos que x es de **orden** r. Si no existe un número natural r tal que $x^r = e$, decimos que x es de **orden infinito**.

Cuando consideremos grupos no abelianos utilizaremos la notación multiplicativa y cuando los grupos sean abelianos utilizaremos la notación aditiva, aunque por costumbre se usará la notación multiplicativa para los grupos cíclicos (los cuales son abelianos).

Tenemos las siguientes propiedades (conocidas como las leyes de los exponentes) en notación multiplicativa

$$x^n x^m = x^{n+m}, (x^n)^m = x^{nm}, x^{-n} = (x^n)^{-1}$$

y, en notación aditiva

$$nx + mx = (n+m)x, m(nx) = (mn)x, (-n)x = -(nx).$$

Si además, el grupo G es abeliano, se tiene

$$n(x+y) = nx + ny$$

Observe que (una vez resueltos los Problemas 4.2 y 4.3) para cada $n \in \mathbb{N}$ hay un grupo cíclico de orden n, $(n) = n\mathbb{Z}$. Observe también que si tenemos dos grupos cíclicos de orden n, al tomar sus generadores, podemos hacer una correspondencia biunívoca con cada potencia del generador de manera que tendríamos esencialmente un solo grupo cíclico de orden n. En otras palabras, dos grupos cíclicos del mismo orden son isomorfos, como veremos abajo.

4.7 Teorema. Sea $(G, \cdot)$ un grupo cíclico infinito. Entonces la función

$$h : \mathbb{Z} \longrightarrow G$$

dada por

$$n \longmapsto x^n$$

para un elemento fijo x de G es un isomorfismo de grupos.

Demostración. $h(n+m) = x^{n+m} = x^n x^m = h(n)h(m)$, luego h es un homomorfismo. Si $h(n) = x^n = x^m = h(m)$, entonces $n = m$. Luego h es inyectiva. Para cada $x^n \in G$, el entero n va a dar a x^n bajo h. Luego h es suprayectiva.♦

4.8 Teorema. Todo grupo cíclico finito de orden n con generador de orden n es isomorfo a $\mathbb{Z}_n$.

Demostración. Sea G un grupo cíclico de orden n. Sea x un generador de G tal que $x^n = e$. Definamos

$$h : \mathbb{Z}_n \longrightarrow G$$

dada por

$$[m] \longmapsto h([m]) = x^m.$$

Supongamos que $h([j]) = h([k])$, entonces $x^j = x^k$. Luego, $x^{j-k} = e$. Así, $j - k = rn$ y $n \mid j - k$. Por lo tanto, $[j] = [k]$ en $\mathbb{Z}_n$.O bien, supongamos que ker $h = \{[j]\}$. Entonces $h([j]) = e$. Luego $x^j = e = x^0$. Así, $[j] = [0]$ en $\mathbb{Z}_n$. Por lo tanto h es inyectiva. Es fácil ver que h está bien definida, es homomorfismo y es suprayectiva, (Problema 4.5).♦

4.9 Observación. Considere un grupo cíclico generado por un elemento x de orden n y q un entero tal que $n = mq$. Las distintas potencias de x, digamos

$$x^q, x^{2q}, x^{3q}, ..., x^{mq} = x^n = e,$$

forman un subgrupo cíclico de (x) de orden m.

También, si N es un subgrupo no trivial de (x) podemos tomar el menor entero positivo m tal que $x^m \in N$. Como $e = x^n = x^{mq}$, $m \mid n$ y (x) consta de $m = n/q$ elementos. Finalmente, si $o(G) = n$, entonces x^j es un generador de G si, y sólo si $(n, j) = 1$, (Problema 4.7).

4.10 Ejemplo. Considere $(\mathbb{Z}_{12}, +)$. Los generadores de $\mathbb{Z}_{12}$ son los elementos j tales que $(12, j) = 1$, esto es $j = 1, 5, 7$ y 11. Así, $\mathbb{Z}_{12} = (1) = (5) = (7) = (11)$. Las posibilidades para q y m en $12 = qm$ son 1 y 12, 2 y 6, 3 y 4, 4 y 3, 6 y 2, 12 y 1 respectivamente. Así, las distintas potencias de un generador x,

$$x^{1q}, x^{2q}, x^{3q}, ..., x^{mq} = x^{12} = 0$$

forman un subgrupo cíclico de (x) de orden m. Si tomamos $x = 1$ por facilidad de cálculo, obtendremos las potencias de 1: Para $q = 1$, $m = 12$, $\{1^{1\cdot 1}, 1^{2\cdot 1}, 1^{3\cdot 1}, ..., 1^{12\cdot 1} = 1^{12} = 0\}$ las cuales se convierten, en notación aditiva en $\{1 \cdot 1, 2 \cdot 1, 3 \cdot 1, ..., 12 \cdot 1 = 0\}$ que es precisamente $(1) = \mathbb{Z}_{12}$. De manera semejante, para $q = 2$, $m = 6$, obtenemos $\{1^{1\cdot 2}, 1^{2\cdot 2}, 1^{3\cdot 2}, ..., 1^{6\cdot 2} = 1^{12} = 0\}$ las cuales se convierten, en notación aditiva en $\{2 \cdot 1, 4 \cdot 1, 6 \cdot 1, ..., 12 \cdot 1 = 0\} = \{2, 4, 6, 8, 10, 0\} = (2)$. Para $q = 3$, $m = 4$, obtenemos $\{1^{1\cdot 3}, 1^{2\cdot 3}, 1^{3\cdot 3}, 1^{4\cdot 3} = 1^{12} = 0\}$ las cuales se convierten, en notación aditiva en $\{3 \cdot 1, 6 \cdot 1, 9 \cdot 1, 12 \cdot 1 = 0\} = \{3, 6, 9, 0\} = (3)$. Para $q = 4$, $m = 3$, obtenemos $\{1^{1\cdot 4}, 1^{2\cdot 4}, 1^{3\cdot 4} = 1^{12} = 0\}$ las cuales se convierten, en notación aditiva en $\{4 \cdot 1, 8 \cdot 1, 12 \cdot 1 = 0\} = \{4, 8, 0\} = (4)$. Para $q = 6$, $m = 2$, obtenemos $\{1^{1\cdot 6}, 1^{2\cdot 6} = 1^{12} = 0\}$ las cuales se convierten, en notación aditiva en $\{6 \cdot 1, 12 \cdot 1 = 0\} = \{6, 0\} = (6)$. Finalmente, para $q = 12$, $m = 1$, obtenemos $\{1^{1\cdot 12} = 0\}$ la cual se convierte, en notación aditiva en $\{12 \cdot 1 = 0\} = \{0\} = (0) = O$. Así, tenemos un diagrama de contención o red de subgrupos de $\mathbb{Z}_{12}$:

$$\begin{array}{ccccc}
 & & \mathbb{Z}_{12} = (1) & & \\
 & / & | & \backslash & \\
(2) & & | & & (3) \\
| & \backslash & | & & | \\
(4) & & | & & (6) \\
 & \backslash & & / & \\
 & & O & &
\end{array}$$

Problemas.

4.1 Sea $h : G \longrightarrow G'$ un homomorfismo de grupos multiplicativos. Pruebe que $h(x^n) = (h(x))^n$, $n \in \mathbb{Z}$.

4.2 Pruebe que los múltiplos de $\mathbb{Z}$, $n\mathbb{Z}$ con $n \in \mathbb{Z}$, son subgrupos de $\mathbb{Z}$.

4.3 Pruebe que todo subgrupo de $\mathbb{Z}$ es cíclico.

4.4 Pruebe que cualquier subgrupo de un grupo cíclico es cíclico. Sugerencia: utilice el Problema 4.2 para el caso infinito y la observación 4.9 para el caso finito.

4.5 Complete la demostración del Teorema 4.8.

4.6 Pruebe que solamente existen (salvo isomorfismo) un solo grupo de orden 1, 2 y 3; 2 grupos de orden 4 y 2 grupos de orden 6.

4.7 Sea G un grupo cíclico de orden n generado por x. Pruebe que x^j es un generador de G si, y sólo si $(n, j) = 1$.

4.8 Encuentre los subgrupos y la red de subgrupos para $(\mathbb{Z}_{18}, +)$, $(\mathbb{Z}_{24}, +)$ y $(\mathbb{Z}_{31}, +)$. ¿Qué puede intuir para $(\mathbb{Z}_p, +)$ con p primo?

.

Capítulo II

II.1 Sucesiones Exactas

En esta sección estudiaremos sucesiones finitas e infinitas de homomorfismos

$$\cdots \longrightarrow G' \xrightarrow{f} G \xrightarrow{g} G'' \longrightarrow \cdots$$

de grupos. Comenzaremos por estudiar sucesiones en las cuales el núcleo del homomorfismo "saliente" contiene a la imagen del homomorfismo "entrante".

1.1 Definición. Diremos que una sucesión de grupos

$$\cdots \longrightarrow G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \xrightarrow{f_{i+1}} \cdots$$

es **semiexacta** en G_i si $im\ f_{i-1} \subset \ker f_i$. Si es semiexacta en cada grupo, la llamaremos **sucesión semiexacta**.

Esta definición equivale, como a continuación veremos, a que la composición de los dos homomorfismos, el "entrante" y el "saliente", es el homomorfismo trivial. Denotaremos por abuso con e el elemento de identidad de cualquier grupo o bien con e_{G_i} para especificar la identidad del grupo G_i y con O el **morfismo trivial** o "**cero**".

1.2 Proposición. Una sucesión de grupos

$$\cdots \longrightarrow G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \xrightarrow{f_{i+1}} \cdots$$

es semiexacta en G_i si, y sólo si, la composición $f_i \circ f_{i-1} = O$.

Demostración. Supongamos que la sucesión es semiexacta en G_i. Entonces $im\ f_{i-1} \subset \ker f_i$. Veamos que la composición $[f_i \circ f_{i-1}](x) = O(x) = e_{G_{i+1}}$ para toda $x \in G_{i-1}$. Como $f_{i-1}(x) \in im\ f_{i-1} \subset \ker f_i$, tenemos que$f_i(f_{i-1}(x)) = e_{G_{i+1}} = O(x)$. Luego, como x es arbitraria, $f_i \circ f_{i-1} = O$. Ahora, supongamos que $f_i \circ f_{i-1} = O$. Sea $y \in im\ f_{i-1}$ arbitraria. Entonces existe $x \in G_{i-1}$ tal que $f_{i-1}(x) = y$. Entonces $f_i(y) = f_i(f_{i-1}(x)) = O(x) = e_{G_{i+1}}$, por lo que $y \in f_i^{-1}(e) = \ker f_i$. Hemos visto que, si $y \in im\ f_{i-1}$, entonces $y \in \ker f_i$ para cualquier y. Luego, $im\ f_{i-1} \subset \ker f_i$.♦

1.3 Definición. Diremos que una sucesión de grupos

$$\cdots \longrightarrow G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \xrightarrow{f_{i+1}} \cdots$$

es **exacta** en G_i si es semiexacta e $im\ f_{i-1} \supset \ker f_i$. Si es exacta en cada grupo, la llamaremos **sucesión exacta**.

Equivalentemente, dicha sucesión es exacta en G_i si, y sólo si, $im\ f_{i-1} = \ker f_i$. Toda sucesión exacta es semiexacta, pero no toda sucesión semiexacta es exacta. A una sucesión exacta de la forma

$$e \longrightarrow G' \xrightarrow{f} G \xrightarrow{g} G'' \longrightarrow e$$

la llamaremos **sucesión exacta corta**.

1.4 Ejemplo. Considere la sucesión

$$O \xrightarrow{h} \mathbb{Z}_2 \xrightarrow{f=\times 2} \mathbb{Z}_4 \xrightarrow{g} \mathbb{Z}_2 \xrightarrow{k} O.$$

Aquí, f está dada por $f(0) = 0$ y $f(1) = 2$; $g(0) = g(2) = 0$ y $g(1) = g(3) = 1$. Es fácil comprobar que f y g así definidos son homomorfismos de grupos. Es claro que $im\ h = \{0\} = \ker\ f$, $im\ f = \{0, 2\} = \ker\ g$, e $im\ g = \{0, 1\} = \ker\ k$. Luego, es una sucesión exacta corta.

1.5 Ejemplo. Considere la sucesión

$$O \xrightarrow{h} \mathbb{Z}_2 \xrightarrow{f} \mathbb{Z}_2 \times \mathbb{Z}_2 \xrightarrow{g} \mathbb{Z}_2 \xrightarrow{k} O.$$

Aquí, f está dada por $f(0) = (0, 0)$ y $f(1) = (1, 0)$; $g(0, 0) = g(1, 0) = 0$ y $g(0, 1) = g(1, 1) = 1$. Es fácil comprobar que f y g así definidos son homomorfismos de grupos. Es claro que $im\ h = \{0\} = \ker\ f$, $im\ f = \{(0, 0), (1, 0)\} = \ker\ g$, e $im\ g = \{0, 1\} = \ker\ k$. Luego, es una sucesión exacta corta.

A menudo suprimiremos $\circ$ de la notación $g \circ f$ y simplemente escibiremos gf. Consideremos una sucesión exacta de grupos

$$H' \xrightarrow{f} H \xrightarrow{g} G \xrightarrow{h} G''$$

con f epimorfismo y h monomorfismo. Entonces $im\ f = H$ y $\ker h = e$. Como la sucesión es exacta, $H = im\ f = \ker g$ e $im\ g = \ker h = e$; luego, g es el homomorfismo trivial. Inversamente, si g es el homomorfismo trivial, entonces f es epimorfismo y h es monomorfismo. Por lo tanto, tenemos la siguiente

1.6 Proposición. Si

$$H' \xrightarrow{f} H \xrightarrow{g} G \xrightarrow{h} G''$$

es una sucesión exacta de grupos, h es un monomorfismo si, y sólo si, g es trivial; g es trivial si, y sólo si, f es epimorfismo.

Así, cuando tenemos una sucesión exacta corta de la forma

$$e \longrightarrow G' \xrightarrow{f} G \xrightarrow{g} G'' \longrightarrow e$$

la escribiremos indistintamente como

$$G' \overset{f}{\rightarrowtail} G \overset{g}{\twoheadrightarrow} G''$$

donde $\rightarrowtail$ denota inyectividad y $\twoheadrightarrow$ suprayectividad.

1.7 Definición. Sean G, G', H, H' grupos, con f, f', g, g' homomorfismos de grupos. Decimos que el **diagrama**

$$\begin{array}{ccc} G & \xrightarrow{f'} & H \\ g' \downarrow & & \downarrow f \\ G' & \xrightarrow{g} & H' \end{array}$$

conmuta si $f \circ f' = g \circ g' \colon G \longrightarrow H'$.

1.8 Proposición. Sean $G' \overset{f'}{\rightarrowtail} G \overset{f}{\twoheadrightarrow} G''$ y $H' \overset{g'}{\rightarrowtail} H \overset{g}{\twoheadrightarrow} H''$ dos sucesiones exactas cortas, y supongamos que, en el siguiente diagrama conmutativo

$$\begin{array}{ccccc} G' & \overset{f'}{\rightarrowtail} & G & \overset{f}{\twoheadrightarrow} & G'' \\ \downarrow h' & & \downarrow h & & \downarrow h'' \\ H' & \overset{g'}{\rightarrowtail} & H & \overset{g}{\twoheadrightarrow} & H'' \end{array}$$

dos de los tres homomorfismos h', h, h'' son isomorfismos. Entonces el tercero es también isomorfismo.

Demostración. Supongamos que h' y h'' son isomorfismos. Veamos que h es monomorfismo: sea $x \in \ker h$; entonces $gh(x) = g(e_H) = h''f(x) = e_{H''}$. Como h'' es isomorfismo, entonces $f(x) = e_{G''}$. Por lo tanto, existe $x' \in G'$ tal que $f'(x') = x$, por ser exacta la sucesión superior. Entonces $hf'(x') = h(x) = e_H = g'h'(x')$. Como $g'h'$ es inyectiva, entonces $x' = e_G$. Luego, $f'(x') = x = e_G$.

Ahora veamos que h es epimorfismo: Sea $y \in H$. Como h''es un isomorfismo, existe $x'' \in G''$ tal que $g(y) = h''(x'')$. Como f es suprayectiva, existe $z \in G$ tal que $f(z) = x''$. Luego,

$$g(y - h(z)) = g(y) - gh(z) = g(y) - h''f(z) = g(y) - h''(x'') = g(y) - g(y) = e_{H''}.$$

Por lo tanto, $y - h(z) \in \ker g$. Como la sucesión inferior es exacta, existe $y' \in H'$ con $g'(y') = y - h(z)$. Como h' es isomorfismo, existe $x' \in G'$ tal que $h'(x') = y'$. Luego

$$h(f'(x') + z) = hf'(x') + h(z) = g'h'(x') + h(z) = g'(y') + y - g'(y') = y.$$

Si definimos $x = f'(x') + z$, tendremos que $h(x) = y$. Los otros dos casos posibles los dejamos como ejercicio, véase el Problema 1.6.♦

Observemos que la proposición anterior establece los isomorfismos sólo cuando existe la función $h\colon G \longrightarrow H$ compatible con los isomorfismos dados y el diagrama conmuta. Por ejemplo, si consideramos el siguiente diagrama

$$\begin{array}{ccccccccc} e & \longrightarrow & Z_2 & \xrightarrow{\times 2} & Z_4 & \longrightarrow & Z_2 & \longrightarrow & e \\ \shortparallel & & \shortparallel & & & & \shortparallel & & \shortparallel \\ e & \longrightarrow & Z_2 & \longrightarrow & Z_2 \times Z_2 & \longrightarrow & Z_2 & \longrightarrow & e \end{array}$$

hemos visto que $Z_2 \times Z_2$ no es isomorfo a Z_4.

Sea $\{C_n\}_{n \in Z}$ una familia de grupos abelianos y $\{\partial_n : C_n \longrightarrow C_{n-1}\}_{n \in \mathbb{Z}}$ una familia de homomorfismos de grupos abelianos tales que $\partial_n \circ \partial_{n+1} = 0$. Llamaremos **complejo de cadenas** (o **cadena**) a la pareja $C = \{C_n, \partial_n\}$, y lo escribimos

$$C : \cdots \longrightarrow C_{n+1} \xrightarrow{\partial_{n+1}} C_n \xrightarrow{\partial_n} C_{n-1} \longrightarrow \cdots$$

Dicho de otra manera, un complejo de cadenas (o cadena), es una sucesión semiexacta descendente de grupos abelianos con índices en $\mathbb{Z}$.

Sean $C = \{C_n, \partial_n\}$ y $D = \{D_n, \partial'_n\}$ dos complejos de cadenas de grupos abelianos. Un **morfismo de cadenas** $\varphi : C \longrightarrow D$ es una familia de homomorfismos de grupos abelianos $\{\varphi_n : C_n \longrightarrow D_n\}$ tal que los cuadrados, en el siguiente diagrama conmutan:

$$\begin{array}{ccccccccccc} C: & \cdots & \xrightarrow{\partial_{n+2}} & C_{n+1} & \xrightarrow{\partial_{n+1}} & C_n & \xrightarrow{\partial_n} & C_{n-1} & \xrightarrow{\partial_{n-1}} & \cdots \\ \downarrow\varphi & & & \downarrow\varphi_{n+1} & & \downarrow\varphi_n & & \downarrow\varphi_{n-1} & & \\ D: & \cdots & \xrightarrow{\partial'_{n+2}} & D_{n+1} & \xrightarrow{\partial'_{n+1}} & D_n & \xrightarrow{\partial'_n} & D_{n-1} & \xrightarrow{\partial'_{n-1}} & \cdots \end{array}$$

Problemas.

1.1 Defina homomorfismos adecuados para que, para un número primo p, las sucesiones

$$O \longrightarrow \mathbb{Z}_p \longrightarrow \mathbb{Z}_{p^2} \longrightarrow \mathbb{Z}_p \longrightarrow O$$

$$O \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}_p \longrightarrow O$$

sean exactas cortas.

1.2 Pruebe que, en una sucesión exacta de grupos

$$G' \xrightarrow{f} G \xrightarrow{g} G'' \xrightarrow{h} H \xrightarrow{k} H'$$

f es un epimorfismo y k un monomorfismo si, y sólo si, $G'' = e$.

1.3 Pruebe que, si $e \longrightarrow G \longrightarrow e$ es una sucesión exacta de grupos, entonces $G = e$.

1.4 Sea

$$G' \xrightarrow{f} G \xrightarrow{g} G'' \xrightarrow{h} H' \xrightarrow{k} H \xrightarrow{q} H''$$

una sucesión exacta de grupos. Pruebe que g, k son homomorfismos triviales si, y sólo si, h es isomorfismo, y que h es isomorfismo si, y sólo si, f es epimorfismo y q monomorfismo.

1.5 Pruebe que, si

$$e \longrightarrow H' \xrightarrow{h} G \longrightarrow e$$

es una sucesión exacta de grupos entonces h es un isomorfismo.

1.6 Pruebe los dos casos restantes de la Proposición 1.8.

1.7 Sea $\{C^n\}_{n\in Z}$ una familia de grupos abelianos y $\{\delta^n : C^n \longrightarrow C^{n+1}\}_{n\in\mathbb{Z}}$ una familia de homomorfismos de grupos abelianos tales que $\delta^{n+1} \circ \delta^n = 0$. Llamaremos **complejo de cocadenas** (o **cocadena**) a la pareja $C = \{C^n, \partial^n\}$, y lo escribimos

$$C : \cdots \longrightarrow C^{n-1} \xrightarrow{\delta^{n-1}} C^n \xrightarrow{\delta^n} C^{n+1} \xrightarrow{\delta^{n+1}} \cdots$$

Dicho de otra manera, un complejo de cocadenas (o cocadena), es una sucesión semiexacta ascendente de grupos abelianos con índices en $\mathbb{Z}$. Defina el concepto de **morfismo de cocadenas** $\Psi : C \longrightarrow D$.

II.2 Grupos Cociente

Consideremos el primer ejemplo de la sección 1. Ahí repartimos los números enteros en tres cajas donde ningún entero está en dos o más cajas, solamente está en una sola caja. Etiquetamos las cajas con tres etiquetas. Al conjunto de cajas le dimos una estructura de grupo definiéndole una operación binaria. El lector comprobó que efectivamente es un grupo conmutativo. A las cajas las llamaremos **clases laterales** y al grupo lo llamaremos **grupo cociente**. En este caso es el cociente de $\mathbb{Z}$ "módulo" $3\mathbb{Z}$, el cual denotamos $\mathbb{Z}_3$.

Recordando el concepto de espacio vectorial cociente estudiado en el curso de Álgebra Lineal (ver Ll2) y considerando la parte aditiva se tenía que para el caso en que G es un grupo conmutativo y H un subgrupo de G con $x \in G$, denotábamos con $x+H$ el conjunto $\{x+y|y \in H\}$. Dichos elementos $x+H$ los llamamos **clases laterales** de H en G. Como $0 \in H$ y $x = x+0 \in x+H$, cada $x \in G$ pertenece a una clase lateral. Se comprobó que cualesquiera dos clases laterales son ajenas o son iguales. Se denotó con G/H el conjunto de todas las clases laterales de H en G y se le dio a G/H una estructura de grupo mediante

$$+\colon G/H \times G/H \to G/H$$

dada por

$$((x+H),(y+H)) \longmapsto ((x+y)+H)$$

También se comprobó que la operación binaria anterior está bien definida y que define una estructura de grupo abeliano (la parte aditiva de espacio vectorial) en G/H. Llamamos a G/H, **grupo cociente** de G módulo H.

También, se vio que si H es un subgrupo del grupo G y si $y \in x+H$, entonces existe $w \in H$ tal que $y = x+w$. Así $y-x = w \in H$. Luego, si $y-x \in H$ entonces $y-x = w \in H$. Entonces $y = x+w \in x+H$. También $y-x \in H \iff -(y-x) = x-y \in H \iff x \in y+H$. En resumen,

$$y \in x+H \iff y-x \in H \iff x \in y+H$$

Finalmente, se consideró $p\colon G \to G/H$ dada por $x \longmapsto x+H$. Si $x, w \in G$, entonces

$$p(x+w) = (x+w)+H = (x+H)+(w+H) = p(x)+p(w).$$

Por lo tanto, p es un homomorfismo llamado **proyección canónica**.

Todo esto se realizó para espacios vectoriales sobre un campo K. Recuérdese de nuevo que la parte aditiva es un grupo conmutativo.

Pero para el caso no conmutativo ¿qué sucede? Imitaremos todo lo anterior y lo adecuaremos a la situación no conmutativa. Para comenzar, considere de nuevo el primer ejemplo de la sección 1. Ahí se tomó una relación de equivalencia llamada congruencia módulo 3, donde $x \equiv y \ (mod\ 3)$ sí, y sólo si $3 \mid -x+y$, o bien, dicho de otra manera, que $-x+y \in 3\mathbb{Z}$. Lo que haremos es generalizar esta relación de equivalencia al caso en que tengamos un grupo no abeliano utilizando notación multiplicativa como sigue:

2.1 Definición. Consideremos un subgrupo H de un grupo $(G, \cdot)$ y elementos $x, y \in G$. Diremos que x es **congruente por la izquierda con** y si $x^{-1}y \in H$ (es decir, si $y = xh$ para alguna $h \in H$) y la denotamos con $x \equiv_i y$ $(mod\ H)$. Análogamente, diremos que x es **congruente por la derecha con** y si $xy^{-1} \in H$ y la denotamos con $x \equiv_d y \ (mod\ H)$.

Observe que para el caso abeliano, los conceptos de congruencia izquierda y derecha coinciden pues $x^{-1}y \in H$ sí, y sólo si, $(x^{-1}y)^{-1} = y^{-1}x = xy^{-1} \in H$.

2.2 Proposición. Las relaciones de congruencia izquierda y derecha son relaciones de equivalencia.

Demostración. Como $x \equiv_i x \ (\text{mod } H) \iff x^{-1}x = e \in H$, se tiene la reflexibilidad. Como $x \equiv_i y \ (mod\ H) \iff x^{-1}y \in H \iff (x^{-1}y)^{-1} \in H \iff y^{-1}x \in H \iff y \equiv_i x \ (mod\ H)$ se tiene la simetría. Finalmente, si $x \equiv_i y \ (mod\ H)$ y $y \equiv_i z \ (mod\ H)$ entonces $x^{-1}y \in H$ y $y^{-1}z \in H$. Luego $(x^{-1}y)(y^{-1}z) \in H \iff x^{-1}ez = x^{-1}z \in H$ Así $x \equiv_i z \ (mod\ H)$ y se tiene la transitividad. Análogamente para la congruencia derecha.⧫

2.3 Proposición. Las clases de equivalencia izquierdas y derechas $[x]$ de la relación definida arriba son de la forma

$$xH = \{xh \mid h \in H\}$$

y

$$Hx = \{hx \mid h \in H\}$$

respectivamente.

Demostración. Las clases de equivalencia de cualquier elemento x de G son de la forma (utilizando la simetría):

$$\begin{aligned}
[x] &= \{y \in G \mid y \equiv_i x \ (mod\ H)\} \\
&= \{y \in G \mid x \equiv_i y \ (mod\ H)\} \\
&= \{y \in G \mid x^{-1}y = h \in H\} \\
&= \{y \in G \mid y = xh; h \in xH\} \\
&= \{xh \mid h \in H\} = xH.
\end{aligned}$$

Análogamente para las clases de equivalencia bajo la relación de congruencia módulo H derechas.⧫

Observe que un grupo G es unión de sus clases laterales izquierdas o derechas de H en G. También, observe que dos clases laterales o son ajenas o son iguales. Las clases de equivalencia xH y Hx las llamaremos **clases laterales izquierdas y derechas** respectivamente.

Consideremos el conjunto de todas las clases laterales izquierdas y denotémoslo con G/H. Deseamos darle a este conjunto una estructura de grupo y hacer de la **proyección natural o canónica** $p : G \longrightarrow G/H$ un homomorfismo. Esto no siempre es posible pero veamos a continuación cuando sí lo es.

2.4 Definición. Diremos que el subgrupo H de G es **normal** en G (denotado $H \lhd G$) si para toda $x \in G$, $xHx^{-1} \subset H$ donde $xHx^{-1} = \{xhx^{-1} \mid h \in H\}$.

En esta definición, puesto que $xHx^{-1} \subset H$ vale para todo elemento $x \in G$, en particular vale para $x^{-1} \in G$. Luego, $x^{-1}Hx \subset H$. Así, para toda $h \in H$, $h = x(x^{-1}hx)x^{-1} \in xHx^{-1}$. Luego $H \subset xHx^{-1}$ y $xHx^{-1} = H$. De aquí es fácil ver que toda clase lateral izquierda es derecha y que $xH = Hx$ para toda $x \in G$ (Problema 2.4). También observe que todo subgrupo de un grupo abeliano es normal y que los subgrupos triviales son normales en G (Problema 2.5).

2.5 Proposición. Un subgrupo H de G es normal si, y sólo si, $(xH)(yH) = (xy)H$ para todo $x, y \in G$.

Demostración. Supongamos que H es normal y tomemos dos elementos cualesquiera $x, y \in G$. Es fácil ver que $(xH)(yH) = (xyH)$ Problema 2.9. Ahora, supongamos que $(xH)(yH) = (xy)H$ para todo $x, y \in G$. Sean $h \in H$ y $x \in G$ arbitrarios. Entonces

$$xhx^{-1} = (xh)(x^{-1}e) \in (xH)(x^{-1}H) = eH = H,$$

por lo tanto, H es normal.♦

2.6 Teorema. Sea H un subgrupo normal de G. Entonces G/H es un grupo con operación binaria

$$\cdot : G/H \times G/H \longrightarrow G/H$$

dada por

$$((xH),(yH)) \mapsto \cdot((xH),(yH)) = (xH) \cdot (yH) = (xH)(yH) = (xy)H.$$

Además, la proyección canónica $p : G \longrightarrow G/H$ es un epimorfismo cuyo núcleo es H, i.e. $\ker p = H$.

Demostración. Es inmediato comprobar que G/H cumple las axiomas de grupo con $eH = H$ como elemento de identidad y $x^{-1}H$ como inverso de xH.

Como $p(xy) = (xy)H = (xH)(yH) = p(x)p(y)$ y p es suprayectiva, entonces es un epimorfismo. Finalmente,

$$\begin{aligned}\ker(p) &= \{x \in G \mid p(x) = eH = H\} = \\ &= \{x \in G \mid xH = H\} = \{x \in G \mid x \in H\} \\ &= H.\blacklozenge\end{aligned}$$

2.7 Corolario. Si $H \lhd G$ entonces H es el núcleo de un homomorfismo g de G en G' para un grupo G', i.e. $H = \ker(g : G \longrightarrow G')$ para un grupo G'.

Demostración. Como H es normal, entonces es el núcleo de un epimorfismo como en el teorema anterior.♦

2.8 Proposición. Si $H = \ker(g : G \longrightarrow G')$ para un grupo G' entonces $H \lhd G$.

Demostración. Sean $h \in H$ y $x \in G$ arbitrarios. Entonces

$$g(xhx^{-1}) = g(x)g(h)g(x^{-1}) = g(x)eg(x^{-1}) = g(x)(g(x))^{-1} = e$$

Luego, $xhx^{-1} \in \ker(g : G \longrightarrow G') = H$.♦

Por el corolario y proposición anteriores, la condición de normalidad es necesaria y suficiente para tener el concepto de grupo cociente.

2.9 Teorema. (**Lagrange**) Si G es un grupo de orden n y $H < G$, entonces $o(H) \mid o(G)$.

Demostración. Como G es unión de sus clases laterales izquierdas, el número de elementos n de G, es igual al producto del número de clases laterales izquierdas r por el número de elementos de cada clase $m = o(H)$ ya que las clases laterales de H tienen el mismo número de elementos m (Problema 2.2) y o son ajenas o son iguales. Así, $n = rm$, es decir, $o(H) \mid o(G)$.♦

Al número de clases laterales izquierdas (o derechas) de un subgrupo $H < G$ lo denotaremos $(G : H)$ y lo llamaremos **índice** *de* H *en* G, es decir, $(G : H) = o(G/H)$. Por el Problema 2.4, el índice de H en G no depende de si se consideran clases laterales izquierdas o derechas. Puede ser finito o infinito. Claramente, como cada clase lateral tiene $o(H)$ elementos, $(G : H) = o(G)/o(H)$.

2.10 Corolario. Si el orden de un grupo G es primo, entonces G es cíclico.

Demostración. Sea $p = o(G)$ y (x) el subgrupo cíclico generado por el elemento $x \neq e \in G$. Por el teorema de Lagrange $2 \leq o((x)) \mid p$. Luego, $o((x)) = p$ y por lo tanto $(x) = G$ y G es cíclico.♦

Del corolario anterior se desprende que existe uno, y solamente un grupo (salvo isomorfismo) de orden primo. Observe que un grupo de orden primo no puede tener subgrupos propios no triviales. Los subgrupos triviales G y e son normales en G. Así, G/G es el grupo trivial e y G/e es isomorfo a G. Diremos que un grupo G es **simple** si sus únicos subgrupos normales son los triviales. Se sabe que el grupo alternante A_n es simple para $n \geq 5$ como veremos en el siguiente capítulo.

Finalmente tenemos el siguiente

2.11 Teorema. Sea (x) un grupo cíclico generado por x y $h : (x) \longrightarrow H$ un homomorfismo de grupos. Entonces $im\ h = h((x))$ es un subgrupo cíclico de H.

Demostración. Supongamos que (x) es de orden n. Si h es un homomorfismo y x genera (x), como $h(x^r) = [h(x)]^r$ (Problema 2.13), $h(x)$ genera $im\ h$ pues $h(e) = (h(x^n) = [h(x)]^n = e$.♦

Sea $C = \{C_n, \partial_n\}$ un complejo de cadenas o cadena. El **grupo de homología de grado** n **de** C, $H_n(C)$ se define como el cociente $H_n(C) = \ker \partial_n / im\ \partial_{n+1}$. Es decir, dada una cadena

$$C : \cdots \longrightarrow C_{n+1} \xrightarrow{\partial_{n+1}} C_n \xrightarrow{\partial_n} C_{n-1} \longrightarrow \cdots$$

consideramos el núcleo de $\partial_n, \ker \partial_n \subset C_n$, y la imagen de $im\ \partial_{n+1} \subset C_n$, y formamos el cociente $\ker \partial_n / im\ \partial_{n+1}$. Nótese que C es una sucesión semiexacta, es decir, $im\ \partial_{n+1} \subset \ker \partial_n$, y que el cociente $H_n(C) = \ker \partial_n / im\ \partial_{n+1}$ nos mide la inexactitud de C. Efectivamente, si C es exacta, entonces $im\ \partial_{n+1} = \ker \partial_n$ y $H_n(C) = 0$.

Los elementos de C_n se conocen como **cadenas de grado** n, y los homomorfismos ∂_n se llaman **diferenciales** u **operadores frontera**. Los elementos del núcleo de ∂_n se denominan **ciclos de grado** n, denotados con $Z_n(C)$ y los elementos de la imagen de ∂_{n+1} se llaman **fronteras de grado** n, denotados con $B_n(C)$. Así, $H_n(C) = Z_n(C)/B_n(C)$.

Diremos que dos elementos de $H_n(C)$ son **homólogos** si pertenecen a la misma clase lateral. El elemento de $H_n(C)$, determinado por el ciclo c de grado n, se llama **clase de homología de** c y se denota con $[c]$. Entonces, para cada $n \in Z$, definimos un grupo de homología $H_n(C)$. Denominamos a $H_*(C) = \{H_n(C)\}$ **homología de la cadena** C.

Problemas.

2.1 Pruebe que la relación de congruencia derecha es una relación de equivalencia.

2.2 Demuestre que todas las clases laterales de un subgrupo H de un grupo G tienen el mismo número de elementos, es decir $o(xH) = o(H) = o(Hx)$ para toda $x \in G$.

2.3 Encuentre todas las clases laterales para el subgrupo $H = \{0, 3\}$ de Δ_3 de los movimientos rígidos de un triángulo equilátero.

2.4 Pruebe que si $xHx^{-1} = H$, toda clase lateral izquierda es derecha y que $xH = Hx$ para toda $x \in G$. Concluya que esto último implica que, para toda $x \in G$, $xHx^{-1} \subset H$.

2.5 Pruebe que todo subgrupo de un grupo abeliano es normal.

2.6 Pruebe que bajo un homomorfismo de grupos, la imagen homomórfica de un subgrupo normal es normal en la imagen.

2.7 Pruebe que bajo un homomorfismo, la imagen inversa de un subgrupo normal es un subgrupo normal en el dominio.

2.8 Establezca el que un grupo G es unión de sus clases laterales izquierdas o derechas de H en G y que dos clases laterales o son ajenas o son iguales.

2.9 Compruebe que $(xH)(yH) = (xyH)$ en la demostración de 2.5.

2.10 Pruebe que el orden de un elemento x de un grupo finito G divide al orden del grupo.

2.11 Pruebe que si N, H, G son grupos tales que $N < H < G$, entonces $(G : N) = (G : H)(H : N)$ y que si dos de éstos índices son finitos, entonces el tercero también lo es.

2.12 Pruebe que un grupo cociente de un grupo cíclico es cíclico.

2.13 Pruebe que $h(x^r) = [h(x)]^r$, en la demostración del último teorema de esta sección.

2.14 En un grupo G, un elemento de la forma $xyx^{-1}y^{-1}$ se llama **conmutador**. Pruebe que el conjunto de conmutadores genera un subgrupo normal de G, denotado con G' y que el cociente G/G' es abeliano.

2.15 Sea $C = \{C^n, \delta^n\}$ un complejo de cocadenas. Defina el **grupo de cohomología de grado n de C**, $H^n(C)$.

II.3 Teoremas de Isomorfismo

3.1 Definición. Un **automorfismo** de un grupo G es un isomorfismo de G en G.

Para cada elemento $x \in G$, la función

$$\begin{array}{ll} \iota_x: & G \longrightarrow G \text{ dado por} \\ & y \mapsto xyx^{-1} \end{array}$$

es un automorfismo de G, ver Problema 3.1, llamado **automorfismo interior**. En éstos términos podemos decir que H es un subgrupo normal (o invariante) si, y sólo si, H es invariante bajo cada automorfismo interior de G.

3.2 Proposición. Sean $H \lhd G$ y $H' \lhd G'$. Considérense las proyecciones canónicas a los cocientes correspondientes $p: G \longrightarrow G/H$ y $p': G' \longrightarrow G'/H'$. Si $g: G \longrightarrow G'$ es un homomorfismo de grupos tal que $g(H) \subset H'$, entonces $g^*: G/H \longrightarrow G'/H'$ dado por $xH \mapsto g^*(xH) = g(x)H'$ está bien definido y es un homomorfismo de grupos llamado **homomorfismo inducido por** g **en los grupos cociente**. También, el siguiente cuadrado es conmutativo

$$\begin{array}{ccc} G & \xrightarrow{g} & G' \\ \downarrow^{p} & & \downarrow^{p'} \\ G/H & \xrightarrow{g^*} & G'/H' \end{array}$$

e $im\ g^* = p'(im\ g)$ y $\ker g^* = p(g^{-1}(H'))$.

Demostración. Si $x \in G$ y $y \in H$ son arbitrarios, puesto que $g(xy) = g(x)g(y) \in g(x)g(H) \subset g(x)H'$, la imagen de xH bajo g está contenida en una única clase lateral de H', digamos $g(xH) \subset g(x)H'$. Luego, definamos

$$\begin{array}{llll} g^*: & G/H & \longrightarrow & G'/H' \text{ mediante} \\ & xH & \mapsto & g^*(xH) = g(x)H' \end{array}$$

Es inmediato comprobar que g^* está bien definido y para probar que es un homomorfismo, considere cualesquiera clases laterales xH y $x'H$. Entonces,

$$\begin{array}{ll} & g^*((xH)(x'H)) \\ = & g^*((xx')H)) \\ = & g(xx')H' \\ = & (g(x)g(x'))H' \\ = & (g(x)H')(g(x')H') \\ = & g^*(xH)g^*(x'H). \end{array}$$

Veamos que el cuadrado conmuta: consideremos cualquier elemento x de G. Entonces $(p' \circ g)(x) = p'(g(x)) = g(x)H' = g^*(xH) = g^*(p(x)) = (g^* \circ p)(x)$. Luego $(p' \circ g) = (g^* \circ p)$. También, como p y p' son epimorfismos, claramente $im\ g^* = p'(im\ g)$ y $\ker\ g^* = p(g^{-1}(H'))$.♦

3.3 Teorema. Bajo las mismas hipótesis de la proposición anterior, en particular, si g es un epimorfismo con $H' = e$ y $H = \ker\ g$ entonces $G'/H' \cong G'$ y g^* es un isomorfismo en el siguiente diagrama conmutativo:

$$\begin{tikzcd} G \arrow[r, two heads, "g"] \arrow[d, "p"] & G' \arrow[d, "I_{G'}", "\cong"'] \\ G/\ker\ g \arrow[r, "g^*"] & G' \end{tikzcd}$$

Demostración. Si g es un epimorfismo con $H' = e$ y $H = \ker\ g$ entonces $G' = G'/H'$ y g^* es un isomorfismo pues como $\ker\ g^* = p(g^{-1}(e)) = p(\ker g) = p(H) = eH = e_{G/H} = e$, entonces g^* es monomorfismo y como $im\ g^* = p'(im\ g) = G'$ entonces g^* es epimorfismo y por lo tanto es isomorfismo.

Así, se tiene el siguiente diagrama conmutativo:

$$\begin{tikzcd} G \arrow[r, two heads, "g"] \arrow[d, "p"] & G' \arrow[d, "I_{G'}", "\cong"'] \\ G/\ker\ g \arrow[r, "g^*"] & G' \end{tikzcd}$$

♦

3.4 Teorema. Sean $H \lhd G$ y, como caso particular del teorema anterior, $e = H' \lhd G'$ con $H \subset \ker g$. Entonces existe un homomorfismo único $g^* : G/H \longrightarrow G'$ dado por $xH \mapsto g^*(xH) = g(x)H' = g(x)$. Además, $\ker g^* = \ker g/H$ e $im\ g = im\ g^*$. g^* es un isomorfismo si, y sólo si, g es un epimorfismo y $H = \ker g$.

Demostración. Por el teorema anterior, g es un homomorfismo. Es único puesto que está determinado por g. También, $xH \in \ker g^*$ sí, y sólo si $g(x) = e$, lo cual sucede si, y sólo si $x \in \ker g$. Así, $\ker g^* = \{xH \mid x \in \ker g\} = \ker g/H$. Claramente $im\ g = im\ g^*$. Finalmente, g^* es un epimorfismo si, y sólo si g es un epimorfismo y g^* es monomorfismo si, y sólo si $\ker g^* = \ker g/H$ es el subgrupo trivial de G/H lo cual sucede cuando $\ker g = H$.♦

3.5 Corolario. (**Primer Teorema de Isomorfismo**). Bajo las mismas hipótesis del teorema anterior $G/\ker\, g \cong im\ g$.

Demostración. Como g es epimorfismo, $im\ g = G'$, luego $G/\ker\, g \cong im\ g$.♦

En otras palabras, si $g : G \twoheadrightarrow G'$ es un epimorfismo de grupos con núcleo ker g, entonces existe un isomorfismo único $g^* : G/\ker\, g \cong G'$, tal que $g = g^* \circ p$, es decir, cualquier homomorfismo de G con núcleo ker g tiene imagen isomórfica a $G/\ker\, g$. Además, nos dice que cualquier epimorfismo $g : G \twoheadrightarrow G'$ tiene por codominio un grupo cociente, es decir el codominio de g es el cociente del dominio de g entre el núcleo de g. Aún más, nos dice cuál isomorfismo: aquel tal que $im\ g = im\ g^*$. Este resultado, $G/\ker\, g \cong im\ g$ se conoce como el **Primer Teorema de Isomorfismo**. Dado un grupo y un subgrupo normal se puede "determinar" cuál es el grupo cociente sin necesidad de establecer las clases laterales como veremos más adelante.

3.6 Ejemplo. Sea H un subgrupo normal de un grupo G. Consideremos el grupo cociente G/H. Sea $i\colon H \longrightarrow G$ el monomorfismo de inclusión y $p\colon G \longrightarrow G/H$ el epimorfismo de proyección. Entonces $im\ i = H = \ker\ p$ y, por lo tanto,

$$e \longrightarrow H \xrightarrow{i} G \xrightarrow{p} G/H \longrightarrow e$$

es una sucesión exacta corta. Consideremos ahora una sucesión exacta corta

$$e \xrightarrow{h} G' \xrightarrow{f} G \xrightarrow{g} G'' \xrightarrow{k} e.$$

Entonces $im\ f = \ker g$, f es monomorfismo (pues $e = im\ h = \ker f$) y, además, g es epimorfismo (pues $im\ g = \ker k = G''$). Sea $H = im\ f = \ker g$ el cual es un subgrupo normal de G, entonces f establece un isomorfismo $H \xrightarrow{\cong} G'$ y g establece otro isomorfismo $G/H \xrightarrow{\cong} G''$ por el primer teorema de isomorfismo. Por lo tanto, una sucesión exacta corta es una sucesión con un subgrupo y el grupo cociente de un grupo.

3.7 Ejemplo. $g : G \twoheadrightarrow G'$ donde $G = \mathbb{Z}$ y $G' = \mathbb{Z}_n$ es un epimorfismo con núcleo el subgrupo $n\mathbb{Z}$, es decir,

$$e \longrightarrow n\mathbb{Z} \longrightarrow \mathbb{Z} \xrightarrow{g} \mathbb{Z}_n \longrightarrow e$$

es un sucesión exacta corta. Luego, por el teorema anterior $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

3.8 Ejemplo. Sea G es el grupo multiplicativo de los números reales distintos de cero $\mathbb{R}^*$ y G' es el grupo multiplicativo de los reales positivos $\mathbb{P}^*$. Considere el epimorfismo $g : G \twoheadrightarrow G'$ dado por $x \mapsto g(x) = \mid x \mid$ donde $\mid x \mid$ denota el valor absoluto de x. El núcleo de g es $\{\pm 1\}$. Entonces la sucesión

$$e \longrightarrow \{\pm 1\} \longrightarrow \mathbb{R}^* \xrightarrow{g} \mathbb{P}^* \longrightarrow e$$

es exacta. Por el teorema anterior, el grupo cociente $\mathbb{R}^*/\{\pm 1\}$ es isomorfo a $\mathbb{P}^*$.

3.9 Ejemplo. Sea G es el grupo aditivo de los números reales $\mathbb{R}$ y G' es el grupo multiplicativo de los números complejos $\mathbb{S}^1$ con valor absoluto igual a 1. Sea $g : G \twoheadrightarrow G'$ el epimorfismo dado por $\theta \mapsto g(\theta) = e^{2\pi i\theta}$. Su núcleo es $\mathbb{Z}$. Entonces la sucesión

$$e \longrightarrow \mathbb{Z} \longrightarrow \mathbb{R} \xrightarrow{g} \mathbb{S}^1 \longrightarrow e$$

es exacta y por el teorema anterior, $\mathbb{R}/\mathbb{Z} \cong \mathbb{S}^1$.

Generalizaremos el concepto de clase lateral:

3.10 Definición. Sean H y N cualesquiera subgrupos de un grupo G. El **producto** de H y N es $HN = \{xy \mid x \in H, y \in N\}$.

Así, una clase lateral izquierda es $xH = \{x\}H$, para $x \in G$. Podemos generalizar este concepto y definir, para una familia de subgrupos $\{H_i \mid i \in I\}$ con I un conjunto de índices linealmente ordenado

$$\prod_{i \in I} H_i = \{x_1 x_2 x_3 \cdots x_j \mid x_k \in H_{i_k}, i_1 < i_2 < \cdots < i_j, j \geq 0\}$$

Observe que HN no es necesariamente un subgrupo de G pues al multiplicar dos de sus elementos no necesariamente es un elemento de la misma forma. Si G es abeliano entonces sí se tiene un subgrupo de G.

3.11 Teorema. (**Segundo Teorema de Isomorfismo**). Sea $H < G$, $N \lhd G$. Entonces $(HN)/N \cong H/(H \cap N)$.

Demostración. Como $N \lhd G$, es fácil ver que $(H \cap N) \lhd H$. Definamos

$$h : HN \longrightarrow H/(H \cap N) \text{ mediante } xy \mapsto h(xy) = x(H \cap N).$$

Veamos que h está bien definido: supongamos que $x_1 y_1 = xy$, luego $x^{-1}x_1 = yy_1^{-1}$. Así, $x^{-1}x_1 \in H$ y $x^{-1}x_1 \in N$, luego $x^{-1}x_1 \in H \cap N$. Entonces, en $H/(H \cap N)$, $x(H \cap N) = x_1(H \cap N)$ y $h(xy) = h(x_1 y_1)$.

Veamos que h es un homomorfismo. Como $N \lhd G$, $x_1 y_2 = y_2 x_3$. Luego, $h((x_1 y_1)(x_2 y_2)) = h((x_1 x_2)(y_3 y_2)) = x_1 x_2 (H \cap N) = x_1(H \cap N) x_2 (H \cap N) = h((x_1 y_1) h(x_2 y_2))$.

Como $ker\ h = \{xy \in HN \mid x \in H \cap N\} = H/(H \cap N) = N$ y como $h(xe) = x(H \cap N)$ para toda $x \in H$, utilizando el Primer Teorema de Isomorfismo, $HN/N \cong H/(H \cap N)$.♦

3.12 Ejemplo. Considere

$$\begin{aligned} G &= \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}, \\ H &= \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \{0\} \text{ y} \\ N &= \{0\} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \end{aligned}$$

Luego

$$\begin{aligned} HN &= \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z} \text{ y} \\ H\cap N &= \{0\}\times\mathbb{Z}\times\mathbb{Z}\times\{0\} \end{aligned}$$

Por lo tanto,

$$HN/N \cong \mathbb{Z} \cong H/(H\cap N).$$

3.13 Teorema. (**Tercer Teorema de Isomorfismo**). Sean $H \lhd G$ y $N \lhd G$ con $N < H$. Entonces, $G/H \cong (G/N)/(H/N)$.

Demostración. Definamos

$$\begin{aligned} h: \quad & G \longrightarrow (G/N)/(H/N) \text{ mediante} \\ & x \mapsto (xN)(H/N) \end{aligned}$$

Como

$$\begin{aligned} h(xy) &= ((xy)N)(H/N) = ((xN)(yN))(H/N) \\ &= [(xN)(H/N)][(yN)(H/N)] = h(x)h(y), \end{aligned}$$

h es un homomorfismo. Su núcleo es $\ker h = \{k \in G \mid h(k) = H/N\}$. Éstos son precisamente los elementos de H. Utilizando el Primer Teorema de Isomorfismo, $G/H \cong (G/N)/(H/N)$.

$$\begin{array}{ccccc} \ker h & \hookrightarrow & G & \longrightarrow & G/H \\ \shortparallel & & \downarrow & \searrow^{h} & \downarrow\cong \\ H & & G/N & \longrightarrow & (G/N)/(H/N) \end{array}$$

♦

3.14 Ejemplo. Consideremos $N = 6\mathbb{Z} < H = 2\mathbb{Z} < G = \mathbb{Z}$. Entonces $G/H = \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2$. $G/N = \mathbb{Z}/6\mathbb{Z}$. También, $(\mathbb{Z}/6\mathbb{Z})/(2\mathbb{Z}/6\mathbb{Z})$ tiene 2 elementos y es isomorfo a $\mathbb{Z}_2$.

Problemas.

3.1 Pruebe que para cada elemento $x \in G$, el homomorfismo

$$\begin{aligned} \iota_x: \quad & G \longrightarrow G \text{ dado por} \\ & y \mapsto xyx^{-1} \end{aligned}$$

es un automorfismo de G, llamado **automorfismo interior**.

3.2 Considere el conjunto de todos los automorfismos interiores de un grupo G, denotado $In(G)$. Pruebe que es un grupo bajo la composición.

3.3 Considere el conjunto $Aut(G)$ de todos los automorfismos de un grupo G. Pruebe que $Aut(G)$ es un grupo bajo la composición y que $In(G) \lhd Aut(G)$. Se dice que dos automorfismos f, g pertenecen a la misma "**clase de automorfismos**" si $f = h \circ g$ para algún automorfismo h. Pruebe que las clases de automorfismo forman un grupo $Aut(G)/In(G)$ llamado "**automorfismos exteriores** de G".

3.4 En la demostración del Teorema 3.2 proporcione los detalles de que g^* está bien definido. También pruebe que $im\ g^* = p'(im\ g)$ y $\ker g^* = p(g^{-1}(H'))$.

3.5 Proporcione los detalles completos de la demostración del Teorema 3.4.

3.6 Llamaremos **coimágen** y **conúcleo** de un homomorfismo de grupos abelianos $g : G \longrightarrow G''$ a los grupos cocientes de G y G''

$$\begin{aligned} coim\ g &= G/\ker\ g \\ co\ker\ g &= G''/im\ g. \end{aligned}$$

Sea $g\colon G \longrightarrow G''$ un homomorfismo de grupos abelianos. Pruebe que la sucesión

$$e \longrightarrow \ker g \longrightarrow G \longrightarrow G'' \longrightarrow co\ker\ g \longrightarrow e$$

es exacta. Observe que, en este contexto, el Primer Teorema de Isomorfismo dice que $coim\ g \cong im\ g$.

3.7 Pruebe que un homomorfismo de grupos $g : G \to G''$ es monomorfismo (escríbase como repaso) si, y sólo si, $\ker\ g = e$ y que es epimorfismo si, y sólo si, $co\ker\ g = e$.

3.8 Compruebe que las sucesiones mostradas en los ejemplos, son efectivamente, sucesiones exactas cortas.

II.4 Productos

Recordemos que si H y N son cualesquiera subgrupos de un grupo G, el producto de H y N es $HN = \{xy \mid x \in H, y \in N\}$ y para una familia de subgrupos $\{H_i \mid i \in I\}$ con I un conjunto de índices linealmente ordenado

$$\underset{i\in I}{\Pi} H_i = \{x_1x_2x_{3...}x_j \mid x_k \in H_{i_k}, i_1 < i_2 < \cdots < i_j, j \geq 0\}$$

Recuerde que HN no es necesariamente un subgrupo de G pues al multiplicar dos de sus elementos no necesariamente es un elemento de la misma forma. Si G es abeliano entonces sí se tiene un subgrupo de G.

Consideremos una familia de grupos $\{G_i\}$. El **producto directo externo** de esa familia es

$$\underset{i\in I}{\Pi} G_i = \{(x_1, ..., x_n) \mid x_i \in G_i\}$$

el cual tiene una estructura de grupo dada por

$$(x_1, ..., x_n)(y_1, ..., y_n) = (x_1y_1, ..., x_ny_n).$$

Si utilizamos la notación aditiva, escribiremos $\underset{i\in I}{\oplus} G_i$ y la llamaremos **suma directa completa**.

Recordemos que el producto cartesiano $\underset{i\in I}{\Pi} X_i$ de una familia de conjuntos $\{X_i\}_{i\in I}$ es el conjunto de funciones $h : I \longrightarrow \underset{i\in I}{\cup} X_i$ tales que $h(i) = h_i \in X_i$ para toda $i \in I$.

Sean G_1 y G_2 dos grupos. Su **producto** $G_1 \times G_2$ consiste del conjunto de todas las parejas (x, y) con $x \in G_1$, $y \in G_2$ y con operación binaria

$$\begin{array}{rcl} \cdot & : & (G_1 \times G_2) \times (G_1 \times G_2) \longrightarrow (G_1 \times G_2) \\ ((x_1, y_1), (x_2, y_2)) & \mapsto & \cdot((x_1, y_1), (x_2, y_2)) = (x_1, y_1) \cdot (x_2, y_2) = (x_1x_2, y_1y_2) \end{array}$$

Dicha operación binaria lo dota de una estructura de grupo. Las **proyecciones** $(x, y) \mapsto x$ y $(x, y) \mapsto y$ son homomorfismos de grupos

$$\begin{array}{ccccc} & & G_1 \times G_2 & & \\ & \swarrow & & \searrow & \\ G_1 & & & & G_2 \end{array}$$

Observe que toda función $h : \{1, 2\} \longrightarrow G_1 \cup G_2$ tal que $h(1) \in G_1$ y $h(2) \in G_2$ determina un elemento $(x_1, x_2) = (h(1),\ h(2)) \in G_1 \times G_2$ y que inversamente, una pareja $(x_1, x_2) \in G_1 \times G_2$ determina una función $h : \{1,2\} \longrightarrow G_1 \cup G_2$ dado por $h(1) = x_1$ y $h(2) = x_2$. Así, existe una correspondencia biunívoca entre el conjunto de todas las funciones así definidas y el grupo $G_1 \times G_2$.

4.1 Teorema. Sea G un grupo. Consideremos una familia de grupos $\{G_i\}_{i\in I}$ y una familia de homomorfismos $\{\varphi_i : G \longrightarrow G_i\}_{i\in I}$. Entonces existe un homomorfismo único $\varphi : G \longrightarrow \prod\limits_{i\in I} G_i$ tal que $p_i \circ \varphi = \varphi_i$ para toda $i \in I$.

Demostración. Consideremos el producto $P = \prod\limits_{i\in I} G_i$ con proyecciones $p_i : \prod\limits_{i\in I} G_i \longrightarrow G_i$. Dado $(G, \varphi_i : G \longrightarrow G_i)$, definamos $\varphi : G \longrightarrow \prod\limits_{i\in I} G_i$ mediante

$$\begin{array}{ccc} g & \mapsto & h_g : \quad I \longrightarrow \cup G_i \\ & & i \longmapsto h_g(i) = \varphi_i(g) \in G_i \end{array}$$

Es fácil ver que φ es un homomorfismo de grupos. También, es claro que $p_i \circ \varphi = \varphi_i$ para toda $i \in I$.

$$\begin{array}{ccc} & & G \\ \varphi_i & & \downarrow \varphi \\ & & \prod\limits_{i\in I} G_i \\ & \swarrow p_i & \\ G_i & & \end{array}$$

Supongamos que $\varphi' : G \longrightarrow \prod\limits_{i\in I} G_i$ es otro homomorfismo tal que $p_i \circ \varphi' = \varphi_i$ para toda $i \in I$. Pero

$$(\varphi'(g))(i) = p_i\varphi'(g) = \varphi_i(g) = h_g(i) = (\varphi(g))(i).$$

Luego $\varphi = \varphi'$.♦

Supongamos que existe otro grupo P' con $p'_i : P' \longrightarrow G_i$ tal que $p'_i \circ \varphi = \varphi_i$ para toda $i \in I$. Consideremos los siguientes diagramas que representan la propiedad aplicada a lo que corresponde:

$$\begin{array}{ccc} & & P' \\ p'_i & & \downarrow \varphi \\ & & P = \prod\limits_{i\in I} G_i \\ & p_i \swarrow & \\ G_i & & \end{array}$$

$$\begin{array}{ccc} & & P = \prod\limits_{i\in I} G_i \\ p_i & & \downarrow \rho \\ & & P' \\ & p'_i \swarrow & \\ G_i & & \end{array}$$

$$
\begin{array}{ccc}
 & & P = \prod\limits_{i \in I} G_i \\
p_i & & \downarrow \rho \circ \varphi \\
 & & P = \prod\limits_{i \in I} G_i \\
 & p_i \swarrow & \\
G_i & &
\end{array}
$$

Como $I_P : P \longrightarrow P$ hace lo mismo que $\rho \circ \varphi$, por la unicidad, $I_P = \rho \circ \varphi$. De manera similar, $\rho \circ \varphi = I_{P'}$. Así, φ es biyectiva (es fácil comprobar que todas las funciones son efectivamente homomorfismos de grupos) y por lo tanto es un isomorfismo.

Esta **propiedad universal del producto directo** determina al producto $\prod\limits_{i \in I} G_i$ de manera única salvo isomorfismo.

Consideremos una familia de grupos $\{G_i\}$. El **producto directo externo débil** de esa familia es

$$\prod_{i \in I}^{d} G_i = \{f \in \prod_{i \in I} G_i \mid f(i) = e_i \in G_i \text{ para casi toda } i \in I\}$$

En el caso en que se tengan solamente grupos abelianos lo llamaremos **suma directa externa** y lo denotaremos $\sum\limits_{i \in I} G_i$. Si I es finito, los productos directos externo y débil coinciden.

4.2 Teorema. Sea G un grupo abeliano. Consideremos una familia de grupos abelianos aditivos $\{G_i\}$ y una familia de homomorfismos $\{\gamma_i : G_i \longrightarrow G\}_{i \in I}$. Entonces existe un homomorfismo único $\gamma : \sum\limits_{i \in I} G_i \longrightarrow G$ tal que $\gamma \circ \iota_i = \gamma_i$ para toda $i \in I$.

Demostración. Consideremos elementos distintos de cero $g_{i_1}, \ldots, g_{i_s} = \{g_{i_j}\} \in \sum\limits_{i \in I} G_i$ y defínase

$$
\begin{array}{lcccl}
\gamma : & \sum\limits_{i \in I} G_i & \longrightarrow & G & \qquad\qquad \text{mediante} \\
 & 0 & \mapsto & 0 & \\
 & \{g_i\} & \mapsto & \gamma(\{g_i\}) & = \gamma_{i_1}(g_{i_1}) + \ldots + \gamma_{i_s}(g_{i_s}) = \Sigma_{j=1}^{s} \gamma_{ij}(g_{ij})
\end{array}
$$

esta última suma sobre los índices para los cuales $g_i \neq 0$ el cual consta de un número finito. Es inmediato comprobar que γ es un homomorfismo tal que $\gamma \circ \iota_i = \gamma_i$ para toda $i \in I$ pues G es conmutativo.

$$
\begin{array}{ccc}
 & & G \\
\gamma_i & & \uparrow \gamma \\
 & & \sum\limits_{i \in I} G_i \\
 & \nearrow \iota_i & \\
G_i & &
\end{array}
$$

Observe que $\{g_i\} \in \sum\limits_{i\in I} G_i, \{g_i\} = \Sigma\iota_j(g_j)$, esta última suma sobre los índices para los cuales $g_i \neq 0$ el cual consta de un número finito. Si $\eta : \sum\limits_{i\in I} G_i \longrightarrow G$ es tal que $\eta \circ \iota_i = \gamma_i$ para toda $i \in I$ entonces

$$\eta(\{g_i\}) = \eta(\Sigma\iota_j(g_j)) = \Sigma\gamma_i(g_i) = \Sigma\gamma\iota_i(g_i) = \gamma(\Sigma\iota_i(g_i)) = \gamma(\{g_i\}).$$

Luego $\eta = \gamma$ y por lo tanto γ es única.♦

Este teorema determina a $\sum\limits_{i\in I} G_i$ de manera única salvo isomorfismo.

A continuación veamos en un caso de dos factores, cuándo un grupo G es isomorfo al producto directo externo débil de sus subgrupos.

4.3 Proposición. Sean H y N cualesquiera subgrupos normales de un grupo G. Si $HN = G$ y $H \cap N = e$ entonces $H \times N \cong G$.

Demostración. Como $HN = G$, si $g \in G$, $xy = g$ con $x \in H, y \in N$. Veamos que x y y están determinados en forma única por g: pues si $g = x_1y_1$ entonces $xy = x_1y_1$. Luego $x^{-1}x_1 = yy_1^{-1}$. Como este elemento está en la intersección de H y N, $x^{-1}x_1 = yy_1^{-1} = e$. Luego $x = x_1$ y $y = y_1$.

Ahora establezcamos un isomorfismo entre $H \times N$ y G. Definamos $h : H \times N \longrightarrow G$ dado por $(x, y) \longmapsto h(x, y) = xy$. h es un homomorfismo pues si consideramos el conmutador $x^{-1}y^{-1}xy$ entonces $(x^{-1}y^{-1}x)y \in N$ pues N es normal en G y $x^{-1}(y^{-1}xy) \in H$ pues H es normal en G. Así, como $x^{-1}y^{-1}xy$ está en la intersección de H y N, $x^{-1}y^{-1}xy = e$, luego $xy = yx$. Así, $h((x_1, y_1)(x_2, y_2)) = h(x_1x_2, y_1y_2) = x_1x_2y_1y_2 = x_1y_1x_2y_2 = h(x_1, y_1)h(x_2, y_2)$. Finalmente, es fácil ver que h es biyectiva (Problema 4.12).♦

4.4 Definición. Diremos que un grupo G es un **produco directo (interno)** de H y N si H y N son subgrupos normales de G tal que $HN = G$ y $H \cap N = e$.

Observe que en esta definición H y N son subgrupos de G. Si $G = H \times N$ como producto directo externo, podemos considerar a G como producto directo interno pero de los subgrupos que son imágenes de H y N, a saber de $H \times \{1\}$ y $\{1\} \times N$, mas no de H y N. Entonces es claro que los dos tipos de productos proporcionan en realidad grupos isomorfos y usaremos el nombre de producto directo a secas.

4.5 Proposición. Sean $\{X_i\}_{i\in I}$ y $\{Y_i\}_{i\in I}$ familias de grupos abelianos, X y Y grupos abelianos. Entonces $Hom(\sum\limits_{i\in I} X_i, Y) \cong \prod_{i\in I} Hom(X_i, Y)$.

Demostración. Definamos ρ mediante $\rho(\varphi) = (\varphi\iota_i)_{i\in I}$. Es claro que ρ es un homomorfismo. Veamos que ρ es monomorfismo: supongamos que $\rho(\varphi) = 0$; entonces $(\varphi\iota_i) = 0$ para cada $i \in I$. Es decir, en el siguiente diagrama

$$\begin{array}{ccc} & & Y \\ & 0 \nearrow & \uparrow \varphi \\ X_i & \xrightarrow{\iota_i} & \sum\limits_{i\in I} X_i \end{array}$$

el homomorfismo $0\colon X_i \longrightarrow Y$ es tal que $0 = \varphi\iota_i$. Luego, $\varphi = 0$. Por lo tanto, $\ker\rho = \{0\}$. Veamos que ρ es un epimorfismo: sea $(\varphi_i)_{i\in I} \in \prod_{i\in I} Hom(X_i, Y)$. Entonces tenemos $\varphi_i\colon X_i \longrightarrow Y$ para cada $i \in I$. Por la propiedad universal de la suma directa, existe un homomorfismo $\varphi\colon \sum\limits_{i\in I} X_i \longrightarrow Y$ tal que $\varphi\iota_i = \varphi_i$ para cada $i \in I$. Luego, $\rho(\varphi) = (\varphi_i)_{i\in I}$.♦

Problemas.

4.1 Pruebe que si $H \lhd G$ y $N \lhd G$, entonces $HN \lhd G$.

4.2 Sean G_1, G_2 y G_3 dos grupos. (i) Pruebe que su producto $G_1 \times G_2$ con la operación binaria definida arriba es efectivamente un grupo.(ii) Pruebe que $G_1 \times G_2 \cong G_2 \times G_1$.(iii) Pruebe que $G_1 \times (G_2 \times G_3) \cong (G_1 \times G_2) \times G_3$.

4.3 Establezca una definición del producto directo externo en términos de la observación anterior al Teorema 4.1.

4.4 Pruebe que $\iota_j : G_j \longrightarrow \underset{i\in I}{\Pi^d} G_i$ dado por $\iota_j(g) = \{g_i\}_{i\in I}$ donde

$$g_i = \left\{ \begin{array}{c} e \text{ para } i \neq j \\ g_j = g \end{array} \right\}$$

es un monomorfismo de grupos llamado **inyección canónica**, que $\iota_i(G_i) \lhd \underset{i\in I}{\Pi} G_i$ y que $\underset{i\in I}{\Pi^d} G_i \lhd \underset{i\in I}{\Pi} G_i$.

4.5 Pruebe que el grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$ es isomorfo al grupo 4 de Klein V. (Sugerencia: Pruebe que $\mathbb{Z}_2 \times \mathbb{Z}_2$ no es cíclico).

4.6 Pruebe que $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.(Sugerencia: pruebe que $\mathbb{Z}_2 \times \mathbb{Z}_3$ es cíclico encontrando un generador y como sólo hay un grupo cíclico de cada orden, el resultado se sigue).

4.7 Pruebe que $\mathbb{Z}_3 \times \mathbb{Z}_3 \ncong \mathbb{Z}_9$.(Sugerencia: compruebe que $\mathbb{Z}_3 \times \mathbb{Z}_3$ no es cíclico).

4.8 Pruebe que el producto directo externo de una familia de grupos $\{G_i\}$, $\underset{i\in I}{\Pi} G_i = \{(x_1, ..., x_n) \mid x_i \in G_i\}$ tiene una estructura de grupo dada por $(x_1, ..., x_n)(y_1, ..., y_n) = (x_1y_1, ..., x_ny_n)$ y que es abeliano si cada grupo de la familia lo es.

4.9 Pruebe que $\mathbb{Z}_i \times \mathbb{Z}_j \cong \mathbb{Z}_{i,j}$ sí, y sólo si el máximo común divisor $(i, j) = 1$.

4.10 Pruebe que para cada $j \in I$ la **proyección canónica**

$$p_j : \underset{i\in I}{\Pi} G_i \longrightarrow G_j$$

dada por $f \longmapsto f(j)$ es un epimorfismo de grupos.

4.11 Proporcione todos los detalles de la demostración del Teorema 4.1.

4.12 Proporcione todos los detalles de la demostración de la Proposición 4.3.

4.13 Pruebe que si $G = H \times N$, entonces $G/(H \times \{1\}) \cong N$.

4.14 Generalice el problema anterior.

4.15 Sean $H_1 \lhd G_1$ y $H_2 \lhd G_2$ subgrupos normales. Pruebe que $H_1 \times H_2 \lhd G_1 \times G_2$ y que $G_1 \times G_2/H_1 \times H_2 \cong G_1/H_1 \times G_2/H_2$.

4.16 Proporcione una generalización de la proposición 4.3.

4.17 Sean $\{X_i\}_{i\in I}$ y $\{Y_i\}_{i\in I}$ familias de grupos abelianos, X y Y grupos abelianos. Pruebe que $Hom(X, \prod_{i\in I} Y_i) \cong \prod_{i\in I} Hom(X, Y_i)$.

Capítulo III

III.1 Grupos Abelianos Finitamente Generados

Diremos que un grupo G está **finitamente generado** si posee un conjunto finito de generadores. El resultado fundamental acerca de los grupos abelianos finitamente generados se puede formular de dos maneras que proporcionan "invariantes", en el sentido siguiente: dos grupos son isomorfos si, y sólo si, poseen los mismos invariantes numéricos.

1.1 Teorema. Todo grupo abeliano finitamente generado G es isomorfo al producto directo de n grupos cíclicos de orden $p_i^{\lambda_i}$ con r grupos cíclicos infinitos, donde los p_i son números primos no necesariamente distintos y las λ_i son enteros positivos. Aún más, el producto directo es único salvo el orden de los factores.

Esto quiere decir que G es de la forma

$$G \cong \mathbb{Z}_{p_1^{\lambda_1}} \times ... \times \mathbb{Z}_{p_n^{\lambda_n}} \times \mathbb{Z} \times ... \times \mathbb{Z}$$

La segunda manera de establecer el resultado fundamental es:

1.2 Teorema. Todo grupo abeliano finitamente generado G es isomorfo al producto directo de n grupos cíclicos de orden m_i con r grupos cíclicos infinitos, donde $m_i \mid m_{i+1}$ para $1 \leq i \leq n-1$.

Esto quiere decir que G es de la forma

$$G \cong \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_n} \times \mathbb{Z} \times ... \times \mathbb{Z}$$

Los enteros m_i se llaman **coeficientes de torsión** de G. Éstos dos teoremas nos proporcionan una clasificación salvo isomorfismo de los grupos abelianos finitamente generados, es decir, si se tiene un grupo abeliano finitamente generado, éste debe ser uno de los de la forma descrita en los teoremas anteriores. Como casos especiales se tienen los descritos en el siguiente

1.3 Teorema. (i) Si G es un grupo abeliano finitamente generado que no posea elementos de orden finito entonces es isomorfo al producto directo de un número finito de copias de $\mathbb{Z}$ y (ii) Si G es un grupo abeliano finito entonces es isomorfo a un producto directo de grupos cíclicos finitos de orden m_i donde $m_i \mid m_{i+1}$ para $1 \leq i \leq n-1$.

Esto es, en el caso (i) $G \cong \mathbb{Z} \times ... \times \mathbb{Z}$ con r copias de $\mathbb{Z}$ y decimos que G es un **grupo abeliano libre de rango** r. En el caso (ii) $G \cong \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_n}$ donde $m_i \mid m_{i+1}$ para $1 \leq i \leq n-1$ los elementos de la lista $m_1, ..., m_n$ se llaman **factores invariantes** del grupo G. Dos grupos abelianos finitos son isomorfos si, y sólo si, poseen los mismos factores invariantes. Se puede dar una lista de todos los grupos abelianos no isomorfos de cierto orden n. Bastaría encontrar todas las listas posibles de $m_1, ..., m_n$ tales que $m_i \mid m_{i+1}$ para $1 \leq i \leq n-1$ con producto n. En resumen tenemos:

1.4 Teorema. Sea $G \cong \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_n} \times \mathbb{Z} \times ... \times \mathbb{Z}$, con r copias de $\mathbb{Z}$, donde $m_i \mid m_{i+1}$ para $1 \leq i \leq n-1$ y $G' \cong \mathbb{Z}_{k_1} \times ... \times \mathbb{Z}_{k_j} \times \mathbb{Z} \times ... \times \mathbb{Z}$, con s copias de $\mathbb{Z}$, donde $k_i \mid k_{i+1}$ para $1 \leq i \leq j-1$. Si $G \cong G'$ entonces $m_i = k_i$ para $1 \leq i \leq n$, $n = j$ y $r = s$.

Aunque ya en un curso de Álgebra Lineal (como el de [Ll2]) se estudia el Teorema de Descomposición Primaria, debido al enfoque de esta presentación de la Teoría de Grupos (como un primer curso), el cual es hacia el Álgebra Homológica y la Topología Algebraica, la demostración de éstos teoremas preferimos posponerlas para un curso posterior de Teoría de Módulos y ver éstos teoremas como caso especial de los teoremas correspondientes para módulos finitamente generados sobre un anillo de ideales principales y así poder exponer otros temas usualmente excluidos del programa. El lector interesado puede ver la demostración en [B-M, Cap. X] o [H, Cap. II y IV]. Veamos a continuación cómo se utilizan.

1.5 Ejemplo. Los posibles grupos de orden 36 se obtienen así: para obtenerlos de la primera manera, descompóngase 36 en potencias de primos como $36 = 2^2 \cdot 3^2$. Luego, los posibles grupos de la primer manera (no isomorfos uno con el otro) son

$$\begin{aligned}
&\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3\\
&\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3\\
&\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9\\
&\mathbb{Z}_4 \times \mathbb{Z}_9
\end{aligned}$$

y de la segunda manera (no isomorfos uno con el otro) son

$$\begin{aligned}
&\mathbb{Z}_6 \times \mathbb{Z}_6\\
&\mathbb{Z}_3 \times \mathbb{Z}_{12}\\
&\mathbb{Z}_2 \times \mathbb{Z}_{18}\\
&\mathbb{Z}_{36}
\end{aligned}$$

Así, tenemos cuatro grupos abelianos (salvo isomorfismo) de orden 36. Los de la primera lista corresponden en el orden escrito a los de la segunda lista.

1.6 Ejemplo. Los posibles grupos de orden 540 se obtienen así: para obtenerlos de la primera manera, descompóngase 540 en potencias de primos como $540 = 2^2 \cdot 3^3 \cdot 5$. Luego, los posibles grupos de la primer manera (no isomorfos uno con el otro) son

$$\begin{aligned}
&\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5\\
&\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5\\
&\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5\\
&\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_5\\
&\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5\\
&\mathbb{Z}_4 \times \mathbb{Z}_{27} \times \mathbb{Z}_5
\end{aligned}$$

y de la segunda manera (no isomorfos uno con el otro) son

$$\begin{aligned}
&\mathbb{Z}_3 \times \mathbb{Z}_6 \times \mathbb{Z}_{30}\\
&\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{60}\\
&\mathbb{Z}_2 \times \mathbb{Z}_{270}\\
&\mathbb{Z}_6 \times \mathbb{Z}_{90}\\
&\mathbb{Z}_3 \times \mathbb{Z}_{180}\\
&\mathbb{Z}_{540}
\end{aligned}$$

Así, tenemos seis grupos abelianos (salvo isomorfismo) de orden 540. Los de la primera lista corresponden en el orden escrito a los de la segunda lista.

Consideremos una cadena $C = \{C_n, \partial_n\}$ de grupos abelianos finitamente generados y el grupo de homología de grado n de C, $H_n(C) = \ker \partial_n / im\ \partial_{n+1} = Z_n(C)/B_n(C)$. Los subgrupos $Z_n(C)$ y $B_n(C)$ de C_n son finitamente generados, luego $H_n(C)$ es finitamente generado. Los coeficientes de torsión de $H_n(C)$ se llaman **coeficientes de torsión de grado n de C** y el rango de $H_n(C)$ se llama **número de Betti $\beta_n(C)$ de grado n de C**. El entero $\chi(C) = \sum_n (-1)^n \beta_n(C)$ se llama **característica de Euler-Poincaré de la cadena C**.

Problemas.

1.1 Encuentre los posibles grupos abelianos salvo isomorfismo de orden 8, 10.

1.2 Encuentre los posibles grupos abelianos salvo isomorfismo de orden 12, 16.

1.3 Encuentre los posibles grupos abelianos salvo isomorfismo de orden 32.

1.4 Encuentre los posibles grupos abelianos salvo isomorfismo de orden 720.

1.5 Encuentre los posibles grupos abelianos salvo isomorfismo de orden 860.

1.6 Encuentre los posibles grupos abelianos salvo isomorfismo de orden 1150.

III.2 Permutaciones, Órbitas y Teoremas de Sylow

Consideremos el conjunto Σ_n consistente de todas las permutaciones del conjunto $I_n = \{1, ..., n\}$, es decir, Σ_n consiste de todas las funciones biyectivas de I_n en I_n. En I.2 vimos que Σ_n es un grupo bajo la operación binaria $\circ$ y que $\mid \Sigma_n \mid = n!$ Recordemos Σ_3 y su tabla correspondiente como en I.1. Sus elementos son

$$\begin{aligned}
\iota &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\
\eta_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \eta_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \eta_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}
\end{aligned}$$

El cálculo de la composición de dos permutaciones lo haremos siguiendo el mismo orden que el de las funciones, por ejemplo:

$$\rho_1 \circ \eta_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \eta_3$$

es decir, primero consideramos η_1 y luego ρ_1. Así,

$$\eta_1 \circ \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \eta_2$$

Su tabla es (considerando la forma de componer dos funciones, primero la derecha (columna izquierda) y después la izquierda (renglón superior)):

$\circ$	ι	ρ_1	ρ_2	η_1	η_2	η_3
ι	ι	ρ_1	ρ_2	η_1	η_2	η_3
ρ_1	ρ_1	ρ_2	ι	η_2	η_3	η_1
ρ_2	ρ_2	ι	ρ_1	η_3	η_1	η_2
η_1	η_1	η_3	η_2	ι	ρ_2	ρ_1
η_2	η_2	η_1	η_3	ρ_1	ι	ρ_2
η_3	η_3	η_2	η_1	ρ_2	ρ_1	ι

Hemos escrito para $I_n = \{1, ..., n\}$ una permutación $\sigma : I_n \longrightarrow I_n$ como

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}.$$

Diremos que una permutación σ de I_n es un **ciclo de longitud** r (o r-ciclo) si existen enteros $i_1, ...i_r$ en I_n tal que

$$\sigma(i) = \begin{cases} i_{j+1} \text{ si } i = i_j \text{ y } 1 \leq j < r \\ i_1 \text{ si } i = i_r \\ i \text{ si } i \neq i_j \text{ y } 1 \neq j \leq r \end{cases}$$

y lo denotamos mediante $\sigma = (i_1, i_2, ..., i_r)$. Por ejemplo,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1, 2, 3)$$

es un ciclo de longitud 3. Observe que $(1, 2, 3) = (2, 3, 1) = (3, 1, 2)$, es decir, hay 3 notaciones para este ciclo y en general véase el Problema 2.3.

Diremos que un ciclo de longitud 2 es una **transposición**. Un ciclo de longitud 1 lo omitiremos usualmente cuando tengamos un producto de ciclos.

Por ejemplo:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 6 & 5 & 4 & 7 \end{pmatrix} = (1, 3, 2)(4, 6)(5)(7)$$

donde $(1, 3, 2)$ es un triciclo, $(4, 6)$ es una transposición, (5) y (7) son ciclos de longitud uno y se acostumbran omitir.

Sea σ una permutación de Σ_n y definamos en $I_n = \{1, ..., n\}$ una relación dada por $i \equiv j$ sí, y sólo si $\sigma^r(i) = j$, para algún entero r. Es inmediato comprobar que tenemos una relación de equivalencia en I_n (Problema 2.4). Las clases de equivalencia las llamaremos **órbitas** de σ. Por ejemplo, la órbita del elemento 1 de la permutación

$$\begin{aligned} & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 5 & 6 & 11 & 2 & 4 & 9 & 7 & 10 & 12 & 8 & 1 \end{pmatrix} \\ = \quad & (1, 3, 6, 4, 11, 8, 7, 9, 10, 12)(2, 5) \end{aligned}$$

es $\{1, 3, 6, 4, 11, 8, 7, 9, 10, 12\}$, la del elemento 2 es $\{2, 5\}$. Observe que si la órbita contiene más de un elemento, entonces forma un ciclo de longitud igual al número de elementos de la órbita. Así, si $O_1, ..., O_k$ son las órbitas (que son ajenas) de una permutación σ y $c_1, ..., c_k$ los ciclos (ajenos) dados por $c_j(i) = \sigma(i)$ si $i \in O_j$ o i si $i \notin O_j$ entonces $\sigma = c_1 c_2 \cdots c_k$. Por lo tanto tenemos la siguiente

2.1 Proposición. Toda permutación σ se puede escribir como producto de ciclos ajenos.♦

Observe que la representación como producto de ciclos ajenos es única salvo por el orden en que aparecen. Claramente la composición de ciclos ajenos sí es conmutativa y como todo ciclo se expresa en la forma $(i_1, i_2, ..., i_r) = (i_1, i_r)(i_1, i_{r-1}) \cdots (i_1, i_3)(i_1, i_2)$ tenemos el

2.2 Corolario. Toda permutación $\sigma \in \Sigma_n$ para $n \geq 2$ es un producto de transposiciones no necesariamente ajenas.♦

Por ejemplo,

$$\begin{aligned} & (1, 3, 6, 4, 11, 8, 7, 9, 10, 12)(2, 5) \\ = \; & (1, 12)(1, 10)(1, 9)(1, 7)(1, 8)(1, 11)(1, 4)(1, 6)(1, 3)(2, 5) \end{aligned}$$

Observe que al descomponer una permutación como producto de transposiciones siempre podemos agregar la transformación identidad escrita como $(i_j, i_k)(i_j, i_k)$ de tal manera que dicha descomposición no es la única posible.

2.3 Definición. Diremos que el grupo G **actúa** (por la izquierda) en un conjunto X si existe una función

$$\begin{array}{rccc} a: & G \times X & \longrightarrow & X \\ & (g, x) & \mapsto & a(g, x) \end{array}$$

donde $a(g, x)$ se denotará gx, tal que se cumpla $(e, x) \mapsto a(e, x) = ex = x$ y $(gg', x) \mapsto a(gg', x) = (gg')x = g(g'x)$.

Si se tiene que G actúa en X se dice que X es un **G-conjunto**. En la notación $(g, x) \mapsto a(g, x) = gx$, el hecho de escribir gx es un abuso común de notación y está definido de manera particular en cada caso. Se puede definir un concepto análogo definiendo la acción por la derecha.

Veamos algunos ejemplos.

2.4 Ejemplo. Todo grupo G es un G-conjunto con la operación binaria vista como acción. También todo grupo puede considerarse un H-conjunto con H un subgrupo de G, aquí se tendría $H \times G \longrightarrow G$ dada por $(h, x) \mapsto a(h, x) = hx$. Dicha acción se llama **translación** (por la izquierda). Todo espacio vectorial V sobre un campo K puede verse como un K-conjunto donde la parte multiplicativa de K actúa en V.

2.5 Ejemplo. I_n es un Σ_n-conjunto con la acción $a : \Sigma_n \times I_n \longrightarrow I_n$ dada por $(\sigma, i) \mapsto a(\sigma, i) = \sigma(i)$.

2.6 Ejemplo. Consideremos una acción de un subgrupo H de G, $a : H \times G \longrightarrow G$ dada por $(h, x) \mapsto a(h, x) = hxh^{-1}$. Esta acción se llama **conjugación** por h. El elemento hxh^{-1} se dice que es un **conjugado** de x.

Sea X un G-conjunto con $a : G \times X \longrightarrow X$. Diremos que dos elementos $x, y \in X$ están **relacionados** y escribiremos $x \sim y$ si, y sólo si, existe $g \in G$ tal que $a(g, x) = gx = y$ para alguna $g \in G$.

2.7 Proposición. $\sim$ es una relación de equivalencia y el conjunto

$$G_x = \{g \in G \mid gx = x\}$$

es un subgrupo de G.

Demostración. Como para cada $x \in X$, $ex = x$, entonces $x \sim x$. Si $x \sim y$ entonces existe $g \in G$ tal que $gx = y$ para alguna $g \in G$. Luego, $x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}y$ y por lo tanto $y \sim x$. Si $x \sim y$ y $y \sim z$ entonces existen $g, g' \in G$ tales que $gx = y$ y $g'y = z$ para algunas $g, g' \in G$. Entonces $(g'g)x = g'(gx) = g'y = z$, luego $x \sim z$. Consideremos $g, g' \in G_x$. Luego $gx = x$ y $g'x = x$. Así, $(gg')x = g(g'x) = gx = x$. Por lo tanto, $gg' \in G_x$. Claramente $ex = x$, luego $e \in G_x$. Finalmente, si $g \in G_x$ entonces $gx = x$ y $x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}x$. Por lo tanto, $g^{-1} \in G_x$. Luego, G_x es un subgrupo de G.♦

El subgrupo G_x se llama **subgrupo de isotropía** de x o **estabilizador** de x. Llamaremos **órbita** de X bajo G a cada clase de equivalencia de la relación $\sim$. Si $x \in X$ llamaremos **órbita** de x a la clase de equivalencia de x la cual denotaremos con Gx.

Daremos nombres a diversas órbitas:

(i) Si un grupo G actúa sobre sí mismo bajo conjugación, la órbita $\{gxg^{-1}\}$ con $g \in G$ la llamaremos **clase conjugada** de x.

(ii) Si el subgrupo $H < G$ actúa en G por conjugación, el grupo de isotropía $H_x = \{h \in H : hx = xh\}$ se llama **centralizador de** x en H y lo denotaremos con $C_H(x)$.

(iii) Si $H = G$, $C_G(x)$ se llamará **centralizador de** x.

(iv) Si $H < G$ actúa por conjugación en el conjunto de los subgrupos de G, entonces el subgrupo de H que deja fijo a K se llamará **normalizador de** K **en** H, denotado $N_H(K) = \{h \in H \mid hKh^{-1} = K\}$.

(v) En particular, si tenemos el caso en que se tome $N_G(K)$ lo llamaremos **normalizador de** K.

2.8 Teorema. Sea X un G-conjunto con $a : G \times X \longrightarrow X$. Si $x \in X$, entonces el número de clases de equivalencia u órbitas es igual al índice de G_x en G, es decir, $\mid Gx \mid = (G : G_x)$.

Demostración. Definamos una función

$$\begin{array}{lccc} \omega : & Gx & \longrightarrow & G/G_x \\ & a(g,x) = gx = y & \mapsto & \omega(a(g,x)) = \omega(gx) = gG_x \end{array} \quad \text{dada por}$$

Veamos que ω está bien definida: supongamos que también $a(h,x) = hx = y$ para $h \in G$. Luego $gx = hx$, $g^{-1}(gx) = g^{-1}(hx)$ y $x = (g^{-1}h)x$. Así, $g^{-1}h \in G_x$, $h \in gG_x$ y $gG_x = hG_x$.

Ahora veamos que ω es inyectiva: si $y, z \in Gx$ y $\omega(y) = \omega(z)$. Entonces existen $h, k \in G$ tal que $a(h, x) = hx = y$ y $a(k, x) = kx = z$, con $k \in hG_x$. Entonces $k = hg$ para alguna $g \in G_x$, luego $z = kx = (hg)x = h(gx) = hx = y$. Por lo tanto, ω es inyectiva.

Veamos que ω es suprayectiva: sea hG_x una clase lateral izquierda. Entonces si $hx = y$, se tiene que $hG_x = \omega(y)$. Luego ω es suprayectiva. Por lo tanto, $\mid Gx \mid = (G : G_x)$.♦

2.9 Corolario. Si $o(G)$ es finito, entonces $o(Gx) \mid o(G)$.

Demostración. Como $o(G)$ es finito, entonces $o(G) = o(Gx)o(G_x)$.♦

2.10 Teorema. Sea G un grupo finito, $g \in G$ y $X_g = \{x \in X \mid gx = x\}$. Si n es el número de órbitas de X en G entonces

$$n = \sum_{g \in G} \mid X_g \mid o(G)^{-1}$$

Demostración. Sea r el número de parejas (g, x) tales que $gx = x$. Hay $\mid X_g \mid$ parejas para cada g y $\mid G_x \mid$ para cada x. Entonces

$$r = \sum_{g \in G} \mid X_g \mid = \sum_{x \in X} \mid G_x \mid .$$

Como $o(Gx) = (G : G_x) = o(G)/o(G_x)$ por el teorema anterior, entonces $o(G_x) = o(G)/o(Gx)$. Así, $r = \sum_{x \in X}(\mid G \mid / \mid Gx \mid) = \mid G \mid \sum_{x \in X}(1/ \mid Gx \mid)$. Pero $1/ \mid Gx \mid$ tiene el mismo valor para toda x en la misma órbita y si O denota cualquier órbita, entonces $\sum_{x \in O}(1/ \mid Gx \mid) = \sum_{x \in O}(1/ \mid O \mid) = 1$. Sustituyendo, obtenemos $r = o(G)n$.♦

2.11 Proposición. Sea X un G-conjunto. La función

$$\begin{array}{rccc} \omega : & G & \longrightarrow & \Sigma_X \\ & g & \mapsto & \omega(g) = \sigma_g(x) = gx \end{array}$$

es un homomorfismo.

Demostración. Veamos que $\sigma_g : X \longrightarrow X$ es efectivamente una permutación: Si $\sigma_g(x) = \sigma_g(y)$, entonces $gx = gy$. Luego $g^{-1}(gx) = g^{-1}(gy)$ y $(g^{-1}g)x = (g^{-1}g)y$. Así, $ex = ey$ y $x = y$. Por lo tanto, σ_g es inyectiva.

Como $\sigma_g(g^{-1}x) = g(g^{-1}x) = (gg^{-1})x = ex = x$, para cada x existe $g^{-1}x$ tal que $\sigma_g(g^{-1}x) = x$. Luego, σ_g es suprayectiva. ω es un homomorfismo pues

$$\begin{array}{rcl} \omega(gg') & = & \sigma_{gg'}(x) = (gg')x = g(g'x) = g\sigma_{g'}(x) \\ & = & \sigma_g(\sigma_{g'}(x)) = \omega(g)(\sigma_{g'}(x)) = \omega(g)\omega(g').♦ \end{array}$$

2.12 Corolario. (**Cayley**) Si G es un grupo entonces existe un monomorfismo $G \longrightarrow \Sigma_G$, es decir, todo grupo es isomorfo a un grupo de permutaciones. Si G es un grupo finito de orden n entonces es isomorfo a un subgrupo de Σ_n.

Demostración. Consideremos la acción de G en sí mismo mediante translación por la izquierda y así aplicamos la proposición anterior obteniendo

$$\begin{array}{rccl} \omega: & G & \longrightarrow & \Sigma_G \text{ dada por} \\ & g & \mapsto & \omega(g) = \sigma_g(x) = gx \end{array}$$

Si $\omega(g) = \sigma_g(x) = gx = I_G$, entonces $\sigma_g(x) = gx = x$ para toda $x \in G$. Si tomamos $x = e$ entonces $ge = e$ y por lo tanto $g = e$. Luego, ω es un monomorfismo. Como caso particular, si $o(G) = n$ entonces $\Sigma_G = \Sigma_n$.

Otra redacción es la siguiente: Propondremos a

$$H = \{\sigma_g : G \longrightarrow G \mid x \mapsto \sigma_g(x) = gx, \text{ para cada } g \in G \text{ fija}\}$$

como candidato a subgrupo de Σ_G. $\sigma_g : G \longrightarrow G$ es claramente una permutación de G pues si $\sigma_g(x) = \sigma_g(y)$ entonces $gx = gy$ y $x = y$, además, si $x \in G$ entonces $\sigma_g(g^{-1}x) = gg^{-1}x = x$. Es inmediato comprobar que H es un subgrupo de Σ_G pues $\sigma_g \circ \sigma_{g'}(x)) = \sigma_g(g'x) = g(g'x) = (gg')x = \sigma_{gg'}(x)$ para toda $x \in G$, como $\sigma_e(x) = ex = x$ para toda $x \in G$, H contiene a la permutación identidad y finalmente, como $\sigma_g\sigma_{g'} = \sigma_{gg'}, \sigma_g\sigma_{g^{-1}} = \sigma_{gg^{-1}} = \sigma_e$ y $\sigma_{g^{-1}}\sigma_g = \sigma_{g^{-1}g} = \sigma_e$ tenemos que $\sigma_{g^{-1}} = (\sigma_g)^{-1}$. Ahora, definamos

$$\begin{array}{ccl} h & : & G \longrightarrow H \text{ mediante} \\ g & \mapsto & h(g) = \sigma_g \end{array}$$

Como

$$h(gg')(x) = \sigma_{gg'}(x) = (gg')x = g(g'x) = \sigma_g(\sigma_{g'}(x)) = (\sigma_g\sigma_{g'})(x)) = h(g)h(g')$$

h es un homomorfismo. Si $h(g) = h(g')$ entonces, en particular, $\sigma_g(e) = ge = g = g' = g'e = \sigma_{g'}(e)$, luego $g = g'$ y h es inyectiva. Luego h es un isomorfismo.♦

Los teoremas de Sylow nos proporcionan información importante acerca de los grupos finitos no conmutativos. Nos dicen, entre otras cosas, que si la potencia de un primo divide al orden de un grupo este posee un subgrupo con ese orden.

2.13 Definición. Un grupo G se dice que es un p**-grupo** (p un número primo), si todos los elementos de G tienen orden una potencia de p.

2.14 Teorema. (**Primer teorema de Sylow**) Sea G un grupo de orden $p^n m$ donde p es primo, $n \geq 1$ y tal que $p \nmid m$. Entonces, G contiene un subgrupo de orden p^i para cada i tal que $1 \leq i \leq n$, y todo subgrupo H de G de orden p^i es un subgrupo normal de un subgrupo de orden p^{i+1} para $1 \leq i < n$.

2.15 Definición. Sea p un número primo. Diremos que P es un p-**subgrupo de Sylow** si P es un p-subgrupo máximo de G i.e si K es un p-grupo tal que $P < K < G$ entonces $P = K$.

2.16 Teorema. (**Segundo teorema de Sylow**) Dos p-subgrupos de Sylow de un grupo finito G son conjugados.

2.17 Teorema. (**Tercer teorema de Sylow**) Si G es un grupo finito y $p \mid o(G)$ (p primo), entonces el número de p-subgrupos de Sylow de G divide al orden de G y es congruente con 1 módulo p.

Véase [A] o [F] para las demostraciones de los teoremas de Sylow.

Problemas.

2.1 Compruebe que $a : \mathbb{Z} \times \mathbb{R} \longrightarrow \mathbb{R}$ dada por $(g, x) \mapsto a(g, x) = gx$ es una acción de $\mathbb{Z}$ en $\mathbb{R}$ llamada translación.

2.2 Considere la acción $a : H \times s(G) \longrightarrow s(G)$ de un subgrupo H de un grupo G en el conjunto $s(G)$ consistente de todos los subgrupos de G dada por $(h, K) \longmapsto hKh^{-1}$. Pruebe que hKh^{-1} es un subgrupo de G isomorfo a K. hKh^{-1} se dice que es un **subgrupo conjugado** de K.

2.3 Pruebe que para un ciclo de longitud r hay exactamente r notaciones en forma de ciclo.

2.4 Pruebe que si σ es una permutación de Σ_n y en $I_n = \{1, ..., n\}$, $i \equiv j$ si, y sólo si $\sigma^r(i) = j$, para algún entero r, entonces $\equiv$ es una relación de equivalencia en I_n.

2.5 Definimos el **signo de una permutación** $\sigma \in \Sigma_n$ como

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

Pruebe que si σ' es otra permutación, entonces $sg(\sigma' \circ \sigma) = sg(\sigma')sg(\sigma)$ y que si τ es una transposición, entonces $sg(\tau) = -1$. Diremos que una permutación es **par** o **impar** si su signo es 1 o -1 respectivamente. Concluya que si $n > 1$, el conjunto de las permutaciones pares de I_n forman un subgrupo A_n de Σ_n llamado **grupo alternante de grado n**.

2.6 Defina un homomorfismo $h : \Sigma_n \longrightarrow \{1, -1\}$ dado por $h(\sigma)$ igual a 1 si σ es par y -1 si σ es impar. Pruebe que A_n es el núcleo de h, y por lo tanto un subgrupo normal de Σ_n tal que $o(A_n) = \frac{n!}{2}$.

2.7 Pruebe que si un número primo p divide al orden de un grupo finito $o(G)$, entonces G tiene un elemento de orden p y por ende un subgrupo de orden p. (**Teorema de Cauchy**)

2.8 Pruebe que un grupo finito es un p-grupo si, y sólo si, el orden de G es una potencia de p.

2.9 Pruebe que si $o(G) = p^n$, p un número primo, entonces posee un centro no trivial.

2.10 Demuestre que si $o(G) = p^2$ para p un número primo, entonces G es cíclico o isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_p$.

2.11 Pruebe que el subgrupo K es normal en $N_G(K)$.

2.12 Pruebe que K es normal en G si, y sólo si $N_G(K) = G$. Compruebe que los 2-subgrupos de Sylow de Σ_3 tienen orden 2 y que éstos son conjugados unos con otros.

2.13 Pruebe que solamente existe un grupo de orden 15.

2.14 Pruebe que no existen grupos simples de orden 15, 20, 30, 36, 48 y 255.

III.3 Grupos Libres

Considérese el producto cartesiano $A = X \times \mathbb{Z}_2$ donde X denota cualquier conjunto y $\mathbb{Z}_2 = \{-1, 1\}$. Para cada elemento x de X usaremos las notación $x^1 = (x, 1)$ y $x^{-1} = (x, -1)$. Consideremos el conjunto K de todas las sucesiones finitas de elementos con repetición del conjunto A. Definamos una operación binaria en K

$$\begin{array}{rcl} K \times K & \to & K \\ (x_1, ..., x_r)(y_1, ..., y_s) & \mapsto & (x_1, ..., x_r, y_1, ..., y_s) \end{array}$$

Llamaremos **alfabeto** a los elementos de A, y **palabras** a los elementos de K, los cuales son productos formales de elementos de A.

3.1 Ejemplo. Tómese $X = \{x_1, x_2, x_3, x_4\}$. Las siguientes expresiones son palabras: $x_1^1 x_2^{-1} x_1^1 x_2^{-1} x_3^1 x_4^{-1} x_2^{-1} x_3^1$, $x_2^{-1} x_3^1 x_4^{-1} x_1^1 x_2^{-1} x_3^1 x_3^1 x_4^{-1}$, $x_3^1 x_4^{-1} x_1^1 x_2^{-1} x_3^1$.

Diremos que una palabra está **reducida** si para todo elemento x de X, x^1 nunca está junto a x^{-1} o viceversa. Sea L el conjunto de todas las palabras reducidas de K y adjuntémosle la palabra vacía (la cual no está en K) misma que denotaremos con 1.

Ahora definamos una operación binaria en L con las siguientes condiciones: si alguno de los elementos x o y es 1 entonces su producto es x o y, de otra manera su producto es una palabra reducida xy. Se puede comprobar que esta operación binaria proporciona a L una estructura de grupo.

3.2 Definición. Un **grupo libre en el conjunto** X es una pareja (L, f) donde L es un grupo y $f : X \longrightarrow L$ es una función tal que, para cualquier función $g : X \longrightarrow G$, G un grupo cualquiera, existe un homomorfismo único $h : L \longrightarrow G$ tal que el siguiente triángulo es conmutativo:

$$\begin{array}{ccc} X & \xrightarrow{f} & L \\ & g \searrow & \downarrow h \\ & & G \end{array}$$

Definamos una función $f : X \longrightarrow L$ mediante $f(x) = x^1 \in L$. Supongamos que $g : X \longrightarrow G$ es cualquier función de X en un grupo G. Definamos una función $h : L \longrightarrow G$ mediante

$$\begin{array}{rcl} h(k) & = & e_G \text{ si } k \text{ es la palabra vacía} \\ h(k) & = & g(x_1)^{\eta_1} g(x_2)^{\eta_2} \cdots g(x_n)^{\eta_n} \text{ si } k = x_1^{\eta_1} x_2^{\eta_2} \cdots x_n^{\eta_n} \\ \text{para } \eta_i & = & \pm 1,\ 1 \le i \le n \end{array}$$

Es fácil comprobar que h es un homomorfismo de grupos tal que $h \circ f = g$. Aún más, si $h' : L \longrightarrow G$ es otro homomorfismo de grupos tal que $h' \circ f = g$. Entonces para la palabra $k = x_1^{\eta_1} x_2^{\eta_2} \cdots x_n^{\eta_n}$ tendríamos que $h'(k) = h'(x_1)^{\eta_1} h'(x_2)^{\eta_2} \cdots h'(x_n)^{\eta_n} = g(x_1)^{\eta_1} g(x_2)^{\eta_2} \cdots g(x_n)^{\eta_n}$. Luego $h = h'$. Así es que tenemos el siguiente

3.3 Teorema. Para cualquier conjunto X siempre existe un grupo libre en X.♦

Considérese un grupo libre en el conjunto X denotado (L, f), donde $f : X \longrightarrow L$ es una función. Veamos que dicha función f es inyectiva: Supongamos que $x, y \in X$ con $x \neq y$. Consideremos un grupo G y $g : X \longrightarrow G$ una función tal que $g(x) \neq g(y)$. Como $h(f(x)) = g(x) \neq g(y) = h(f(y))$ se tiene que $f(x) \neq f(y)$. Aún más, veamos que $f(X)$ genera L: sea H el subgrupo de L generado por $f(X)$. Entonces f define una función $g : X \longrightarrow H$ con $i \circ g = f$ donde i denota la inclusión de H en L. Como L es libre, existe un homomorfismo $h : L \longrightarrow H$ tal que $h \circ f = g$.

$$\begin{array}{ccc} X & \xrightarrow{f} & L \\ & g \searrow & i \uparrow\downarrow h \\ & & H \end{array}$$

Considere el diagrama

$$\begin{array}{ccc} X & \xrightarrow{f} & L \\ & f \searrow & i \circ h \downarrow\downarrow I_L \\ & & L \end{array}$$

Es claro que $I_L \circ f = f$, y $i \circ h \circ f = i \circ g = f$. Por la unicidad, $i \circ h = I_L$. Luego, i debe ser suprayectiva. Así, $H = G$ y $f(X)$ genera L.

Supongamos que (L', g) es otro grupo libre en el mismo conjunto X que L. Entonces podemos considerar el siguiente diagrama:

$$\begin{array}{ccc} X & \xrightarrow{f} & L \\ \| & g \searrow & \downarrow h \\ X & & L' \\ & f \searrow & \downarrow h' \\ & & L \end{array}$$

Aquí, como L es libre, existe un homomorfismo único h tal que $g = h \circ f$ y como también L' es libre, existe un homomorfismo único h' tal que $f = h' \circ g$. Por la unicidad, $I_L = h' \circ h$. Análogamente podemos considerar el diagrama

$$\begin{array}{ccc} X & \xrightarrow{g} & L' \\ \| & f \searrow & \downarrow h' \\ X & & L \\ & g \searrow & \downarrow h \\ & & L' \end{array}$$

y obtener que $I_{L'} = h \circ h'$. Luego, $L \cong L'$. Podemos resumir lo anterior en el siguiente

3.4 Teorema. Sea (L, f) un grupo libre en X. Entonces f es inyectiva y $f(X)$ genera L. Aún más, (L, f) es único salvo isomorfismo.♦

Obsérvese que cada conjunto X determina un único grupo libre. Como f es inyectiva identificaremos X con su imagen y $f(X)$ es un subconjunto generador de L. Podemos decir que toda función $g : X \longrightarrow G$ **se extiende a** un homomorfismo único $h : L \longrightarrow G$. Llamaremos a L **grupo libre generado por los elementos del conjunto** X. Observe que todo grupo libre es infinito.

Sea G cualquier grupo. Podemos escoger un subconjunto X de G que genere a G. Siempre se puede, pues podríamos escoger $X = G$. Consideremos el grupo libre generado por X. Entonces la función de inclusión $g : X \longrightarrow G$ se extiende a un homomorfismo $h : L \longrightarrow G$. h es suprayectiva puesto que X genera G y $X = g(X) \subset h(L)$. Si N es el núcleo de h, por el primer teorema del isomorfismo, $G \cong L/N$. Podemos resumir esto en el siguiente

3.5 Teorema. Cualquier grupo es isomorfo al cociente de un grupo libre.♦

Denotemos con R el conjunto de generadores del subgrupo N del grupo libre L. Como el grupo L está totalmente determinado por el conjunto X y el subgrupo normal N lo está por el conjunto R, el grupo $G \cong L/N$ puede definirse dando un conjunto cuyos elementos los llamaremos **generadores** de G y mediante un conjunto R cuyos elementos los llamaremos **relaciones** que definen G.

Consideremos una palabra reducida $k = x_1^{\eta_1} x_2^{\eta_2} \cdots x_n^{\eta_n} \neq 1$, es decir, un elemento de R tal que si N no es el subgrupo trivial omitimos el 1 del conjunto R. Como $k \in N$, representa el elemento de identidad en el cociente. Lo denotaremos mediante la expresión $x_1^{\eta_1} x_2^{\eta_2} \cdots x_n^{\eta_n} = 1$.

Diremos que los conjuntos X y R dan una **presentación** $(X \mid R)$ del grupo $G \cong L/N$. Puede haber presentaciones diferentes de un mismo grupo. En tal caso las llamaremos, **presentaciones isomorfas**.

3.6 Ejemplo. El grupo diedro D_n $n \geq 2$, es el grupo de orden $2n$ generado por dos elementos, a y b con relaciones $a^n = 1, b^2 = 1$ y $bab = a^{-1}$.

3.7 Ejemplo. $(x \mid \_)$ es una presentación del grupo libre $\mathbb{Z}$. Esto es, un generador, pero ninguna relación. De aquí el término **libre**, es decir, libre de relaciones.

3.8 Ejemplo. $(x \mid x^n = e)$ es una presentación del grupo cíclico $\mathbb{Z}_n$.

3.9 Definición. Un grupo abeliano libre en el conjunto X es una pareja (L, f) donde L es un grupo abeliano y $f : X \longrightarrow L$ es una función tal que, para cualquier función $g : X \longrightarrow G$, G un grupo abeliano cualquiera, existe un homomorfismo único $h : L \longrightarrow G$ tal que el siguiente triángulo es conmutativo:

$$\begin{array}{ccc} X & \xrightarrow{f} & L \\ & g \searrow & \downarrow h \\ & & G \end{array}$$

Los siguientes dos teoremas se prueban exactamente como los correspondientes a grupos libres:

3.10 Teorema. Sea (L, f) un grupo abeliano libre en X. Entonces f es inyectiva y $f(X)$ genera L. Aún más, (L, f) es único salvo isomorfismo.♦

3.11 Teorema. Cualquier grupo abeliano es isomorfo al cociente de un grupo abeliano libre.♦

3.12 Teorema. Para cualquier conjunto X siempre existe un grupo abeliano libre en X.

Demostración. Sea $(K, i : X \to K)$ un grupo libre en un conjunto X. Considérese el grupo cociente $L = K/K'$donde K' denota el subrupo conmutador y la proyección a dicho cociente $p : K \to K/K'$. Veamos que (L, f) es un grupo abeliano libre en X, $f = p \circ i$.

Sea $g : X \to G$ cualquier función de X en un grupo abeliano G. Como K es un grupo libre en X, existe un homomorfismo $k : K \to G$ tal que $k \circ i = g$. Como G es un grupo abeliano, k envía el subgrupo conmutador K' de K al elemento 0 de G. Luego, k induce un homomorfismo $h : L \to G$ tal que $h \circ p = k$. Luego $h \circ p \circ i = k \circ i = g$. La unicidad es inmediata y la dejamos como un ejercicio.♦

Como la función $f = p \circ i$ es inyectiva, podemos identificar X con su imagen $f(X)$ en L. Así, X es un subconjunto de L que genera a L misma. Decimos que la **función g se extiende** a un homomorfismo único h y llamamos a L el **grupo abeliano libre generado por (los elementos) del conjunto X**. Diremos que un grupo cualquiera G es un **grupo abeliano libre**, si es isomorfo a un grupo abeliano libre L generado por un conjunto X. Si $f' : L \to G$ y denotamos con f la restricción de f'a X, entonces (G, f) es un grupo abeliano libre en el conjunto X. Llamaremos **base del grupo abeliano libre** G a la imagen $f(X)$. Es claro que toda función $g : f(X) \to H$ donde H es cualquier grupo abeliano se extiende a un homomorfismo único $h : G \to H$. (Problema 3.3).

3.13 Ejemplo. Considere el grupo que consiste de la suma directa de n copias de $\mathbb{Z}$. Entonces $(1, 0, ..., 0)$, $(0, 1, 0, ...0)$,..., $(0, ..., 0, 1)$ es una base de dicho grupo abeliano libre. El grupo de los enteros módulo n no es abeliano libre.

Problemas.

3.1 Sea L el conjunto de todas las palabras reducidas de K y adjuntémosle la palabra vacía (la cual no está en K) misma que denotaremos con 1. Definamos una operación binaria en L con las siguientes condiciones: si alguno de los elementos x o y es 1 entonces su producto es x o y, de otra manera su producto es una palabra reducida xy. Pruebe que esta operación binaria proporciona una estructura de grupo a L.

3.2 Considere la función $h : L \longrightarrow G$ definida mediante

$$\begin{aligned} h(k) &= e_G \text{ si } k \text{ es la palabra vacía} \\ h(k) &= g(x_1)^{\eta_1} g(x_2)^{\eta_2} \cdots g(x_n)^{\eta_n} \text{ si } k = x_1^{\eta_1} x_2^{\eta_2} \cdots x_n^{\eta_n} \\ \text{para } \eta_i &= \pm 1,\ 1 \leq i \leq n \end{aligned}$$

Compruebe que h es un homomorfismo de grupos tal que $h \circ f = g$ en el contexto del Teorema 3.3.

3.3 Diremos que un grupo cualquiera G es un **grupo abeliano libre**, si es isomorfo a un grupo abeliano libre L generado por un conjunto X. Si $f' : L \to G$ y denotamos con f la restricción de f' a X, entonces (G, f) es un grupo abeliano libre en el conjunto X. Llamaremos **base del grupo abeliano libre** G a la imagen $f(X)$. Pruebe que toda función $g : f(X) \to H$ donde H es cualquier grupo abeliano se extiende a un homomorfismo único $h : G \to H$.

3.4 Decimos que un grupo abeliano libre es de **rango finito o infinito** si posee una base finita o infinita respectivamente. Pruebe que si una base es finita con n elementos (infinita), entonces cualquier otra base es también finita con n elementos (infinita).

3.5 Sean L y L' grupos abelianos libres isomorfos generados por X y X' respectivamente. Pruebe que si X consiste de un número finito de elementos, entonces X' consiste del mismo número de elementos.

3.6 Sea $\{G_j\}_{j \in X}$ una familia de grupos abelianos indizados por el conjunto X con cada $G_j \cong \mathbb{Z}, j \in X$. Defina $L = \{\alpha : X \to \mathbb{Z} \mid \alpha(j) = 0$ para casi toda $j \in X\}$ junto con una operación binaria dada por $(\alpha + \beta)(j) = \alpha(j) + \beta(j)$ $j \in X$.

(i) Pruebe que L es un grupo abeliano.

(ii) Defina $f : X \to L$ mediante $j \mapsto f(j)(i) = 1$ si $i = j, 0$ si $i \neq j$. Pruebe que (L, f) es un grupo abeliano libre en X.

(iii) Pruebe que $\sum_{j \in X} G_j \cong (L, f)$.

(iv) Concluya que un grupo abeliano es de rango m si, y sólo si, es isomorfo a la suma directa de m grupos cíclicos infinitos.

Los siguientes problemas son optativos (no se espera que sean resueltos sin ayuda externa) y establecerán, (junto con los problemas de las secciones y capítulos anteriores) los **grupos de orden menor que** 16, a saber:

Orden	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Número	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1

donde el renglón superior indica el orden del grupo y el renglón inferior indica el número de grupos salvo isomorfismo de ese orden.

3.7 Pruebe que si p es un número primo que divide al orden de un grupo, entonces el grupo contiene un elemento de orden p. Este es el **Teorema de Cauchy**.

3.8 Pruebe que solamente existen dos grupos de orden $2p$ para cada número primo p, uno es cíclico y el otro es D_p.

3.9 Escriba todos los grupos, salvo isomorfismo, de cada orden menor a 16.

3.10 Determine todos los grupos, salvo isomorfismo, de orden 10.

3.11 Compruebe que las siguientes presentaciones de $\mathbb{Z}_6$ son isomorfas: $(x, y \mid xyx^{-1}y^{-1} = e, x^2 = e, y^3 = e)$ y $(x \mid x^6 = e)$.

3.12 Determine todos los grupos, salvo isomorfismo, de orden 8. (Son cinco, de los cuales tres son abebianos y dos son no abelianos).

3.13 Determine todos los grupos, salvo isomorfismo, de orden 12. (Son cinco, dos son abelianos y tres son no abelianos. Sugerencia: utilice los Teoremas de Sylow y argumentos semejantes a los usados en el problema anterior).

III.4 Producto Tensorial

Definiremos un grupo abeliano en el cual solamente se tienen relaciones biaditivas.

4.1 Definición. Sean X y Y grupos abelianos. El **producto tensorial** de X y Y es la pareja (T, f), donde T es un grupo abeliano y $f: X \times Y \to T$ es una función biaditiva, tal que si, G es un grupo abeliano y $g: X \times Y \to G$ es biaditiva, entonces existe una homomorfismo único $h: T \to G$ tal que $g = h \circ f$.

La condición $g = h \circ f$ se puede representar mediante el diagrama

$$\begin{tikzcd} X \times Y \arrow[r, "f"] \arrow[dr, "g"'] & T \arrow[d, "h"] \\ & G \end{tikzcd}$$

La definición anterior nos dice que cualquier función biaditiva $g: X \times Y \to G$ puede expresarse en términos de $f: X \times Y \to T$ como $g(x, y) = h(f(x, y))$ para un homomorfismo único $h: T \to G$.

Veamos a continuación que, si existe, el producto tensorial de dos grupos abelianos es único. Es decir, dados dos productos tensoriales (T, f) y (T', f') de X y Y existe un isomorfismo entre T y T'. Esto es inmediato, pues, por ser T un producto tensorial, existe $h: T \to T'$ tal que $f' = h \circ f$. Análogamente, como T' es un producto tensorial, existe $h': T' \to T$ tal que $f = h' \circ f'$. Consideremos los siguientes diagramas

$$\begin{tikzcd} & T \arrow[d, "h"] & \\ X \times Y \arrow[ur, "f"] \arrow[r, "f'"] \arrow[dr, "f"'] & T' \arrow[d, "h'"] & 1_T \\ & T & \end{tikzcd}$$

$$\begin{tikzcd} & T' \arrow[d, "h'"] & \\ X \times Y \arrow[ur, "f'"] \arrow[r, "f"] \arrow[dr, "f'"'] & T \arrow[d, "h"] & 1_{T'} \\ & T' & \end{tikzcd}$$

Por ser T un producto tensorial, como $1_T: T \to T$ es tal que $1_T \circ f = f$ se tiene que también que $h' \circ h \circ f = f$. Luego, por la unicidad, tenemos que

$h' \circ h = 1_T$. De manera semejante, por ser T' un producto tensorial, como $1_{T'}\colon T' \to T'$ es tal que $1_{T'} \circ f' = f'$ y también $h \circ h' \circ f' = f'$, se tiene, por unicidad, que $h \circ h' = 1_{T'}$. Por lo tanto, h es un isomorfismo. Entonces podemos hablar de el producto tensorial T de X y Y, denotado con $T = X \otimes Y$ o simplemente $X \otimes Y$.

Ahora veamos que, dados dos grupos abelianos, siempre existe su producto tensorial.

4.2 Proposición. Sean X y Y grupos abelianos. Entonces existe un grupo abeliano T que cumple la definición anterior.

Demostración. Sea L el grupo abeliano libre con base $X \times Y$ y sea G el subgrupo de L generado por los elementos de la forma $(x+x', y) - (x, y) - (x', y)$ y $(x, y+y') - (x, y) - (x, y')$ donde $x, x' \in X$ y $y, y' \in Y$. Definamos $X \otimes Y = T = L/G$. Denotemos con $x \otimes y$ la clase lateral $(x, y) + G$. Es inmediato comprobar que $f\colon X \times Y \to X \otimes Y$, dado por $f(x, y) = x \otimes y$ es biaditiva, (Problema 4.1). Veamos que que $X \otimes Y$ es, efectivamente, un producto tensorial. Sea G' un grupo abeliano cualquiera. Consideremos el triángulo

$$\begin{array}{ccc} X \times Y & \xrightarrow{f} & L \\ & {\scriptstyle g}\searrow & \downarrow{\scriptstyle h'} \\ & & G' \end{array}$$

donde g es biaditiva. Como L es libre con base $X \times Y$, existe un homomorfismo $h'\colon L \to G$ tal que $g = h' \circ f$. Es fácil ver que h' se anula en los elementos generadores de G. Por lo tanto, $G \subset \ker h'$, e induce un homomorfismo $h\colon L/G \to G'$ tal que el siguiente triángulo conmuta:

$$\begin{array}{ccc} X \times Y & \xrightarrow{f} & L/G = X \otimes Y \\ & {\scriptstyle g}\searrow & \downarrow{\scriptstyle h} \\ & & G' \end{array}$$

Es fácil comprobar que h es única (Problema 4.1).♦

Para cada $x \in X$ y $y \in Y$, el elemento $f(x, y)$ lo escribiremos en la forma $x \otimes y$. Es fácil comprobar (Problema 4.2) que $f(X \times Y)$ genera el producto tensorial T, el cual denotamos $X \otimes Y$. De manera que cada elemento de $X \otimes Y$ se puede escribir en la forma $\sum_{i=1}^{r} \lambda_i(x_i \otimes y_i)$ con $\lambda_i \in \mathbb{Z}$, $x_i \in X$, $y_i \in Y$. Esta expresión no es única pues se pueden escoger diferentes representantes de una clase lateral. Debido a lo anterior, podemos alternativamente definir $X \otimes Y$ como el grupo abeliano generado por todos los símbolos $x \otimes y$, $x \in X$, $y \in Y$, sujeto a las relaciones

$$\begin{array}{rcl} (x_1 + x_2) \otimes y & = & x_1 \otimes y + x_2 \otimes y \\ x \otimes (y_1 + y_2) & = & x \otimes y_1 + x \otimes y_2 \end{array}$$

Esta expresión no es única pues de la biaditividad de f se tiene que

$$\begin{array}{rcl}(x_1+x_2)\otimes y & = & (x_1\otimes y)+(x_2\otimes y)\\ x\otimes(y_1+y_2) & = & (x\otimes y_1)+(x\otimes y_2)\end{array}$$

donde $x_1, x_2, x \in X$ y $y_1, y_2, y \in Y$. Como caso particular se tiene que, para $\lambda \in \mathbb{Z}, (\lambda x)\otimes y = \lambda(x\otimes y) = x\otimes(\lambda y)$. Si $\lambda = -1$ se tiene que $(-x)\otimes y = -(x\otimes y) = x\otimes(-y)$ y si $\lambda = 0$ se tiene que $0\otimes y = 0 = x\otimes 0$. Por lo tanto, cualquier elemento de $X\otimes Y$ puede escribirse en la forma

$$\sum_{i=1}^{r}(x_i\otimes y_i)$$

donde $x_i \in X$, $y_i \in Y$.

La función biaditiva f se llama **función biaditiva universal** (cualquier otra función biaditiva $g\colon X\times Y\to G$ se obtiene de f). Decimos que debido a la propiedad universal, el grupo abeliano $X\otimes Y$ está determinado en forma única salvo isomorfismo.

Sean $\varphi\colon X'\to X$, $\psi\colon Y'\to Y$ homomorfismos de grupos abelianos y

$$\varphi\times\psi\colon X'\times Y'\to X\times Y$$

dado por

$$(\varphi\times\psi)(x,y) = (\varphi(x),\psi(y)).$$

Sean $f\colon X'\times Y'\to X'\otimes Y'$ y $g\colon X\times Y\to X\otimes Y$ las funciones biaditivas respectivas. Consideremos la función biaditiva

$$g\circ(\varphi\times\psi)\colon X'\times Y'\to X\otimes Y.$$

Como $X'\otimes Y'$ es el producto tensorial, existe un homomorfismo único

$$h\colon X'\otimes Y'\to X\otimes Y$$

que denotaremos con $\varphi\otimes\psi$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} X'\times Y' & \xrightarrow{f} & X'\otimes Y' \\ {\scriptstyle\varphi\times\psi}\downarrow & & \downarrow{\scriptstyle\varphi\otimes\psi} \\ X\times Y & \xrightarrow{g} & X\otimes Y \end{array}$$

i.e.,

$$(\varphi\otimes\psi)\circ f(x,y) = g\circ(\varphi\times\psi)(x,y); (x,y)\in X'\times Y'.$$

Luego

$$(\varphi\otimes\psi)(x\otimes y) = \varphi(x)\otimes\psi(y), x\in X', y\in Y'.$$

Como consecuencia de la unicidad de $\varphi\otimes\psi$ tenemos que si $X' \xrightarrow{\varphi} X \xrightarrow{\varphi'} X''$ y $Y' \xrightarrow{\psi} Y \xrightarrow{\psi'} Y''$ son homomorfismos de grupos abelianos, entonces

$$(\varphi' \circ \varphi) \otimes (\psi' \circ \psi) = (\varphi' \otimes \psi') \circ (\varphi \otimes \psi).$$

En particular, las siguientes proposiciones son inmediatas.

4.3 Proposición. Sean $\psi\colon Y' \to Y$ y $\psi'\colon Y \to Y''$ homomorfismos de grupos abelianos y X un grupo abeliano. Entonces

(i) si $1_X\colon X \to X$ y $1_Y\colon Y \to Y$ son los homomorfismos de identidad entonces $1_X \otimes 1_Y$ es la identidad de $X \otimes Y$, y

(ii) $(1_X \otimes \psi') \circ (1_X \otimes \psi) = (1_X \otimes (\psi' \circ \psi))$.♦

Podemos escribir éstas afirmaciones en el siguiente diagrama:

$$\begin{array}{cccccc} & Y' & & & X\otimes Y' & \\ & \psi\downarrow & & & \downarrow_{1_X\otimes\psi} & \\ 1_Y & Y & \psi'\circ\psi & 1_X\otimes 1_Y & X\otimes Y & 1_X\otimes(\psi'\circ\psi) \\ & \psi'\downarrow & & & \downarrow_{1_X\otimes\psi'} & \\ & Y'' & & & X\otimes Y'' & \end{array}$$

Análogamente tenemos la siguiente

4.4 Proposición. Sean $\varphi\colon X' \to X$ y $\varphi'\colon X \to X''$ homomorfismos de grupos abelianos y Y un grupos abeliano. Entonces

(i) si $1_X\colon X \to X$ y $1_Y\colon Y \to Y$ son los homomorfismos de identidad, entonces $1_X \otimes 1_Y$ es la identidad de $X \otimes Y$, y

(ii) $(\varphi' \otimes 1_Y) \circ (\varphi \otimes 1_Y) = ((\varphi' \circ \varphi) \otimes 1_Y)$.♦

Podemos escribir éstas afirmaciones en el siguiente diagrama:

$$\begin{array}{cccccc} & X' & & & X'\otimes Y & \\ & \varphi\downarrow & & & \downarrow_{\varphi\otimes 1_Y} & \\ 1_X & X & \varphi'\circ\varphi & 1_X\otimes 1_Y & X\otimes Y & (\varphi'\circ\varphi)\otimes 1_Y \\ & \varphi'\downarrow & & & \downarrow_{\varphi'\otimes 1_Y} & \\ & X'' & & & X''\otimes Y & \end{array}$$

Se tiene el siguiente resultado acerca del producto tensorial de una suma directa de grupos abelianos:

4.5 Proposición. (i) Sean X y Y grupos abelianos con $Y = \sum_{i\in I} Y_i$. Entonces

$$X \otimes (\sum_{i\in I} Y_i) \cong \sum_{i\in I} (X \otimes Y_i)$$

(ii) Sean X y Y grupos abelianos y $X=\sum_{i\in I}X_i$. Entonces

$$(\sum_{i\in I}X_i)\otimes Y\cong\sum_{i\in I}(X_i\otimes Y)$$

Demostración. Sea $g\colon X\times(\sum_{i\in I}Y_i)\to\sum_{i\in I}(X\otimes Y_i)$ dada por $g(x,(y_i))=(x\otimes y_i)$. Es fácil comprobar que g es biaditiva. Luego, existe

$$h\colon M\otimes(N_i)\to(M\otimes N_i)$$

tal que el siguiente diagrama conmuta:

$$\begin{tikzcd} X\times(\sum_{i\in I}Y_i) \arrow[r, "f"] \arrow[dr, "g"'] & X\otimes(\sum_{i\in I}Y_i) \arrow[d, "h"] \\ & \sum_{i\in I}(X\otimes Y_i) \end{tikzcd}$$

Sea $\varphi_i\colon X\otimes Y_i\to X\otimes(\sum_{i\in I}Y_i)$ dada por $\varphi_i(x\otimes y_i)=x\otimes\iota_{Y_i}(y_i)$ donde $\iota_{Y_i}\colon Y_i\to\sum_{i\in I}Y_i$ es la inclusión. Luego, por la propiedad universal de la suma directa, existe un homomorfismo único

$$\varphi\colon\sum_{i\in I}(X\otimes Y_i)\to X\otimes(\sum_{i\in I}Y_i)$$

tal que si $\iota_{X\otimes Y_i}\colon X\otimes Y_i\to\sum_{i\in I}(X\otimes Y_i)$ es la inclusión entonces $\varphi_i=\varphi\circ\iota_{X\otimes Y_i}$, es decir, el siguiente diagrama conmuta para toda $i\in I$

$$\begin{tikzcd} & X\otimes(\sum_{i\in I}Y_i) \\ X\otimes Y_i \arrow[ur, "\varphi_i"] \arrow[r, "\iota_{X\otimes Y_i}"'] & \oplus_{i\in I}(X\otimes Y_i) \arrow[u, "\varphi"'] \end{tikzcd}$$

Es fácil comprobar que $\varphi\circ h=1_{X\otimes(\sum_{i\in I}Y_i)}$ y que $h\circ\varphi=1_{\oplus_{i\in I}(X\otimes Y_i)}$. La demostración de (ii) es análoga.♦

4.6 Proposición. (i) Si $Y'\overset{\psi}{\rightarrowtail}Y\overset{\psi}{\twoheadrightarrow}Y''$ es una sucesión exacta de grupos abelianos y X un grupo abeliano, entonces

$$X\otimes Y'\xrightarrow{1_X\otimes\psi}X\otimes Y\xrightarrow{1_X\otimes\psi'}X\otimes Y''\to 0$$

es una sucesión exacta. (ii) Si $X'\overset{\varphi}{\rightarrowtail}X\overset{\varphi'}{\twoheadrightarrow}X''$ es una sucesión exacta de grupos abelianos y Y un grupo abeliano, entonces

$$X'\otimes Y\xrightarrow{\varphi\otimes 1_Y}X\otimes Y\xrightarrow{\varphi'\otimes 1_Y}X''\otimes Y\to 0$$

es una sucesión exacta.

Demostración. (i) Veamos que $1_X \otimes \psi'$ es un epimorfismo: sea $t'' = \sum(x_i \otimes y_i'') \in X \otimes Y''$, $x_i \in X$, $y_i'' \in Y''$. Como ψ' es un epimorfismo, existe $y_i \in Y$ tal que $\psi'(y_i) = y_i''$ para toda i. Luego,

$$(1_X \otimes \psi')(\sum(x_i \otimes y_i)) = \sum(x_i \otimes y_i'').$$

Como

$$(1_X \otimes \psi')(1_X \otimes \psi) = (1_X \otimes \psi'\psi) = 1_X \otimes 0 = 0$$

se tiene que $im(1_X \otimes \psi) \subset \ker(1_X \otimes \psi')$. Resta únicamente comprobar que $(1_X \otimes \psi) \supset \ker(1_X \otimes \psi')$, lo cual dejamos al lector, así como la parte (ii).♦

El resultado anterior es lo mejor que podemos obtener. Por ejemplo, si consideramos la sucesión exacta

$$\mathbb{Z} \overset{2.\_}{\rightarrowtail} \mathbb{Z} \twoheadrightarrow \mathbb{Z}/2$$

donde 2._ denota la multiplicación por dos, al hacer el producto tensorial con $Y = Z/2$ obtenemos

$$\mathbb{Z} \otimes \mathbb{Z}/2 \xrightarrow{2_*} \mathbb{Z} \otimes \mathbb{Z}/2 \twoheadrightarrow \mathbb{Z}/2 \otimes \mathbb{Z}/2$$

la cual es equivalente a

$$\mathbb{Z}/2 \xrightarrow{2_*} \mathbb{Z}/2 \twoheadrightarrow \mathbb{Z}/2$$

pero 2_* no es inyectivo.

A continuación estableceremos algunas **propiedades del producto tensorial**.

4.7 Proposición. Sea Y un grupo abeliano. Entonces $Y \otimes \mathbb{Z} \cong Y \cong \mathbb{Z} \otimes Y$.

Demostración. Sea $g\colon Y \times \mathbb{Z} \to Y$ la función biaditiva dada por $g(y, \lambda) = \lambda y$, $\lambda \in \mathbb{Z}$, $y \in Y$. Entonces existe una homomorfismo único $h\colon Y \otimes \mathbb{Z} \to Y$ tal que $h \circ f = g$, es decir, el siguiente diagrama conmuta:

$$\begin{tikzcd} Y \times \mathbb{Z} \arrow[r, "f"] \arrow[dr, "g"'] & Y \otimes \mathbb{Z} \arrow[d, "h"] \\ & Y \end{tikzcd}$$

La función biaditiva g es suprayectiva pues $g(y, 1) = 1 \cdot y = y$. Como $h \circ f = g$ entonces h es suprayectiva.

Veamos que h es inyectiva: sea $x \in Y \otimes \mathbb{Z}$. Entonces existen elementos $\{y_i\}_{i=1}^n$ en Y y $\{\lambda_i\}_{i=1}^n$ en $\mathbb{Z}$ tales que x es de la forma $\sum_{i=1}^n (y_i \otimes \lambda_i)$ para $y_i \in Y$, $\lambda_i \in \mathbb{Z}$. Pero

$$x = \sum_{i=1}^n (y_i \otimes \lambda_i) = \sum_{i=1}^n (\lambda_i y_i \otimes 1) = (\sum_{i=1}^n \lambda_i y_i) \otimes 1 = y \otimes 1.$$

Luego
$$h(x) = h(y\otimes 1) = h(f(y,1)) = g(y,1) = 1\cdot y = y.$$
Si $h(y\otimes 1) = 0$ entonces $y = 0$ y por lo tanto $x = y\otimes 1 = 0$. Así, h es inyectivo. Dejamos al lector probar que $Y \cong \mathbb{Z}\otimes Y$ (Problema 4.5).♦

4.8 Proposición. Sean X, Y, Z grupos abelianos. Entonces
$$(X\otimes Y)\otimes Z \cong X\otimes (Y\otimes Z) \cong X\otimes Y\otimes Z$$

Demostración. Consideremos la función biaditiva
$$g''\colon X\times Y \to X\otimes Y\otimes Z$$
dada por $g''(x,y) = x\otimes y\otimes w$ para $w\in Z$ fija, la cual induce un homomorfismo
$$h_w\colon X\otimes Y \to X\otimes Y\otimes Z$$
tal que
$$h_w(x\otimes y) = x\otimes y\otimes w.$$
Sea
$$g\colon (X\otimes Y)\times Z \to X\otimes Y\otimes Z$$
dada por
$$g(t,w) = h_w(t).$$
g es biaditiva y por lo tanto induce un homomorfismo
$$h\colon (X\otimes Y)\otimes Z \to X\otimes Y\otimes Z$$
tal que
$$h((x\otimes y)\otimes w) = x\otimes y\otimes w.$$
Construyamos ahora una función
$$h'\colon X\otimes Y\otimes Z \to (X\otimes Y)\otimes Z$$
tal que $h'\circ h = 1_{(X\otimes Y)\otimes Z}$ y $h\circ h' = 1_{X\otimes Y\otimes Z}$. Para construir h' considere la función
$$g'\colon X\times Y\times Z \to (X\otimes Y)\otimes Z$$
dada por
$$g'(x,y,w) = (x\otimes y)\otimes w.$$
g' es lineal en cada variable, luego induce un homomorfismo
$$h'\colon X\otimes Y\otimes Z \to (X\otimes Y)\otimes Z$$
tal que
$$h(x\otimes y\otimes w) = (x\otimes y)\otimes w.$$

Es inmediato comprobar que $h' \circ h = 1_{(X\otimes Y)\otimes Z}$ y que $h \circ h' = 1_{X\otimes Y\otimes Z}$ y, por lo tanto, h y h' son isomorfismos. La demostración de que $X\otimes(Y\otimes Z) \cong X\otimes Y\otimes Z$ es análoga.♦

Problemas.

4.1 Pruebe que en la Proposición 4.2 $f\colon X\times Y \to X\otimes Y$, dado por $f(x,y) = x\otimes y$ es biaditiva, h' se anula en los elementos generadores de G y h es única.

4.2 Verifique que $f(X \times Y)$ genera a $X \otimes Y$. (Sugerencia:defina un homomorfismo $i\colon X \times Y \to X \otimes Y$ y utilice la unicidad para mostrar que i es suprayectiva.)

4.3 Sea $g\colon X \times (\sum\limits_{i\in I} Y_i) \to \sum\limits_{i\in I}(X \otimes Y_i)$ dada por $g(x,(y_i)) = (x \otimes y_i)$ como en la Proposición 4.5. Compruebe que g es biaditiva. También compruebe que $\varphi \circ h = 1_{X\otimes(\sum\limits_{i\in I} Y_i)}$ y que $h \circ \varphi = 1_{\oplus_{i\in I}(X\otimes Y_i)}$. Realice la demostración de la parte (ii).

4.4 En la Proposición 4.6 compruebe que $(1_X \otimes \psi) \supset \ker(1_X \otimes \psi')$, así como la parte (ii).

4.5 Pruebe que $Y \cong \mathbb{Z} \otimes Y$.

4.6 Pruebe que $X \otimes Y \cong Y \otimes X$.

4.7 Pruebe que $X \otimes (Y \otimes Z) \cong X \otimes Y \otimes Z$.

4.8 Pruebe que si $X' \overset{\varphi}{\rightarrowtail} X \overset{\varphi'}{\twoheadrightarrow} X''$ es una sucesión exacta de grupos abelianos que se escinde y Y un grupo abeliano, entonces

$$0 \to X' \otimes Y \xrightarrow{\varphi\otimes 1_Y} X \otimes Y \xrightarrow{\varphi'\otimes 1_Y} X'' \otimes Y \to 0$$

es una sucesión exacta que se escinde.

Bibliografía

[A] Armstrong, M.A. Groups and Symmetry. UTM. Springer. 1988.

[B-M] Birkhoff, G. MacLane, S. Algebra.Macmillan. 1968.

Bourbaki, N. Algebra I. Addison Wesley. 1973.

[F] Fraleigh, J.B. Abstract Algebra. Addison Wesley. 2003.

Hu, S-T. Elements of Modern Algebra. Holden-Day. 1965.

[H] Hungerford, T.W. Algebra. Springer. 1980.

Lang, S. Algebra. Addison Wesley. 1965.

[Ll1] Lluis-Puebla, E. Álgebra Homológica, Cohomología de Grupos y K-Teoría Algebtraica Clásica. Segunda Edición. Publicaciones Electrónicas. Sociedad Matemática Mexicana. Serie: Textos. Vol. 5. 2005.

[Ll2] Lluis-Puebla, E. Álgebra Lineal. Sitesa. 1997.

Robinson, J.S. A Course in the Theory of Groups. Springer. 1980.

Rotman, J.J. The Theory of groups. Allyn and Bacon. 1976.

.

Lista de Símbolos

Índice Analítico

A

B

C

D

E

F

G

H

I

J

L

M

N

O

S

T

.

Contraportada

El éxito de la Teoría de Grupos es impresionante y extraordinario. Es quizás, la rama más poderosa e influyente de toda la Matemática. Influye en casi todas las disciplinas científicas, artísticas y en la propia Matemática de una manera fundamental. El concepto de estructura y los relacionados con éste, como el de isomorfismo, juegan un papel decisivo en la Matemática actual. Este texto contiene el material correspondiente al curso sobre la materia que se imparte en la Facultad de Ciencias de la Universidad Nacional Autónoma de México. Sigue el enfoque de los otros textos del autor sobre Álgebra Lineal y Álgebra Homológica. En él se escogió una presentación moderna donde se introduce el lenguaje de diagramas conmutativos y propiedades universales, tan requerido en la matemática actual así como en la Física y en la Ciencia de la Computación, entre otras disciplinas.

El texto consta de tres capítulos con cuatro secciones cada uno. Cada sección contiene una serie de problemas que se resuelven con creatividad utilizando el material expuesto, mismos que constituyen una parte fundamental del texto. Tienen también como finalidad, la de permitirle al estudiante redactar matemática. El libro está diseñado para un primer curso sobre la Teoría de Grupos el cual se cubre en su totalidad en cuarenta horas de clase. El autor ha decidido incluir este texto dentro de las Publicaciones Electrónicas de la Sociedad Matemática Mexicana con el ánimo de predicar con el ejemplo y mostrar (como matemático y Editor Ejecutivo) la confianza en este tipo de publicación.

El autor, Emilio Lluis-Puebla, realizó sus Estudios Profesionales y de Maestría en Matemática en México. En 1980 obtuvo su Doctorado en Matemática en Canadá. Es catedrático de la Universidad Nacional Autónoma de México en sus Divisiones de Estudios Profesionales y de Posgrado desde hace veintiocho años. Ha formado varios profesores e investigadores que laboran tanto en México como en el extranjero. Su trabajo matemático ha quedado establecido en sus artículos de investigación y divulgación que ha publicado sobre la K-Teoría Algebraica y la Cohomología de Grupos en las más prestigiadas revistas nacionales e internacionales. Ha sido Profesor Visitante en Canadá.

Recibió varias distinciones académicas, entre otras, la medalla Gabino Barreda al más alto promedio en la Maestría, Investigador Nacional (1984-1990) y Cá-tedra Patrimonial de Excelencia del Conacyt (1992-1993). Es autor de varios libros sobre K-Teoría Algebraica, Álgebra Homológica, Álgebra Lineal y Teoría Matemática de la Música publicados en las editoriales con distribución mundial Addison Wesley, Birkhäuser y Springer Verlag entre otras.

Es miembro de varias asociaciones científicas como la Real Sociedad Matemática Española y la American Mathematical Society. Es presidente de la Academia de Ciencias del Instituto Mexicano de Ciencias y Humanidades, presidente de la Academia de Matemática de la Sociedad Mexicana de Geografía y Estadística y presidente 2000-2002 de la Sociedad Matemática Mexicana.