

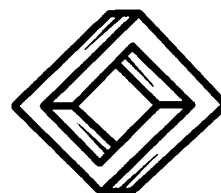
**Publicaciones Electrónicas  
Sociedad Matemática Mexicana**

**Una introducción a la  
Teoría de Grupos  
con aplicaciones en la  
Teoría Matemática de la Música**

**Octavio A. Agustín-Aquino  
Janine du Plessis  
Emilio Lluís-Puebla  
Mariana Montiel**

**[www.sociedadmatematicamexicana.org.mx](http://www.sociedadmatematicamexicana.org.mx)**

**Serie: Textos. Vol. 10 (2009)  
ISBN 968-9161-36-9**



Una introducción a la  
Teoría de Grupos  
con aplicaciones en la  
Teoría Matemática de la Música

**Octavio A. Agustín-Aquino**

*Universidad Nacional Autónoma de México*

**Janine du Plessis**

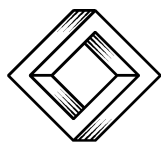
*Georgia State University*

**Emilio Lluís-Puebla**

*Universidad Nacional Autónoma de México*

**Mariana Montiel**

*Georgia State University*



Publicaciones Electrónicas  
Sociedad Matemática Mexicana

2009 Primera Edición: Sociedad Matemática Mexicana,  
Publicaciones Electrónicas  
ISBN 968-9161-37-7 (versión en línea)  
ISBN 968-9161-38-5 (versión en CD)  
ISBN 968-9161-36-9 (versión en papel)

Hecho en México.

# 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 (en la Música, en particular) y en la propia Matemática de una manera fundamental. La Teoría de Grupos extrae lo esencial de diversas situaciones donde aparece algún tipo de *simetría* o *transformación*. 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 (o inclusive los distintos objetos de la Música (!)).

Este texto está basado en el de “Teoría de Grupos: un primer curso” de Emilio Lluís-Puebla publicado en esta misma serie. Contiene el material correspondiente al curso sobre la materia que se imparte en la Facultad de Ciencias de la Universidad Nacional Autónoma de México, aunado a material optativo introductorio a un curso básico de la Teoría Matemática de la Música.

Este texto sigue el enfoque de los otros textos del Emilio Lluís-Puebla 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.

La obra consta de cuatro capítulos. 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. A lo largo de los primeros tres capítulos se incluyen ejemplos representativos (no numerados) de la aplicaciones de la Teoría de Grupos a la Teoría de Matemática de la Música, para estudiantes que ya tienen conocimiento de la Teoría Musical.

En el capítulo 4 se exponen con detalle más aplicaciones de la Teoría de Grupos a la Teoría Musical. Se explican algunos aspectos básicos de la Teoría

Matemática de la Música y, en el proceso, se pretende dar elementos a lectores de diversos antecedentes, tanto en la Matemática como en la Música. Por este motivo, los ejemplos se siguen de algunos aspectos teóricos sobresalientes de los capítulos previos; los aspectos y términos musicales son introducidos conforme se van necesitando para que un lector sin formación musical pueda entender la esencia de cómo la Teoría de Grupos es empleada para explicar ciertas relaciones musicales ya establecidas. Asimismo, para el lector con conocimiento de la Teoría Musical, este capítulo provee elementos concretos, así como motivación, para comenzar a comprender la Teoría de Grupos.

Finalmente, agregamos que hemos decidido incluir este texto dentro de las Publicaciones Electrónicas de la Sociedad Matemática Mexicana con el ánimo de predicar con el ejemplo y mostrar la confianza en este tipo de publicaciones.

Octavio A. Agustín-Aquino

*Universidad Nacional Autónoma de México*

Janine du Plessis

*Georgia State University*

Emilio Lluís-Puebla

*Universidad Nacional Autónoma de México*

Mariana Montiel

*Georgia State University*

# Índice General

<b>Prefacio</b>	<b>III</b>
<b>Introducción</b>	<b>1</b>
<b>Capítulo 1</b>	<b>7</b>
1.1 Operaciones Binarias . . . . .	7
1.2 Estructuras Algebraicas . . . . .	13
1.3 Propiedades Elementales . . . . .	24
1.4 Grupos Cíclicos . . . . .	32
<b>Capítulo 2</b>	<b>37</b>
2.1 Sucesiones Exactas . . . . .	37
2.2 Grupos Cociente . . . . .	42
2.3 Teoremas de Isomorfismo . . . . .	49
2.4 Productos . . . . .	54
<b>Capítulo 3</b>	<b>61</b>
3.1 Grupos Abelianos Finitamente Generados . . . . .	61
3.2 Permutaciones, Órbitas y Teoremas de Sylow . . . . .	64
3.3 Grupos Libres . . . . .	72
3.4 Producto Tensorial . . . . .	78
<b>Capítulo 4</b>	<b>87</b>
4.1 Antecedentes Musicales . . . . .	88
4.2 Las Transformaciones T e I . . . . .	91
4.3 Las Transformaciones P, L y R . . . . .	96
4.4 El Isomorfismo entre PLR y TI . . . . .	103
4.5 La Dualidad de los Grupos TI y PLR . . . . .	106
<b>Bibliografía y Referencias</b>	<b>113</b>
<b>Lista de Símbolos</b>	<b>115</b>
<b>Índice Analítico</b>	<b>117</b>



# 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 decía el periodista y filólogo 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 in-



creíble. 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 profesionalista 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 semejanza 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. Esta 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), para la propia Teoría de Grupos (grupo diédrico y simétrico) o para la Música, en lo que respecta a la escala cromática. 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).

La idea de una conexión entre la Matemática y la Música ha tenido aceptación a lo largo de la historia y el alcance de esa conexión ha sido ampliado significativamente desde que fue hecha explícita, por primera vez, por Pitágoras de Samos. El capítulo 4 presentará una faceta del desarrollo moderno de la Teoría Matemática de la Música, basada en su naturaleza transformacional. En este aspecto, la Teoría de Grupos desempeña un papel protagónico.

Los fundamentos de esta aplicación pueden ser atribuidos, en particular, a David Lewin, quien desarrolló la Teoría Transformacional, y dio lugar a una nueva forma de teoría musical, diseñada para analizar la música moderna. Esta nueva teoría se conoce como la Teoría Neo-Riemanniana.

La Teoría Neo-Riemanniana está inspirada en la obra del teórico alemán de la música Hugo Riemann, quien contribuyó mucho a los esfuerzos de establecer relaciones entre tonos e intervalos. La necesidad de este cambio surgió de los cambios industriales, políticos y sociales que ocurrían a lo largo del siglo XIX. Era inevitable que hubiera un efecto importante sobre la música de ese tiempo, y estos cambios frecuentemente eran expresados por medio de modulaciones audaces, progresiones innovadoras de acordes, disonancias y resoluciones y, en general, mucho menos preparación para los cambios abruptos en la Música. Estas radicales transformaciones dieron lugar, en la Música, al posromanticismo y, finalmente, a la atonalidad. Naturalmente, la teoría tonal de la Música no podía seguir cumpliendo con su responsabilidad y nuevas herramientas tenían que ser construidas para poder analizar y explicar esta música en evolución; así nació la teoría Riemanniana.

Mientras que Riemann estaba interesado, primordialmente, en sustituir el sistema de etiquetar los acordes y eventos musicales en boga, Lewin vio la potencialidad de estas etiquetas para describir el movimiento entre estos eventos musicales. El trabajo de Lewin toma forma en su contribución extensiva a la definición de las operaciones que describen el movimiento musical (eso es, la Teoría Transformacional) y, yendo aún más lejos, aplica la Teoría de Grupos a la Música. Estos conjuntos de transformaciones no sólo forman grupos, sino que son isomorfos entre sí y al grupo diedral. Es más, satisfacen varias propiedades

que nos permiten concluir que existe una dualidad.

Algunos piensan que la Matemática es un juego simple que sola y fríamente interesa al intelecto. Esto sería el olvidar, afirma 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 los autores 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 1

## 1.1. 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

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

Segundo, pregúntese: ¿cómo se relacionan dos conjuntos “adecuadamente”? Sean  $A$  y  $B$  dos conjuntos cualesquiera. Diremos que  $f : A \rightarrow B$  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  $f : A \rightarrow B$  dada por la siguiente asociación

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

es una función, mientras que la asociación

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

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  $f$ :

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

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  $f : G \times G \rightarrow G$  donde  $(x, y) \mapsto f(x, y)$ .

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

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

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

Si la operación binaria  $f$  la denotamos simplemente como  $+$  (la suma usual en  $\mathbb{Z}$ ) entonces  $(3, 2) \mapsto +(3, 2) = 3+2$  que es igual a 5. Si la operación binaria  $f$  la denotamos como  $\cdot$  (la multiplicación usual en  $\mathbb{Z}$ ), entonces  $(3, 2) \mapsto \cdot(3, 2) = 3 \cdot 2$  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  $f, g, h, \diamond, \blacktriangle, \clubsuit, \heartsuit, \times, \otimes, *$ , etc; escojamos  $+$ . Así

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

con

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

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

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

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

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

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  $\mathbb{Z}_5$

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

de la siguiente manera:

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

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

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

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





Figura 1.1: La escala cromática.



Figura 1.2: Las escalas de C mayor (izquierda) y de F mayor (derecha).

**Ejemplo.** En la Teoría Matemática de la Música es muy útil interpretar a la escala cromática equitemperada (figura 1.1) como el grupo  $\mathbb{Z}_{12}$ , con las asociaciones

$$\begin{aligned} C &\mapsto 0, C\sharp \mapsto 1, D \mapsto 2, D\sharp \mapsto 3, \\ E &\mapsto 4, F \mapsto 5, F\sharp \mapsto 6, G \mapsto 7, \\ G\sharp &\mapsto 8, A \mapsto 9, A\sharp \mapsto 10, B \mapsto 11, \end{aligned}$$

si nos interesa la altura de un tono<sup>1</sup> sin tomar en cuenta la octava<sup>2</sup> en la que se encuentra.

De esta manera, es fácil transponer melodías, escalas o acordes. Por ejemplo, la escala de C mayor  $\{C, D, E, F, G, A, B\} = \{0, 2, 4, 5, 7, 9, 11\}$  se puede transponer a la de F mayor (figura 1.2) sumando 5 a cada nota. De manera explícita, tenemos que

$$\begin{aligned} \{0 + 5, 2 + 5, 4 + 5, 5 + 5, 7 + 5, 9 + 5, 11 + 5\} \\ = \{5, 7, 9, 10, 0, 2, 4\} = \{F, G, A, A\sharp, C, D, E\}. \end{aligned}$$

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

<sup>1</sup>El **tono** es la percepción que se tiene de la frecuencia de un sonido. En la Música se eligen algunos tonos fijos para realizar las composiciones, como es el caso de los que conforman la escala cromática equitemperada. Véase el capítulo 4, sección 1.

<sup>2</sup>Una **octava** es la distancia (o intervalo) que se percibe entre un tono y otro con el doble (o la mitad) de su frecuencia. Véase el capítulo 4, sección 1.

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  $\Delta_3$  de los movimientos rígidos de un triángulo equilátero con vértices  $A, B, C$ , es decir, las rotaciones sobre el bari-centro de  $0^\circ$ ,  $120^\circ$  y  $240^\circ$  y las reflexiones sobre las medianas. Denotemos éstos movimientos rígidos de la siguiente manera:

$$\begin{aligned} 0 &= [ABC/ABC], 1 = [ABC/BCA], 2 = [ABC/CAB] \\ 3 &= [ABC/ACB], 4 = [ABC/CBA], 5 = [ABC/BAC] \end{aligned}$$

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  $\Delta_3$ :

$$\circ : \Delta_3 \times \Delta_3 \rightarrow \Delta_3$$

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

Calculemos:

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

esto es

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

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

esto es

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

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

esto es

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

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  $f : G \times G \rightarrow G$ , denotado  $(G, f)$  la cual cumple con ser asociativa, poseer elemento de identidad e inversos. La imagen de  $(x, y)$  en  $G$  la denotamos  $(x, y) \mapsto f(x, y)$ . Por abuso o conveniencia de notación denotamos  $f(x, y)$  como  $xy$  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  $\Delta_3$  con su operación 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  $f : G \rightarrow G$ ,  $g : G^2 = G \times G \rightarrow G$ ,  $h : G \times G \times G \rightarrow G$  o bien  $j : G^n = G \times \dots \times G \rightarrow G$  dando así lugar a **operaciones unarias**, **binarias**, **ternarias** o  **$n$ -arias**. La **operación nula** es una función  $i : \{e\} \rightarrow G$ .

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  $\Delta_3$  con la operación binaria definida en el Ejemplo 1.3 es un grupo.

**1.5** Sea  $\Sigma_3$  el conjunto de las permutaciones de 1, 2, 3. Calcule el número de elementos de  $\Sigma_3$ . Defina una operación binaria en  $\Sigma_3$  y construya su tabla.

**1.6** Sea  $\Sigma_n$  el conjunto de las permutaciones de un conjunto con  $n$  elementos. Calcule el número de elementos de  $\Sigma_n$ .

**1.7** Construya una tabla que represente la suma de todos los elementos de  $\mathbb{Z}_6$  y compárela con las tablas de  $\Sigma_3$  y  $\Delta_3$ . Observe que las tablas de  $\Sigma_3$  y  $\Delta_3$  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.

## 1.2. 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 [L12] 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  $\mu$  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

$$+: G \times G \rightarrow G$$

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  $(\mathbb{Z}, +)$ ,  $(n\mathbb{Z}, +)$ ,  $n \in \mathbb{Z}$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{Q}^* = \mathbb{Q} - \{0\}, \cdot)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{R}^* = \mathbb{R} - \{0\}, \cdot)$ ,  $(\mathbb{C}, +)$ ,  $(\mathbb{C}^* = \mathbb{C} - \{0\}, \cdot)$ ,  $(\mathbb{Z}_n, +)$ ,  $(\Delta_3, \circ)$ ,  $(\Sigma_3, \circ)$ ,  $(\Sigma_n, \circ)$ ,  $(M_n K, +)$ , donde  $M_n K$  denota las matrices cuadradas de  $n \times n$  con coeficientes en un campo  $K$ ,  $(GL_n K, +)$  y  $(GL_n K, \cdot)$ , donde  $GL_n K$  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).

**Ejemplo.** Es frecuente que los compositores tomen un tema y le apliquen diferentes simetrías para darle variedad a una creación musical.

Tres procedimientos comunes son la **inversión** ( $I_s$ ) respecto al tono  $s$ , la **retrogradación** ( $R$ ) y la **retrogradación con inversión** ( $RI_s$ ). Para fijar ideas, definamos provisionalmente un  **$n$ -motivo** como una sucesión  $\{x_i\}_{i=1}^n$  con  $x_i \in \mathbb{Z}_{12}$  para todo  $i$  (teniendo en cuenta la identificación que vimos en la sección anterior). Denotemos con  $\mathcal{T}(n)$  al conjunto de todos los  $n$ -motivos. Definimos las funciones inversión, la retrogradación y la retrogradación con inversión según

$$\begin{aligned} I_s : \mathcal{T}(n) &\mapsto \mathcal{T}(n), \\ \{x_i\}_{i=1}^n &\mapsto \{y_i = 2s - x_i\}_{i=1}^n, \end{aligned}$$

$$\begin{aligned} R : \mathcal{T}(n) &\mapsto \mathcal{T}(n), \\ \{x_i\}_{i=1}^n &\mapsto \{y_i = x_{n-i+1}\}_{i=1}^n, \end{aligned}$$

y

$$\begin{aligned} RI_s : \mathcal{T}(n) &\mapsto \mathcal{T}(n), \\ \{x_i\}_{i=1}^n &\mapsto \{y_i = 2s - x_{n-i+1}\}_{i=1}^n. \end{aligned}$$

Sea  $s$  un tono fijo en la escala equitemperada y  $\{x_i\}_{i=1}^n \in \mathcal{T}(n)$ . Vemos que

$$\begin{aligned} I_s \circ I_s(\{x_i\}_{i=1}^n) &= I_s(y_i = \{2s - x_i\}_{i=1}^n) \\ &= \{w_i = 2s - (2s - x_i)\}_{i=1}^n \\ &= \{w_i = 2s - 2s + x_i\}_{i=1}^n \\ &= \{w_i = x_i\}_{i=1}^n = \{x_i\}_{i=1}^n, \end{aligned}$$

es decir,  $I_s \circ I_s = \text{id}_{\mathcal{T}(n)}$ . También

$$\begin{aligned} R \circ R(\{x_i\}_{i=1}^n) &= R(\{y_i = x_{n-i+1}\}_{i=1}^n) \\ &= \{w_i = y_{n-i+1}\}_{i=1}^n \\ &= \{w_i = x_{n-(n-i+1)+1}\}_{i=1}^n \\ &= \{w_i = x_{n-n+i-1+1}\}_{i=1}^n \\ &= \{w_i = x_i\}_{i=1}^n = \{x_i\}_{i=1}^n \end{aligned}$$

lo que indica que  $R \circ R = \text{id}_{\mathcal{T}(n)}$ . Por último

$$\begin{aligned} I_s \circ R(\{x_i\}_{i=1}^n) &= I_s(\{y_i = x_{n-i+1}\}_{i=1}^n) \\ &= \{w_i = 2s - y_i\}_{i=1}^n \\ &= \{w_i = 2s - x_{n-i+1}\}_{i=1}^n = IR_s \\ &= \{w_i = y_{n-i+1}\}_{i=1}^n \\ &= R(\{y_i = 2s - x_i\}_{i=1}^n) = R \circ I_s(\{x_i\}_{i=1}^n) \end{aligned}$$

de donde se concluye que

$$I_s \circ R = IR_s = R \circ I_s,$$

y que también implica que

$$\begin{aligned} IR_s \circ IR_s &= (R \circ I_s) \circ (I_s \circ R) \\ &= R \circ (I_s \circ (I_s \circ R)) \\ &= R \circ ((I_s \circ I_s) \circ R) \\ &= R \circ (\text{id}_{\mathcal{T}(n)} \circ R) \\ &= R \circ R \\ &= \text{id}_{\mathcal{T}(n)}. \end{aligned}$$

Lo anterior quiere decir que la composición de funciones restringida al subconjunto

$$\mathcal{ST}_s = \{I_s, R, IR_s, \text{id}_{\mathcal{T}(n)}\}$$



Figura 1.3: Motivo con simetrías.

del conjunto de transformaciones de  $\mathcal{T}(n)$  en sí mismo es cerrada. Como de suyo la composición es asociativa, tenemos que  $(\mathcal{ST}_s, \circ)$  es un grupo, cuya identidad es  $\text{id}_{\mathcal{T}(n)}$  y los inversos de  $I_s$ ,  $R$  e  $IR_s$  son ellos mismos.

Por ejemplo, tomemos el 5-motivo

$$\{x_1 = A = 9, x_2 = G = 7, x_3 = F = 5, x_4 = E = 4, x_5 = G = 7\}$$

que aparece en el compás 29 de la Fuga 6 en D menor del primer libro del “Das Wohltemperierte Klavier” de J. S. Bach. Si lo invertimos respecto al tono  $G = 7$  (recordando que  $2 \cdot 7 = 14 = 2$ ), obtenemos

$$\begin{aligned} \{y_1 = 2 - x_1 = 5, y_2 = 2 - x_2 = 7, \\ y_3 = 2 - x_3 = 9, y_4 = 2 - x_4 = 10, y_5 = 2 - x_5 = 7\} \end{aligned}$$

que es

$$\{y_1 = F, y_2 = G, y_3 = A, y_4 = Bb, y_5 = G\};$$

y se encuentra en el compás 33.

Si lo retrogradamos, resulta el motivo  $\{y_1 = G, y_2 = E, y_3 = F, y_4 = G, y_5 = A\}$  (pues es simplemente ver al original de adelante hacia atrás) que aparece entre el compás 7 y 8. Si le aplicamos una retrogradación con inversión tenemos  $\{y_1 = G, y_2 = Bb, y_3 = A, y_4 = G, y_5 = F\}$ . Una transposición de este último se aprecia en el compás 36 de la obra.

Las transformaciones del motivo se pueden ver en la figura 1.3, donde a) es el motivo original, b) es su inversión respecto a G, c) es su retrogradación y d) es su retrogradación con inversión respecto a G. Una presentación más geométrica de las transformaciones del motivo de Bach se ve en la figura 1.4.

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  $|G|$  indistintamente. Así, varias formas de escribir esto son:  $(\mathbb{Z}_n, +)$  tiene orden  $n$ ,  $o(\Delta_3, \circ) = 6$ ,  $|\Sigma_3| = 6$ ,  $o(\Sigma_n) = n!$ . Si  $|G|$  es infinito (finito) diremos que  $G$  es infinito (finito). Así,  $\mathbb{Z}$  es (constituye un grupo) infinito (bajo la suma usual).

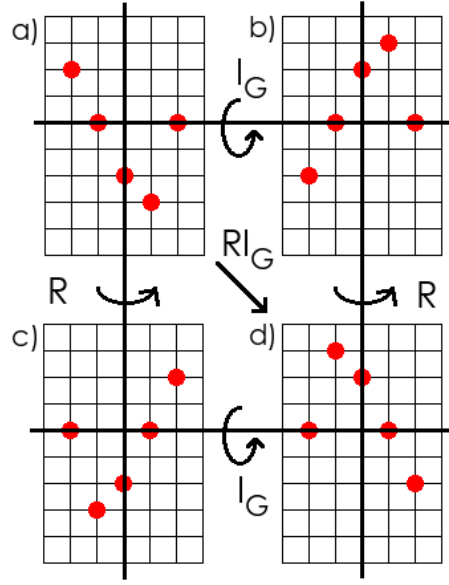


Figura 1.4: Representación geométrica de las simetrías.

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  $f: G \rightarrow G'$  tal que  $f(u \diamond v) = f(u) \star f(v)$ .

**Ejemplo.** Consideremos el conjunto de funciones

$$T = \{e^t : t \in \mathbb{Z}_{12}\}$$

donde definimos

$$\begin{aligned} e^t : \mathbb{Z}_{12} &\rightarrow \mathbb{Z}_{12}, \\ a &\mapsto a + t. \end{aligned}$$

Entonces  $(T, \circ)$  es un grupo, donde  $\circ$  es la composición de funciones. Este grupo es isomorfo a  $(\mathbb{Z}_{12}, +)$ , bajo el isomorfismo

$$\begin{aligned} \phi : \mathbb{Z}_{12} &\rightarrow T, \\ x &\mapsto e^x. \end{aligned}$$

Efectivamente,

$$\phi(x + y) = e^{x+y} = e^x \circ e^y = \phi(x) \circ \phi(y);$$



dejamos al lector demostrar que  $\phi$  es biyectiva y que su inversa también es un homomorfismo.

Desde el punto de vista musical,  $T$  es el grupo de todas las transposiciones, y esto demuestra que es isomorfo a la escala cromática equitemperada. Para más detalles sobre las transposiciones, véase el capítulo 4, sección 4.2.

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

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

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

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

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

**Ejemplo.** Sea  $GL(\mathbb{Z}_{12}) = \{1, 5, 7, 11\} \subseteq \mathbb{Z}_{12}$  (los elementos de  $\mathbb{Z}_{12}$  con inverso multiplicativo). Si  $G = (\mathbb{Z}_{12}, +)$ , entonces definiendo la acción

$$\begin{aligned} \circ : GL(\mathbb{Z}_{12}) \times \mathbb{Z}_{12} &\rightarrow \mathbb{Z}_{12} \\ (u, x) &\mapsto ux \end{aligned}$$

tenemos que  $\mathbb{Z}_{12}$  es un grupo con operadores en  $GL(\mathbb{Z}_{12})$ . Efectivamente

$$\circ(u, x + y) = u(x + y) = ux + uy = \circ(u, x) + \circ(u, y).$$

El conjunto de operadores es, de hecho, un grupo bajo la multiplicación en  $\mathbb{Z}_{12}$ . Recordemos que  $\mathbb{Z}_{12}$  puede interpretarse como la escala temperada módulo octavas, así que estos operadores tienen mucha importancia porque sirven para clasificar acordes, escalas o motivos considerando equivalentes a aquellos que se transforman de acuerdo a  $GL(\mathbb{Z}_{12})$ , y esto tiene un significado musical. Por ejemplo, si  $11 \in GL(\mathbb{Z}_{12})$  actúa en  $\mathbb{Z}_{12}$  invierte los tonos, una operación muy utilizada en el contrapunto y la manipulación de motivos.

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  $\Omega$ , cada elemento de  $\Omega$  (llamado **operador**) define un endomorfismo (i.e. un homomorfismo de  $G \rightarrow G$ ) del grupo  $G$ . Consideremos  $\Omega = \mathbb{Z}$  y para  $x \in G$ ,  $n \in \mathbb{Z}$  definamos

$$\begin{aligned} \circ : \mathbb{Z} \times G &\longrightarrow G, \\ (n, x) &\longmapsto n \circ x = x^n. \end{aligned}$$

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  $\Lambda$  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  $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Z}_n, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(M_n K, +, \cdot)$ ,  $(K, +, \cdot)$ ,  $(K[x], +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$  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  $\Lambda$  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  $\Lambda$  en el grupo conmutativo de  $\Lambda'$  y que también es un homomorfismo del semigrupo de  $\Lambda$  en el semigrupo de  $\Lambda'$ , 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  **$\Lambda$ -módulo (izquierdo)**. Entonces, como caso particular de los  $\Lambda$ -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  $\Lambda$ -módulos, basta tomar  $K = \Lambda$  un anillo conmutativo con 1. En particular, relacionamos dos  $\Lambda$ -módulos mediante un **homomorfismo de  $\Lambda$ -módulos**.

Los  $\Lambda$ -módulos son generalizaciones de los conceptos de grupo conmutativo y de espacio vectorial, y son los objetos de estudio del Álgebra Homológica (véase [L1]). Imitando a los espacios vectoriales, si un  $\Lambda$ -módulo posee una *base*, lo llamaremos  **$\Lambda$ -módulo libre**. No todo  $\Lambda$ -módulo posee base, es decir, no todo  $\Lambda$ -módulo es libre, pero todo espacio vectorial o  $K$ -módulo es libre, es decir, sí posee una base. Diremos que un  $\Lambda$ -módulo es **proyectivo** si es sumando directo de un libre y que es **finitamente generado** si posee un conjunto finito de generadores.

**Ejemplo.** El producto cartesiano  $\mathcal{I} = \mathbb{Z}_{12} \times \mathbb{Z}_{12}$  puede verse como el conjunto de todos los **intervalos de contrapunto** equitemperados: la primera componente representa el tono “base” del intervalo y la segunda su “longitud”. Por ejemplo, el par  $(0, 0)$  representaría al unísono (u octava, no habría diferencia) con tono base C, mientras que el par  $(2, 7)$  representaría una quinta ascendente sobre D (o también una cuarta descendente sobre D)<sup>3</sup>.

En este conjunto podemos definir una suma

$$\begin{aligned} + : \mathcal{I} \times \mathcal{I} &\rightarrow \mathcal{I}, \\ ((a, b), (c, d)) &\mapsto (a + c, b + d). \end{aligned}$$

y una multiplicación por escalar

$$\begin{aligned} \cdot : \mathbb{Z}_{12} \times \mathcal{I} &\rightarrow \mathcal{I}, \\ (k, (c, d)) &\mapsto (kc, kd). \end{aligned}$$

que lo convierte en un  $\mathbb{Z}_{12}$ -módulo. Estas operaciones tienen significado musical. Por ejemplo, la multiplicación por el escalar  $-1 = 11 \in \mathbb{Z}_{12}$  equivale a invertir los intervalos y reflejar el punto base con respecto al tono C. Sumar  $(c, 0)$  a cualquier elemento de la forma  $(a, b)$  equivale a transponer al tono base  $a$  en  $c$  unidades y pero preservando la distancia del intervalo. Tales procedimientos son comunes en el contrapunto.

Un **álgebra** sobre  $\Lambda$  ( $\Lambda$  un anillo conmutativo con uno) es un conjunto  $A$  que simultáneamente es un anillo y un  $\Lambda$ -módulo. Es decir, un álgebra  $(A, +, \mu, \cdot)$  es un  $\Lambda$ -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:

$$\begin{aligned} (\lambda u + \lambda' v)w &= \lambda(uw) + \lambda'(vw) \\ w(\lambda u + \lambda' v) &= \lambda(wu) + \lambda'(wv) \quad \text{para } \lambda, \lambda' \in \Lambda; u, v, w \in A \end{aligned}$$

En particular se tiene que  $(\lambda u)v = \lambda(uv) = u(\lambda v)$  y por lo tanto  $\lambda uv$  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.

<sup>3</sup>Esta ambigüedad se resuelve dándole a un intervalo de contrapunto  $\xi \in \mathcal{I}$  una **orientación**, que es  $+$  si es ascendente y  $-$  si es descendente y se escribe  $(\xi, +)$  o  $(\xi, -)$ . Si no se especifica, se sobreentiende que la orientación es ascendente.

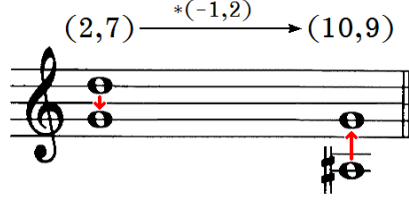


Figura 1.5: Multiplicación del intervalo descendente  $((2, 7), -)$  por  $(-1, 2)$  para obtener  $((10, 9), +)$ .

**Ejemplo.** Podemos definir una multiplicación en  $\mathcal{I}$  de la siguiente manera:

$$\begin{aligned} * : \mathcal{I} \times \mathcal{I} &\rightarrow \mathcal{I}, \\ ((a, b), (c, d)) &\mapsto (ac, ad + bc). \end{aligned}$$

De esta manera  $(\mathcal{I}, +, \cdot, *)$  se convierte en una álgebra sobre  $\mathbb{Z}_{12}$ , pues por un lado

$$\begin{aligned} ((a, b) + (c, d)) * (u, v) &= (a + c, b + d) * (u, v) \\ &= ((a + c)u, (a + c)v + (b + d)u) \\ &= (au + cu, av + cv + bu + du) \\ &= (au, av + bu) + (cu, cv + du) \\ &= (a, b) * (u, v) + (c, d) * (u, v), \end{aligned}$$

por otro

$$\begin{aligned} (u, v) * ((a, b) + (c, d)) &= (u, v) * (a + c, b + d) \\ &= (u(a + c), u(b + d) + v(a + c)) \\ &= (ua + uc, ub + ud + va + vc) \\ &= (ua, va + ub) + (uc, ud + cv) \\ &= (u, v)(a, b) + (u, v)(c, d) \end{aligned}$$

y también

$$\begin{aligned} (k \cdot (a, b)) * (u, v) &= (ka, kb) * (u, v) \\ &= (kau, kav + kbu) \\ &= k(au, av + bu) = k \cdot ((a, b) * (u, v)). \end{aligned}$$

Esta multiplicación es significativa desde el punto de vista musicológico. Para dar una razón, definamos primero las funciones

$$\begin{aligned} \alpha_+ : \mathcal{I} &\mapsto \mathbb{Z}_{12}, \\ (x, y) &\mapsto x + y, \end{aligned}$$

y

$$\begin{aligned}\alpha_- : \mathcal{I} &\mapsto \mathbb{Z}_{12}, \\ (x, y) &\mapsto x - y.\end{aligned}$$

Las funciones  $\alpha_+$  y  $\alpha_-$  permiten, dado un intervalo de contrapunto  $(x, y) \in \mathcal{I}$ , recuperar el “extremo” del intervalo dependiendo de su orientación. Por ejemplo, si  $((7, 7), +)$  es la quinta *ascendente* sobre G, el “extremo” lo podemos obtener sumando al tono base la “longitud” del intervalo

$$\alpha_+(7, 7) = 7 + 7 = 2$$

es decir, el tono de D. Si ahora  $((2, 7), -)$  es la quinta *descendente* sobre D, el “extremo” resulta de restar al tono base la “longitud” del intervalo

$$\alpha_-(2, 7) = 2 - 7 = 7,$$

que es el tono de G.

Observemos que

$$\begin{aligned}\alpha_+((-1, 2) * (x, y)) &= \alpha_+(-x, 2x - y) \\ &= -x + (2x - y) \\ &= x - y = \alpha_-(x, y).\end{aligned}$$

Esta relación, en términos musicales, nos dice que si tenemos al intervalo de contrapunto descendente  $((x, y), -)$  con extremo  $x - y$ , lo podemos cambiar por el intervalo de contrapunto ascendente

$$((-1, 2) * (x, y), +) = ((-x, 2x - y), +)$$

si nos interesa que se preserve su “extremo”. Por ejemplo, a la quinta descendente sobre D  $((2, 7), -)$  la cambiamos por

$$((-1, 2) * (2, 7), +) = ((-2, 4 - 7), +) = ((10, 9), +),$$

que es la sexta mayor ascendente sobre A $\sharp$ . Ambos intervalos de contrapunto tienen como “extremo” al tono G (figura 1.5).

Lo anterior es importante en el contrapunto, donde generalmente se requiere que los intervalos que hay entre dos voces tengan una misma orientación (ya sea ascendente o descendente). Si llegan a tener direcciones opuestas en algún momento (como cuando se cruzan las voces), entonces podemos cambiar la orientación de algunos intervalos multiplicándolos por  $(-1, 2)$  hasta uniformarla, pero preservando invariante una de las voces.

Para más detalles sobre el significado musicológico de  $\mathcal{I}$  visto como  $\mathbb{Z}_{12}$ -álgebra y sus aplicaciones al contrapunto, puede consultarse [M], parte VII.

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.**  $(M_n K, +, \cdot, \mu)$ , donde  $M_n K$  denota las matrices cuadradas de  $n \times n$  con coeficientes en un campo  $K$  ( $\mu$  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  $A = (A_0, A_1, A_2, \dots)$  de álgebras  $A_i$ , una para cada índice  $i \in \mathbb{N}$ .

Para quienes han estudiado, dentro de un curso elemental de Álgebra Lineal, el Álgebra Multilineal (como en [L12]), recordarán los siguientes conceptos que no son requisitos para este texto.

**2.10 Ejemplo.** Sea  $T^k(V) = \otimes^k V = V \otimes_K \dots \otimes_K V$  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

$$\cdot : T^k V \times T^l V \rightarrow T^{k+l} V \text{ mediante} \\ (u_1 \otimes \dots \otimes u_k) \cdot (v_1 \otimes \dots \otimes v_l) = u_1 \otimes \dots \otimes u_k \otimes v_1 \otimes \dots \otimes v_l$$

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

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

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

Entonces tenemos un álgebra graduada

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

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.

### 1.3. 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

$$\cdot: G \times G \rightarrow G$$

es una operación binaria

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

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  $\emptyset$  (con acción, la única posible de  $\emptyset$  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  $xa' = y$ . Entonces  $xa = xa'$ , luego  $a = a'$ . 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

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

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

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  $f: G \rightarrow G'$  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  $f: G \rightarrow G'$  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  $f: G \rightarrow G'$  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  $f: G \rightarrow G'$  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  $f: G' \rightarrow G$  y  $g: G \rightarrow G''$  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  $f: G \rightarrow G'$  un homomorfismo de grupos. Diremos que  $f$  es un **isomorfismo**, y escribiremos  $f: G \xrightarrow{\cong} G'$  si existe un homomorfismo  $g: G' \rightarrow G$  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,  $f: G \rightarrow G'$

es isomorfismo si, y sólo si, es biyectiva. Diremos que dos grupos  $G$  y  $G'$  son **isomorfos** si existe un isomorfismo  $f : G \xrightarrow{\cong} G'$  y escribiremos  $G \cong G'$ .

**3.12 Definición.** Sea  $f : G \rightarrow G'$  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  $\operatorname{im} f$ , 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  $\operatorname{im} f = G'$  diremos que  $f$  es un **epimorfismo** y lo denotamos  $f : G \twoheadrightarrow G'$  y si  $f$  es tal que  $\ker f = \{e\}$  e  $\operatorname{im} f = G'$  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  $f : G \rightarrow G$  y diremos que es **automorfismo** si dicha  $f$  es biyectiva.

**3.13 Proposición.** Sean  $f : G' \rightarrow G$ ,  $g : G \rightarrow G''$  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  $f : G \rightarrow G'$  es **trivial** si  $f(x) = e'$  para todo  $x \in G$ . Es decir,  $\operatorname{im} f = \{e'\}$ . 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 **subgrupo** 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 subgrupo 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,  $x + y \in \cap_i H_i$ ,  $e \in \cap_i H_i$ ,  $x^{-1} \in \cap_i H_i$ . ♦

**3.19 Proposición.** Sea  $f : G \rightarrow G'$  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  $f(H) = \{f(x) | x \in H\}$  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  $f : G \rightarrow G'$  un homomorfismo de grupos. Entonces  $\text{im } f$  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  $\text{Hom}(X, Y)$  el conjunto de homomorfismos del grupo abeliano  $X$  en el grupo abeliano  $Y$ . Sean  $f, g : X \rightarrow Y$  homomorfismos de grupos abelianos y definamos  $f + g : X \rightarrow Y$  mediante  $(f + g)(x) = f(x) + g(x)$ . Es fácil comprobar que esta definición hace de  $\text{Hom}(X, Y)$  un grupo abeliano, (Problema 3.21).

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

$$\psi_* = \text{Hom}(X, \psi): \text{Hom}(X, Y') \rightarrow \text{Hom}(X, Y)$$

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

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

$$\varphi^* = \text{Hom}(\varphi, Y): \text{Hom}(X, Y) \rightarrow \text{Hom}(X', Y)$$

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

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

$$\begin{array}{ccc} (X \xrightarrow{f} Y') & \in & \text{Hom}(X, Y') \\ \parallel \downarrow \psi & & \downarrow \psi_* \\ (X \xrightarrow{g} Y) & \xrightarrow{1_Y} & \text{Hom}(X, Y) \\ \parallel \downarrow \psi' & & \downarrow \psi'_* \\ (X \xrightarrow{h} Y'') & \in & \text{Hom}(X, Y'') \end{array} \quad \begin{array}{c} \curvearrowright \psi'_* \circ \psi_* \end{array}$$

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

$$\begin{array}{ccc} (X' \xrightarrow{f} Y) & \in & \text{Hom}(X', Y) \\ \downarrow \varphi \parallel & & \uparrow \varphi^* \\ (X \xrightarrow{g} Y) & \xrightarrow{1_X} & \text{Hom}(X, Y) \\ \downarrow \varphi' \parallel & & \uparrow \varphi'^* \\ (X'' \xrightarrow{h} Y) & \in & \text{Hom}(X'', Y) \end{array} \quad \begin{array}{c} \curvearrowright (\varphi' \circ \varphi)^* \end{array}$$

## 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 diedral** 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  $f: G \rightarrow G'$  dado por  $f(u_1, \dots, u_n) = (u_1, u_2, \dots, u_{n-1}, 0)$  es un homomorfismo.

**3.9** Sea  $G$  un grupo. Pruebe que la función  $1_G: G \rightarrow G$  y la función  $O_G: G \rightarrow G$  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)  $f: K^n \rightarrow K^m$ ,  $f(x) = Ax$  donde  $A$  es una matriz de  $m \times n$  con elementos en el campo  $K$ .

(ii)  $f: K^2 \rightarrow K^2$ ,  $f(x, y) = (4y, 0)$ .

(iii)  $f: K^3 \rightarrow K^3$ ,  $f(x, y, z) = (-z, x, y)$ .

(iv)  $f: K^2 \rightarrow K^2$ ,  $f(x, y) = (x^2, 2y)$ .

(v)  $f: K^5 \rightarrow K^4$ ,  $f(u, v, x, y, z) = (2uy, 3xz, 0, 4u)$ .

(vi)  $f: K^3 \rightarrow K^3$ ,  $f(x, y, z) = (x + 2, y + 2, z + 2)$ .

**3.11** Establezca, si es posible, homomorfismos no triviales en los siguientes casos:

(i)  $1 \longrightarrow \mathbb{Z}_2$ .

(ii)  $\mathbb{Z}_2 \xrightarrow{\times 2} \mathbb{Z}_4$ .

(iii)  $\mathbb{Z}_4 \longrightarrow \mathbb{Z}_2$ .

(iv)  $\mathbb{Z}_2 \longrightarrow 1$ .

(v)  $\mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ .

$$(vi) \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2.$$

$$(vii) \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2.$$

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

**3.13** Pruebe que si  $f: G \rightarrow G'$  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  $f: G \rightarrow G'$  un homomorfismo de grupos biyectivo. Pruebe que la función inversa  $f^{-1}: G' \rightarrow G$  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  $f: G \rightarrow G'$  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  $f: G \rightarrow G'$  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  $f: X \times Y \rightarrow G$  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

$$(i) f(\lambda x, y) = \lambda f(x, y) = f(x, \lambda y) \text{ para toda } x \in X, y \in Y \text{ y } \lambda \in \mathbb{Z}.$$

$$(ii) f \text{ nunca es inyectiva a menos que } X = Y = 0.$$

**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  $f, g: X \rightarrow Y$  homomorfismos de grupos abelianos y definamos  $f + g: X \rightarrow Y$  mediante  $(f + g)(x) = f(x) + g(x)$ . Pruebe que esta definición hace de  $Hom(X, Y)$  un grupo abeliano.

**3.22** Sea  $\psi: Y' \rightarrow Y$  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

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

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

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

$$\varphi^* = \text{Hom}(\varphi, Y): \text{Hom}(X, Y) \rightarrow (X', Y)$$

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

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

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

## 1.4. Grupos Cíclicos

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

**4.1 Proposición.** El conjunto  $\{x^n | n \in \mathbb{Z}\}$  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  $x^{n-1}, \dots, x^1, e = x^n$  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. ♦



**Ejemplo.** Consideremos el subgrupo cíclico infinito de  $(\mathbb{R}^*, \cdot)$  (los números reales no nulos con la multiplicación usual) generado por el elemento

$$x = \sqrt[12]{2}. \quad (1.1)$$

El número  $x$  es, por definición, el cociente de las frecuencias entre un tono y otro que está un **semitono** por arriba (véase el capítulo 4, sección 1). Los números  $x^k$  (salvo multiplicar por una constante) corresponden a las frecuencias en hercios de los tonos utilizados en la Música con la afinación equitemperada.

Por el teorema 4.7 se tiene que  $(x)$  es isomorfo a  $(\mathbb{Z}, +)$ . Abusaremos de este isomorfismo para asociarle un tono a cada elemento del grupo  $(\mathbb{Z}, +)$  o al grupo  $(\mathbb{Z}_{12}, +)$ , como puede verse en la sección 2 del capítulo 3.

Además, tal isomorfismo refleja el modo en que nuestro cerebro interpreta las distancias (o intervalos) musicales (para más detalles, véase la sección 2 del capítulo 3 y la sección 1 del capítulo 4).

**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  $n|j - k$ . 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

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

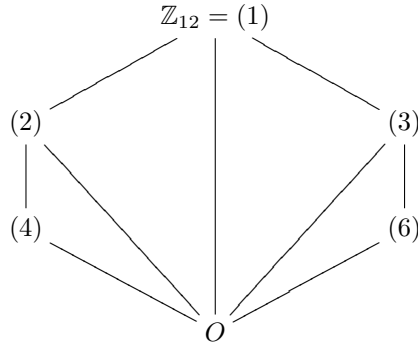
forman un subgrupo cíclico de  $(x)$  de orden  $m$ .

También, si  $N$  es un subgrupo no trivial de  $(x)$  podemos tomar el menor entero positivo  $m$  tal que  $x^m \in N$ . Como  $e = x^n = x^{mq}$ ,  $m|n$  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  $x$ ,

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

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



## 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 2

## 2.1. 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  $\text{im } f_{i-1} \subset \ker f_i$ . 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  $\text{im } f_{i-1} \subset \ker f_i$ . 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  $f_{i-1}(x) \in \text{im } f_{i-1} \subset \ker f_i$ , 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  $y \in \text{im } f_{i-1}$  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  $y \in \text{im } f_{i-1}$ , entonces  $y \in \ker f_i$  para cualquier  $y$ . Luego,  $\text{im } f_{i-1} \subset \ker f_i$ . ♦

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

Equivalentemente, dicha sucesión es exacta en  $G_i$  si, y sólo si,  $\text{im } f_{i-1} = \ker f_i$ . 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  $\text{im } h = \{0\} = \ker f$ ,  $\text{im } f = \{0, 2\} = \ker g$ , e  $\text{im } g = \{0, 1\} = \ker k$ . 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  $\text{im } h = \{0\} = \ker f$ ,  $\text{im } f = \{(0, 0), (1, 0)\} = \ker g$ , e  $\text{im } g = \{0, 1\} = \ker k$ . Luego, es una sucesión exacta corta.

**Ejemplo.** Sea  $M$  un  $R$ -módulo (que ciertamente es un grupo bajo la adición), y

$$M^k = \underbrace{M \oplus M \oplus \cdots \oplus M}_k.$$

En una primera aproximación, los objetos musicales (llámese una escala, un acorde, un motivo, el ritmo) pueden verse como un subconjunto de algún módulo  $M^k$  apropiado. Es de gran interés en la Teoría Matemática de la Música

clasificar a los objetos musicales salvo isomorfismos de  $M^k$  que tengan algún significado musical. Por ejemplo, ¿cuántas acordes o escalas diferentes hay si consideramos equivalentes a todas sus transposiciones? o ¿cuántos motivos hay si las permutaciones de sus elementos se consideran esencialmente el mismo motivo?

Una sucesión exacta corta que se utiliza en la clasificación de objetos musicales es

$$0 \rightarrow M \xrightarrow{\Delta_{n+1}} M^{n+1} \xrightarrow{d_{n+1}} M^n \rightarrow 0$$

donde  $\Delta_k$  es el morfismo diagonal

$$\begin{aligned} \Delta_k : M &\rightarrow M^k, \\ m &\mapsto \underbrace{(m, m, \dots, m)}_k \end{aligned}$$

y  $d_{k+1}$  el morfismo de diferencias

$$\begin{aligned} d_{k+1} : M^{k+1} &\rightarrow M, \\ (m_0, \dots, m_k) &\mapsto (m_1 - m_0, \dots, m_k - m_0). \end{aligned}$$

Como  $\Delta_{n+1}(m) = 0$  si y sólo si  $m = 0$ , tenemos que  $\ker \Delta_{n+1} = 0$ . También

$$d_{n+1}(m_0, \dots, m_n) = (m_1 - m_0, \dots, m_n - m_0) = (0, \dots, 0)$$

si, y sólo si,  $m_k = m_0$  para  $k = 1, \dots, n$ . Por lo tanto,  $\ker d_{n+1} = \text{im } \Delta_{n+1}$ . Finalmente,  $d_{n+1}$  es suprayectiva, pues para cualquier  $(m_1, \dots, m_n)$  se tiene que

$$d_{n+1}(0, m_1, \dots, m_n) = (m_1 - 0, \dots, m_n - 0) = (m_1, \dots, m_n).$$

En otras palabras,  $\text{im } d_{n+1} = M^n$ .

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

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

con  $f$  epimorfismo y  $h$  monomorfismo. Entonces  $\text{im } f = H$  y  $\ker h = e$ . Como la sucesión es exacta,  $H = \text{im } f = \ker g$  e  $\text{im } g = \ker h = e$ ; 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

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

la escribiremos indistintamente como

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

donde  $\xrightarrow{f}$  denota inyectividad y  $\xrightarrow{g}$  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  $f \circ f' = g \circ g': G \longrightarrow H'$ .

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

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

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  $h: G \rightarrow H$  compatible con los isomorfismos dados y el diagrama conmuta. Por ejemplo, si consideramos el siguiente diagrama

$$\begin{array}{ccccccc}
 e & \longrightarrow & \mathbb{Z}_2 & \xrightarrow{\times 2} & \mathbb{Z}_4 & \longrightarrow & \mathbb{Z}_2 \longrightarrow e \\
 \parallel & & \parallel & & & & \parallel & \parallel \\
 e & \longrightarrow & \mathbb{Z}_2 & \longrightarrow & \mathbb{Z}_2 \times \mathbb{Z}_2 & \longrightarrow & \mathbb{Z}_2 \longrightarrow e
 \end{array}$$

hemos visto que  $\mathbb{Z}_2 \times \mathbb{Z}_2$  no es isomorfo a  $\mathbb{Z}_4$ .

Sea  $\{C_n\}_{n \in \mathbb{Z}}$  una familia de grupos abelianos y  $\{\partial_n : C_n \rightarrow C_{n-1}\}_{n \in \mathbb{Z}}$  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

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

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**  $\varphi : C \rightarrow D$  es una familia de homomorfismos de grupos abelianos  $\{\varphi_n : C_n \rightarrow D_n\}$  tal que los cuadrados, en el siguiente diagrama conmutan:

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

## Problemas

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

$$\begin{array}{ccccccc}
 O & \longrightarrow & \mathbb{Z}_p & \longrightarrow & \mathbb{Z}_{p^2} & \longrightarrow & \mathbb{Z}_p \longrightarrow O \\
 O & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z}_p \longrightarrow O
 \end{array}$$

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  $e \rightarrow G \rightarrow e$  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  $\{C^n\}_{n \in \mathbb{Z}}$  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  $C = \{C^n, \delta^n\}$ , y lo escribimos

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

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**  $\Psi : C \longrightarrow D$ .

## 2.2. 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

$$+ : G/H \times G/H \rightarrow G/H$$

dada por

$$((x + H), (y + H)) \mapsto ((x + y) + H).$$

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  $p: G \rightarrow G/H$  dada por  $x \mapsto x + H$ . 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  $x \equiv y \pmod{3}$  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  $x \equiv_i y \pmod{H}$ . Análogamente, diremos que  $x$  es **congruente por la derecha con  $y$**  si  $xy^{-1} \in H$  y la denotamos con  $x \equiv_d y \pmod{H}$ .

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  $x \equiv_i x \pmod{H} \iff x^{-1}x = e \in H$ , se tiene la reflexibilidad. Como  $x \equiv_i y \pmod{H} \iff x^{-1}y \in H \iff (x^{-1}y)^{-1} \in H \iff y^{-1}x \in H \iff y \equiv_i x \pmod{H}$  se tiene la simetría. Finalmente, si  $x \equiv_i y \pmod{H}$  y  $y \equiv_i z \pmod{H}$  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  $x \equiv_i z \pmod{H}$  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

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

y

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

respectivamente.

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

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

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  $H \triangleleft G$ ) si para toda  $x \in G$ ,  $xHx^{-1} \subset H$  donde  $xHx^{-1} = \{xhx^{-1} | h \in H\}$ .

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.  $\blacklozenge$

**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,

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

**2.7 Corolario.** Si  $H \triangleleft G$  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.  $\blacklozenge$

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

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

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  $o(H) | o(G)$ .

**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,  $o(H) | o(G)$ . ♦

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  $2 \leq o((x)) | p$ . 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  $h : (x) \rightarrow H$  un homomorfismo de grupos. Entonces  $\text{im } h = h((x))$  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  $\text{im } h$  pues  $h(e) = (h(x^n))^n = [h(x)]^n = e$ . ♦

**Ejemplo.** El cerebro humano percibe dos tonos como esencialmente idénticos cuando sus frecuencias guardan una razón igual a  $2^r$  con  $r \in \mathbb{Z}$ . Es decir, “identifica” dos frecuencias  $u, w \in (x) < (\mathbb{R}^*, \cdot)$  cuando  $u^{-1}w \in (x^{12})$ , donde  $x$  es el número real dado por la ecuación (1.1). Efectivamente,

$$x^{12} = (\sqrt[12]{2})^{12} = 2$$

y  $u^{-1}w = \frac{w}{u} \in (2) = (x^{12})$  significa que  $\frac{w}{u} = 2^r$  para algún  $r \in \mathbb{Z}$ .

Puesto que

$$\begin{aligned} h : \mathbb{Z} &\rightarrow (x), \\ n &\mapsto x^n, \end{aligned}$$

define un isomorfismo entre  $\mathbb{Z}$  y  $(x)$ , resulta que para la percepción humana los tonos esencialmente distintos son aquellos del cociente

$$\frac{(x)}{(x^{12})} \cong \frac{\mathbb{Z}}{12\mathbb{Z}} = \mathbb{Z}_{12};$$

el lector debe verificar que, efectivamente,  $(x^{12}) \cong 12\mathbb{Z}$  bajo el isomorfismo  $h$ .

Así se justifica el abuso de nomenclatura al identificar tanto a un elemento de  $\mathbb{Z}$  como a uno de  $\mathbb{Z}_{12}$  con un tono. Esto también es muy útil para definir rigurosamente el concepto de escala. Una **escala**  $E$  es un subconjunto de  $\mathbb{Z}$  (al que vemos como tonos) tal que

$$e^{12}(E) = E + 12 = E$$

es decir,  $x + 12 \in E$  para todo  $x \in E$ .

Las escalas se comportan bien bajo la proyección canónica  $p : \mathbb{Z} \rightarrow \mathbb{Z}_{12} = \frac{\mathbb{Z}}{12\mathbb{Z}}$ , en el sentido de que

$$p^{-1}(p(E)) = E.$$

Al conjunto  $p(E) \subseteq \mathbb{Z}_{12}$  se le llama **acorde de la escala**<sup>1</sup>. Generalmente se abusa de la nomenclatura al referirse a una escala por su acorde, como en el ejemplo de la sección 1 del capítulo 1.

De hecho, dado un subconjunto  $S \subseteq \mathbb{Z}_{12}$ , podemos definir una escala a través de

$$E = p^{-1}(S);$$

el lector debe demostrar que esto efectivamente define una escala y que el acorde de dicha escala es precisamente  $S$ . Por ejemplo, la escala que proviene de  $S = \mathbb{Z}_{12}$  es justamente la escala cromática.

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

Los elementos de  $C_n$  se conocen como **cadenas de grado  $n$** , y los homomorfismos  $\partial_n$  se llaman **diferenciales** u **operadores frontera**. Los elementos del núcleo de  $\partial_n$  se denominan **ciclos de grado  $n$** , denotados con  $Z_n(C)$  y los elementos de la imagen de  $\partial_{n+1}$  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  $n \in \mathbb{Z}$ , definimos un grupo de homología  $H_n(C)$ . Denominamos a  $H_*(C) = \{H_n(C)\}$  **homología de la cadena  $C$** .

<sup>1</sup>En el capítulo 3, sección 2, se verá que este nombre es muy apropiado.

## 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  $\Delta_3$  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  $(xH)(yH) = (xy)H$  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  $C$** ,  $H^n(C)$ .

## 2.3. 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

$$\iota_x : G \longrightarrow G \text{ dado por} \\ y \mapsto xyx^{-1}$$

es un automorfismo de  $G$ , ver Problema 3.1, llamado **automorfismo interior**. En estos 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  $H \triangleleft G$  y  $H' \triangleleft G'$ . 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  $\text{im } g^* = p'(\text{im } g)$  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

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

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

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

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  $\text{im } g^* = p'(\text{im } g)$  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:

$$\begin{array}{ccc} G & \xrightarrow{g} & G' \\ p \downarrow & & \cong \downarrow I_{G'} \\ G/\ker g & \xrightarrow{g^*} & G'. \end{array}$$

**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  $\text{im } g^* = p'(\text{im } g) = G'$  entonces  $g^*$  es epimorfismo y por lo tanto es isomorfismo.

Así, se tiene el siguiente diagrama conmutativo

$$\begin{array}{ccc} G & \xrightarrow{g} & G' \\ p \downarrow & & \cong \downarrow I_{G'} \\ G/\ker g & \xrightarrow{g^*} & G'. \end{array}$$

♦

**3.4 Teorema.** Sean  $H \triangleleft G$  y, como caso particular del teorema anterior,  $e = H' \triangleleft G'$  con  $H \subset \ker g$ . Entonces existe un homomorfismo único  $g^* : G/H \rightarrow G'$  dado por  $xH \mapsto g^*(xH) = g(x)H' = g(x)$ . Además,  $\ker g^* = \ker g/H$  e  $\text{im } g = \text{im } g^*$ .  $g^*$  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,  $xH \in \ker g^*$  si, y sólo si  $g(x) = e$ , lo cual sucede si, y sólo si  $x \in \ker g$ . Así,  $\ker g^* = \{xH | x \in \ker g\} = \ker g/H$ . Claramente  $\text{im } g = \text{im } g^*$ . 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  $G/\ker g \cong \text{im } g$ .

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

En otras palabras, si  $g : G \rightarrow G'$  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 isomorfa

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  $\text{im } g = \text{im } g^*$ . Este resultado,  $G/\ker g \cong \text{im } g$  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  $i : H \rightarrow G$  el monomorfismo de inclusión y  $p : G \rightarrow G/H$  el epimorfismo de proyección. Entonces  $\text{im } i = H = \ker p$  y, por lo tanto,

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

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  $\text{im } f = \ker g$ ,  $f$  es monomorfismo (pues  $e = \text{im } h = \ker f$ ) y, además,  $g$  es epimorfismo (pues  $\text{im } g = \ker k = G''$ ). Sea  $H = \text{im } f = \ker g$  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.**  $g : G \rightarrow G'$  donde  $G = \mathbb{Z}$  y  $G' = \mathbb{Z}_n$  es un epimorfismo con núcleo el subgrupo  $n\mathbb{Z}$ , es decir,

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

es una 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  $x \mapsto g(x) = |x|$  donde  $|x|$  denota el valor absoluto de  $x$ . El núcleo de  $g$  es  $\{\pm 1\}$ . Entonces la sucesión

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

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

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

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  $HN = \{xy | x \in H, y \in N\}$ .

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

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

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  $H < G$ ,  $N \triangleleft G$ . Entonces  $(HN)/N \cong H/(H \cap N)$ .

**Demostración.** Como  $N \triangleleft G$ , es fácil ver que  $(H \cap N) \triangleleft H$ . 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  $x^{-1} x_1 = y y_1^{-1}$ . 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  $N \triangleleft G$ ,  $x_1 y_2 = y_2 x_3$ . 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  $\ker h = \{xy \in HN | x \in H \cap N\} = H/(H \cap N) = N$  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  $H \triangleleft G$  y  $N \triangleleft G$  con  $N < H$ . Entonces,  $G/H \cong (G/N)/(H/N)$ .

**Demostración.** Definamos

$$h : G \longrightarrow (G/N)/(H/N) \text{ mediante} \\ x \mapsto (xN)(H/N).$$

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,  $G/H \cong (G/N)/(H/N)$ .

$$\begin{array}{ccccc} \ker h & \xrightarrow{\subset} & G & \xrightarrow{\quad} & G/H \\ \parallel & & \downarrow & \searrow h & \downarrow \cong \\ H & & G/N & \longrightarrow & (G/N)/(H/N) \end{array}$$

◆

**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

$$\iota_x : G \longrightarrow G \text{ dado por} \\ y \mapsto xyx^{-1}$$

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

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

**3.3** Considere el conjunto  $\text{Aut}(G)$  de todos los automorfismos de un grupo  $G$ . Pruebe que  $\text{Aut}(G)$  es un grupo bajo la composición y que  $\text{In}(G) \triangleleft \text{Aut}(G)$ . 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  $\text{Aut}(G)/\text{In}(G)$  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  $\text{im } g^* = p'(\text{im } g)$  y  $\ker g^* = p(g^{-1}(H'))$ .

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

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

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

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

$$e \longrightarrow \ker g \longrightarrow G \longrightarrow G'' \longrightarrow \text{coker } g \longrightarrow e$$

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

**3.7** Pruebe que un homomorfismo de grupos  $g : G \rightarrow G''$  es monomorfismo (escribase como repaso) si, y sólo si,  $\ker g = e$  y que es epimorfismo si, y sólo si,  $\text{coker } g = e$ .

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

## 2.4. Productos

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

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

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

$$\prod_{i \in I} G_i = \{(x_1, \dots, x_n) | x_i \in G_i\}$$

el cual tiene una estructura de grupo dada por

$$(x_1, \dots, x_n)(y_1, \dots, y_n) = (x_1 y_1, \dots, x_n y_n).$$

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



Figura 2.1: Un motivo de tres notas.

**Ejemplo.** La suma directa completa

$$\mathbb{Z}_m \oplus \mathbb{Z}_n$$

se usa en la Teoría Matemática de la Música para estudiar los motivos en escalas  $n$ -temperadas y con inicios<sup>2</sup>  $m$ -cíclicos. De modo más específico, si

$$\begin{aligned} p_1 : \mathbb{Z}_m \oplus \mathbb{Z}_n &\rightarrow \mathbb{Z}_m, \\ (x, y) &\mapsto x \end{aligned}$$

es la primera proyección, un **motivo**  $\mu$  en  $\mathbb{Z}_m \oplus \mathbb{Z}_n$  es un elemento del conjunto potencia<sup>3</sup>  $\wp(\mathbb{Z}_m \oplus \mathbb{Z}_n)$  de  $\mathbb{Z}_m \oplus \mathbb{Z}_n$  tal que  $p_1(u) \neq p_1(v)$  para todo  $u, v \in \mu$ . La idea es que, dado un inicio  $t$ , no concurren en él más de una nota.

Por ejemplo,  $\{(0, 0), (1, 2), (2, 4)\} \subseteq \mathbb{Z}_3 \oplus \mathbb{Z}_{12}$  representa el motivo C, D, E (en ese orden) en un compás ternario, como el que se ve en la figura 2.1. Por otro lado, el conjunto  $\{(0, 0), (1, 2), (1, 4)\} \subseteq \mathbb{Z}_3 \oplus \mathbb{Z}_{12}$  no es un motivo pues  $p_1(1, 2) = 1 = p_1(1, 4)$ , lo que significaría que en el inicio 1 concurren los tonos C y D.

Recordemos que el producto cartesiano  $\prod_{i \in I} X_i$  de una familia de conjuntos  $\{X_i\}_{i \in I}$  es el conjunto de funciones  $h : I \rightarrow \bigcup_{i \in I} X_i$  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

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

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

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

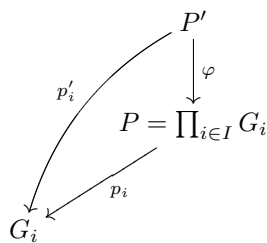
<sup>2</sup>Traducimos como *inicio* la voz inglesa *onset*, que corresponde al punto en un compás en el que inicia el sonido de una nota.

<sup>3</sup>El símbolo  $\wp X$  denota el conjunto potencia de  $X$ .

**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  $\varphi : G \longrightarrow \prod_{i \in I} G_i$  tal que  $p_i \circ \varphi = \varphi_i$  para toda  $i \in I$ .

$$\begin{aligned} g &\mapsto h_g : I \longrightarrow \cup G_i \\ i &\longmapsto h_g(i) = \varphi_i(g) \in G_i. \end{aligned}$$
$$\begin{array}{ccc}
 & G & \\
 \varphi_i \swarrow & \downarrow \varphi & \\
 G_i & \leftarrow p_i & \prod_{i \in I} G_i
 \end{array}$$
$$(\varphi'(g))(i) = p_i \varphi'(g) = \varphi_i(g) = h_g(i) = (\varphi(g))(i).$$

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:



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

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

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,  $\varphi$  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  $\prod_{i \in I} G_i$  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  $\sum_{i \in I} G_i$ . 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  $\gamma : \sum_{i \in I} G_i \longrightarrow G$  tal que  $\gamma \circ \iota_i = \gamma_i$  para toda  $i \in I$ .

**Demostración.** Consideremos elementos distintos de cero  $g_{i_1}, \dots, g_{i_s} = \{g_{i_j}\} \in$



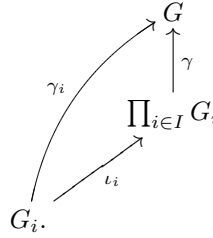
$\sum_{i \in I} G_i$  y defínase

$$\gamma : \sum_{i \in I} G_i \longrightarrow G \quad \text{mediante}$$

$$0 \mapsto 0,$$

$$\{g_i\} \mapsto \gamma(\{g_i\}) = \gamma_{i_1}(g_{i_1}) + \dots + \gamma_{i_s}(g_{i_s}) = \sum_{j=1}^s \gamma_{ij}(g_{ij}),$$

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



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

$$\eta(\{g_i\}) = \eta\left(\sum \iota_j(g_j)\right) = \sum \gamma_i(g_i) = \sum \gamma \iota_i(g_i) = \gamma\left(\sum \iota_i(g_i)\right) = \gamma(\{g_i\}).$$

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

Este teorema determina a  $\sum_{i \in I} G_i$  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  $(x, y) \mapsto h(x, y) = xy$ .  $h$  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 **producto 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  $\text{Hom}(\sum_{i \in I} X_i, Y) \cong \prod_{i \in I} \text{Hom}(X_i, Y)$ .

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

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

el homomorfismo  $0: X_i \rightarrow Y$  es tal que  $0 = \varphi \circ \iota_i$ . Luego,  $\varphi = 0$ . Por lo tanto,  $\ker \rho = \{0\}$ . Veamos que  $\rho$  es un epimorfismo: sea  $(\varphi_i)_{i \in I} \in \prod_{i \in I} \text{Hom}(X_i, Y)$ . Entonces tenemos  $\varphi_i: X_i \rightarrow Y$  para cada  $i \in I$ . Por la propiedad universal de la suma directa, existe un homomorfismo  $\varphi: \sum_{i \in I} X_i \rightarrow Y$  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  $H \triangleleft G$  y  $N \triangleleft G$ , entonces  $HN \triangleleft G$ .

**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  $\iota_j: G_j \rightarrow \prod_{i \in I}^d G_i$  dado por  $\iota_j(g) = \{g_i\}_{i \in I}$  donde

$$g_i = \begin{cases} e, & \text{para } i \neq j, \\ g, & \text{para } i = j, \end{cases}$$

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

**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  $\mathbb{Z}_3 \times \mathbb{Z}_3 \not\cong \mathbb{Z}_9$ . (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  $\{G_i\}$ ,  $\prod_{i \in I} G_i = \{(x_1, \dots, x_n) | x_i \in G_i\}$  tiene una estructura de grupo dada por

$$(x_1, \dots, x_n)(y_1, \dots, y_n) = (x_1 y_1, \dots, x_n y_n)$$

y que es abeliano si cada grupo de la familia lo es.

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

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

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

dada por  $f \mapsto f(j)$  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  $H_1 \triangleleft G_1$  y  $H_2 \triangleleft G_2$  subgrupos normales. Pruebe que  $H_1 \times H_2 \triangleleft G_1 \times G_2$  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  $\text{Hom}(X, \prod_{i \in I} Y_i) \cong \prod_{i \in I} \text{Hom}(X, Y_i)$ .

# Capítulo 3

## 3.1. 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  $\lambda_i$  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

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

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  $m_i | m_{i+1}$  para  $1 \leq i \leq n-1$ .

Esto quiere decir que  $G$  es de la forma

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

Los enteros  $m_i$  se llaman **coeficientes de torsión** de  $G$ . Estos 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  $m_i|m_{i+1}$  para  $1 \leq i \leq n-1$ .

Esto es, en el caso (i)  $G \cong \mathbb{Z} \times \dots \times \mathbb{Z}$  con  $r$  copias de  $\mathbb{Z}$  y decimos que  $G$  es un **grupo abeliano libre de rango  $r$** . En el caso (ii)  $G \cong \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_n}$  donde  $m_i|m_{i+1}$  para  $1 \leq i \leq n-1$  los elementos de la lista  $m_1, \dots, m_n$  se llaman **factores invariantes** 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  $m_1, \dots, m_n$  tales que  $m_i|m_{i+1}$  para  $1 \leq i \leq n-1$  con producto  $n$ . En resumen tenemos:

**1.4 Teorema.** Sea  $G \cong \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_n} \times \mathbb{Z} \times \dots \times \mathbb{Z}$ , con  $r$  copias de  $\mathbb{Z}$ , donde  $m_i|m_{i+1}$  para  $1 \leq i \leq n-1$  y  $G' \cong \mathbb{Z}_{k_1} \times \dots \times \mathbb{Z}_{k_j} \times \mathbb{Z} \times \dots \times \mathbb{Z}$ , con  $s$  copias de  $\mathbb{Z}$ , donde  $k_i|k_{i+1}$  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 [L12]) 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 estos teoremas preferimos posponerlas para un curso posterior de Teoría de Módulos y ver estos 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  $C$ ,  $H_n(C) = \ker \partial_n / \text{im } \partial_{n+1} = Z_n(C) / B_n(C)$ . 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.

## 3.2. Permutaciones, Órbitas y Teoremas de Sylow

Consideremos el conjunto  $\Sigma_n$  consistente de todas las permutaciones del conjunto  $I_n = \{1, \dots, n\}$ , es decir,  $\Sigma_n$  consiste de todas las funciones biyectivas de  $I_n$  en  $I_n$ . En I.2 vimos que  $\Sigma_n$  es un grupo bajo la operación binaria  $\circ$  y que  $|\Sigma_n| = n!$ . Recordemos  $\Sigma_3$  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  $\eta_1$  y luego  $\rho_1$ . 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)):

$\circ$	$\iota$	$\rho_1$	$\rho_2$	$\eta_1$	$\eta_2$	$\eta_3$
$\iota$	$\iota$	$\rho_1$	$\rho_2$	$\eta_1$	$\eta_2$	$\eta_3$
$\rho_1$	$\rho_1$	$\rho_2$	$\iota$	$\eta_2$	$\eta_3$	$\eta_1$
$\rho_2$	$\rho_2$	$\iota$	$\rho_1$	$\eta_3$	$\eta_1$	$\eta_2$
$\eta_1$	$\eta_1$	$\eta_3$	$\eta_2$	$\iota$	$\rho_2$	$\rho_1$
$\eta_2$	$\eta_2$	$\eta_1$	$\eta_3$	$\rho_1$	$\iota$	$\rho_2$
$\eta_3$	$\eta_3$	$\eta_2$	$\eta_1$	$\rho_2$	$\rho_1$	$\iota$

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

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

Diremos que una permutación  $\sigma$  de  $I_n$  es un **ciclo de longitud  $r$**  (o  $r$ -ciclo) si existen enteros  $i_1, \dots, i_r$  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  $\sigma = (i_1, i_2, \dots, i_r)$ . 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  $\sigma$  una permutación de  $\Sigma_n$  y definamos en  $I_n = \{1, \dots, n\}$  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  $\sigma$ . Por ejemplo, la órbita del elemento 1 de la permutación

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

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  $O_1, \dots, O_k$  son las órbitas (que son ajenas) de una permutación  $\sigma$  y  $c_1, \dots, c_k$  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  $\sigma$  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  $(i_1, i_2, \dots, i_r) = (i_1, i_r)(i_1, i_{r-1}) \cdots (i_1, i_3)(i_1, i_2)$  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

$$\begin{aligned} a : G \times X & \longrightarrow X, \\ (g, x) & \longmapsto a(g, x), \end{aligned}$$

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  $\Sigma_n$ -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  $(h, x) \mapsto a(h, x) = h x h^{-1}$ . Esta acción se llama **conjugación** por  $h$ . El elemento  $h x h^{-1}$  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  $a(g, x) = g x = y$  para alguna  $g \in G$ .

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

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

es un subgrupo de  $G$ .

**Demostración.** Como para cada  $x \in X$ ,  $e x = x$ , entonces  $x \sim x$ . Si  $x \sim y$  entonces existe  $g \in G$  tal que  $g x = y$  para alguna  $g \in G$ . Luego,  $x = e x = (g^{-1} g) x = g^{-1} (g x) = g^{-1} y$  y por lo tanto  $y \sim x$ . Si  $x \sim y$  y  $y \sim z$  entonces existen  $g, g' \in G$  tales que  $g x = y$  y  $g' y = z$  para algunas  $g, g' \in G$ . Entonces  $(g' g) x = g' (g x) = g' y = z$ , luego  $x \sim z$ . Consideremos  $g, g' \in G_x$ . Luego  $g x = x$  y  $g' x = x$ . Así,  $(g g') x = g (g' x) = g x = x$ . Por lo tanto,  $g g' \in G_x$ . Claramente  $e x = x$ , luego  $e \in G_x$ . Finalmente, si  $g \in G_x$  entonces  $g x = x$  y  $x = e x = (g^{-1} g) x = g^{-1} (g x) = g^{-1} x$ . 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  $\{g x g^{-1}\}$  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  $H_x = \{h \in H : h x = x h\}$  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  $N_H(K) = \{h \in H \mid h K h^{-1} = K\}$ .

(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,  $|Gx| = (G : G_x)$ .

**Demostración.** Definamos una función

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

Veamos que  $\omega$  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  $\omega$  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,  $\omega$  es inyectiva.

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

**2.9 Corolario.** Si  $o(G)$  es finito, entonces  $o(Gx)|o(G)$ .

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

**Ejemplo.** Definamos un **acorde**  $S$  como un subconjunto de la escala  $\mathbb{Z}_{12}$ , es decir  $S \in \wp(\mathbb{Z}_{12})$ . El grupo

$$\overrightarrow{GL}(\mathbb{Z}_{12}) = \{e^t \cdot u : t \in \mathbb{Z}_{12}, u \in GL(\mathbb{Z}_{12})\}$$

llamado **grupo afín general** de  $\mathbb{Z}_{12}$  (o grupo de **simetrías afines** de  $\mathbb{Z}_{12}$ ) actúa sobre  $\wp(\mathbb{Z}_{12})$  a través de

$$\begin{aligned} \alpha : T \times \wp(\mathbb{Z}_{12}) &\rightarrow \wp(\mathbb{Z}_{12}), \\ (e^t \cdot u, \{x\}) &\mapsto \{e^t \cdot u(x)\} = \{ux + t\}. \end{aligned}$$

Por ejemplo, al acorde de D menor<sup>1</sup>  $\{D, F, A\} = \{2, 5, 9\}$  lo podemos transponer al acorde de E menor usando a  $e^2 \cdot 1$ , es decir

$$\begin{aligned} e^2 \cdot 1(\{D, F, A\}) &= e^2 \cdot 1(\{2, 5, 9\}) \\ &= \{e^2 \cdot 1(2), e^2 \cdot 1(5), e^2 \cdot 1(9)\} \\ &= \{4, 7, 11\} = \{E, G, B\}. \end{aligned}$$

Guerino Mazzola ha calculado todos los grupos de isotropía de los acordes de  $\mathbb{Z}_{12}$ , y una tabla que resume tal información se encuentra en su libro *The Topos of Music* [M], en el apéndice L. En particular, el grupo de isotropía de un acorde mayor es siempre trivial (es decir, es  $\{e^0 \cdot 1\}$ ), por lo que la cardinalidad de su órbita es  $|\overrightarrow{GL}(\mathbb{Z}_{12})| = 48$  y lo mismo sucede con los acordes menores.

<sup>1</sup>Para las definiciones de acorde mayor y menor, véase el capítulo 4.

Esto quiere decir que, desde el punto de vista afín, hay 48 acordes mayores o menores en la órbita de cada uno de ellos, o que esencialmente existe un solo acorde mayor (o menor). Por otro lado, un acorde aumentado  $\mathcal{A}$  (por ejemplo,  $C^{\text{aug}} = \{0, 4, 8\}$ ) tiene un grupo de isotropía de cardinalidad 12. Por lo tanto, hay

$$o(\overrightarrow{GL}(\mathbb{Z}_{12})\mathcal{A}) = \frac{o(\overrightarrow{GL}(\mathbb{Z}_{12}))}{o(\overrightarrow{GL}(\mathbb{Z}_{12})_{\mathcal{A}})} = \frac{48}{12} = 4$$

elementos en su órbita, y esencialmente doce acordes aumentados desde el punto de vista afín.

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

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

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

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

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

**Ejemplo.** Denotemos a  $\mathbb{Z}_{12} \oplus \mathbb{Z}_{12}$  con  $\mathbb{Z}_{12}^2$  y consideremos el grupo

$$\overrightarrow{GL}(\mathbb{Z}_{12}^2) = \{e^{(s,t)} \cdot (u, v) : s, t \in \mathbb{Z}_{12}, u, v \in GL(\mathbb{Z}_{12})\}$$

y su acción sobre los motivos en  $\mathbb{Z}_{12}^2$ . Harald Friperntinger (véase [M]) ha calculado el número de órbitas de esta acción sobre todos estos motivos y, en particular, el número de clases de los motivos de 72 elementos. Según sus cálculos, este número es

$$2\,230\,741\,522\,540\,743\,033\,415\,296\,821\,609\,381\,912 = 2.23 \dots \times 10^{23}.$$

que rebasa incluso a la cantidad aproximada de estrellas en la Vía Láctea, que es  $10^{11}$ .

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

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

es un homomorfismo.

**Demostración.** Veamos que  $\sigma_g : X \rightarrow X$  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,  $\sigma_g$  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,  $\sigma_g$  es suprayectiva.  $\omega$  es un homomorfismo pues

$$\begin{aligned}\omega(gg') &= \sigma_{gg'}(x) = (gg')x = g(g'x) = g\sigma_{g'}(x) \\ &= \sigma_g(\sigma_{g'}(x)) = \omega(g)(\sigma_{g'}(x)) = \omega(g)\omega(g'). \blacklozenge\end{aligned}$$

**2.12 Corolario. (Cayley)** Si  $G$  es un grupo entonces existe un monomorfismo  $G \rightarrow \Sigma_G$ , 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  $\Sigma_n$ .

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

$$\begin{aligned}\omega : G &\rightarrow \Sigma_G \text{ dada por} \\ g &\mapsto \omega(g) = \sigma_g(x) = gx.\end{aligned}$$

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,  $\omega$  es un monomorfismo. Como caso particular, si  $o(G) = n$  entonces  $\Sigma_G = \Sigma_n$ .

Otra redacción es la siguiente: Propondremos a

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

como candidato a subgrupo de  $\Sigma_G$ .  $\sigma_g : G \rightarrow G$  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  $\Sigma_G$  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

$$\begin{aligned}h &: G \rightarrow H \text{ mediante} \\ g &\mapsto h(g) = \sigma_g.\end{aligned}$$

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.  $\blacklozenge$

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  $p|o(G)$  ( $p$  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  $\sigma$  es una permutación de  $\Sigma_n$  y en  $I_n = \{1, \dots, n\}$ ,  $i \equiv j$  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

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

Pruebe que si  $\sigma'$  es otra permutación, entonces  $sg(\sigma' \circ \sigma) = sg(\sigma')sg(\sigma)$  y que si  $\tau$  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  $\Sigma_n$  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  $\sigma$  es par y  $-1$  si  $\sigma$  es impar. Pruebe que  $A_n$  es el núcleo de  $h$ , y por lo tanto un subgrupo normal de  $\Sigma_n$  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  $\Sigma_3$  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.

### 3.3. 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 la 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  $K$

$$\begin{aligned} K \times K &\rightarrow K, \\ (x_1, \dots, x_r)(y_1, \dots, y_s) &\mapsto (x_1, \dots, x_r, y_1, \dots, y_s). \end{aligned}$$

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:  $x_1^1 x_2^{-1} x_1^1 x_2^{-1} x_3^1 x_4^{-1} x_2^{-1} x_1^1$ ,  $x_2^{-1} x_3^1 x_4^{-1} x_1^1 x_2^{-1} x_3^1 x_3^1 x_4^{-1}$ ,  $x_3^1 x_4^{-1} x_1^1 x_2^{-1} x_1^1$ .

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:

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

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

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

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  $h \circ f = g$ .

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

Considere el diagrama

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

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:

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

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

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

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**  $(X|R)$  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 diedral  $D_n$   $n \geq 2$ , 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.**  $(x|_)$  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.**  $(x|x^n = e)$  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:

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

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

Sea  $g : X \rightarrow G$  cualquier función de  $X$  en un grupo abeliano  $G$ . Como  $K$  es un grupo libre en  $X$ , existe un homomorfismo  $k : K \rightarrow G$  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  $h : L \rightarrow G$  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  $f' : L \rightarrow G$  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  $g : f(X) \rightarrow H$  donde  $H$  es cualquier grupo abeliano se extiende a un homomorfismo único  $h : G \rightarrow H$ . (Problema 3.3).

**3.13 Ejemplo.** Considere el grupo que consiste de la suma directa de  $n$  copias de  $\mathbb{Z}$ . Entonces  $(1, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, \dots, 0, 1)$  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  $f' : L \rightarrow G$  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  $g : f(X) \rightarrow H$  donde  $H$  es cualquier grupo abeliano se extiende a un homomorfismo único  $h : G \rightarrow H$ .

**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  $L = \{\alpha : X \rightarrow \mathbb{Z} \mid \alpha(j) = 0 \text{ para casi toda } j \in X\}$  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  $f : X \rightarrow L$  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:

<i>Orden</i>	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
<i>Número</i>	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:

$$(x, y | xyx^{-1}y^{-1} = e, x^2 = e, y^3 = e) \text{ y } (x | x^6 = e).$$

**3.12** Determine todos los grupos, salvo isomorfismo, de orden 8. (Son cinco, de los cuales tres son abelianos 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).

### 3.4. 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  $f: X \times Y \rightarrow T$  es una función biaditiva, tal que si,  $G$  es un grupo abeliano y  $g: X \times Y \rightarrow G$  es biaditiva, entonces existe un homomorfismo único  $h: T \rightarrow G$  tal que  $g = h \circ f$ .

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

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

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

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  $h: T \rightarrow T'$  tal que  $f' = h \circ f$ . Análogamente, como  $T'$  es un producto tensorial, existe  $h': T' \rightarrow T$  tal que  $f = h' \circ f'$ . Consideremos los siguientes diagramas

$$\begin{array}{ccc}
 & T & \\
 f \nearrow & \downarrow h & \searrow \\
 X \times Y & \xrightarrow{f'} T' & \\
 f \searrow & \downarrow h' & \nearrow \\
 & T &
 \end{array}
 \quad
 \begin{array}{ccc}
 & T' & \\
 f' \nearrow & \downarrow h' & \searrow \\
 X \times Y & \xrightarrow{f} T & \\
 f' \searrow & \downarrow h & \nearrow \\
 & T' &
 \end{array}$$

Por ser  $T$  un producto tensorial, como  $1_T: T \rightarrow T$  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  $1_{T'}: T' \rightarrow T'$  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  $f: X \times Y \rightarrow X \otimes Y$ , dado por  $f(x, y) = x \otimes y$  es biaditiva, (Problema 4.1). Veamos que  $X \otimes Y$  es, efectivamente, un producto tensorial. Sea  $G'$  un grupo abeliano cualquiera. Consideremos el triángulo

$$\begin{array}{ccc}
 X \times Y & \xrightarrow{f} & T \\
 & \searrow g & \downarrow h' \\
 & & G'
 \end{array}$$

donde  $g$  es biaditiva. Como  $L$  es libre con base  $X \times Y$ , existe un homomorfismo  $h': L \rightarrow G$  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  $h: L/G \rightarrow G'$  tal que el siguiente triángulo conmuta:

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

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 alternatively 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

$$\begin{aligned} (x_1 + x_2) \otimes y &= x_1 \otimes y + x_2 \otimes y, \\ x \otimes (y_1 + y_2) &= x \otimes y_1 + x \otimes y_2. \end{aligned}$$

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

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

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  $g: X \times Y \rightarrow G$  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  $\varphi: X' \rightarrow X$ ,  $\psi: Y' \rightarrow Y$  homomorfismos de grupos abelianos y

$$\varphi \times \psi: X' \times Y' \rightarrow X \times Y$$

dado por

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

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

$$g \circ (\varphi \times \psi): X' \times Y' \rightarrow X \otimes Y.$$

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

$$h: X' \otimes Y' \rightarrow X \otimes Y$$

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

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

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  $\psi: Y' \rightarrow Y$  y  $\psi': Y \rightarrow Y''$  homomorfismos de grupos abelianos y  $X$  un grupo abeliano. Entonces

- (i) si  $1_X: X \rightarrow X$  y  $1_Y: Y \rightarrow Y$  son los homomorfismos de identidad entonces  $1_X \otimes 1_Y$  es la identidad de  $X \otimes Y$ , y
- (ii)  $(1_X \otimes \psi') \circ (1_X \otimes \psi) = (1_X \otimes (\psi' \circ \psi)). \blacklozenge$

Podemos escribir estas afirmaciones en el siguiente diagrama:

$$\begin{array}{ccc} Y' & & X \otimes Y' \\ \downarrow \psi & \searrow & \downarrow 1_X \otimes \psi \\ Y & \xrightarrow{\psi' \circ \psi} & X \otimes Y \\ \downarrow \psi' & \swarrow & \downarrow 1_X \otimes \psi' \\ Y'' & & X \otimes Y'' \end{array}$$

$\xrightarrow{X \otimes ?}$        $\xrightarrow{1_X \otimes (\psi' \circ \psi)}$



**4.4 Proposición.** Sean  $\varphi: X' \rightarrow X$  y  $\varphi': X \rightarrow X''$  homomorfismos de grupos abelianos y  $Y$  un grupos abeliano. Entonces

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

$$\begin{array}{ccc}
\begin{array}{c} X' \\ \downarrow \varphi \\ X \\ \downarrow \varphi' \\ X'' \end{array} & \xrightarrow{\varphi' \circ \varphi} & \begin{array}{c} X' \otimes Y \\ \downarrow \varphi \otimes 1_Y \\ X \otimes Y \\ \downarrow \varphi' \otimes 1_Y \\ X'' \otimes Y \end{array} \\
\begin{array}{c} \curvearrowright \\ \uparrow 1_X \\ \downarrow \varphi' \end{array} & & \begin{array}{c} \curvearrowright \\ \uparrow 1_X \otimes 1_Y \\ \downarrow \varphi' \otimes 1_Y \end{array}
\end{array}$$

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

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

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

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

**Demostración.** Sea  $g: X \times (\sum_{i \in I} Y_i) \rightarrow \sum_{i \in I} (X \otimes Y_i)$  dada por  $g(x, (y_i)) = (x \otimes y_i)$ .

$$h: M \otimes (N_i) \rightarrow (M \otimes N_i)$$
$$\begin{array}{ccc} X \times (\sum_{i \in I} Y_i) & \xrightarrow{f} & X \otimes (\sum_{i \in I} Y_i) \\ & \searrow g & \downarrow h \\ & & \sum_{i \in I} (X \otimes Y_i) \end{array}$$

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

$$\varphi: \sum_{i \in I} (X \otimes Y_i) \rightarrow X \otimes \left( \sum_{i \in I} Y_i \right)$$

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

$$\begin{array}{ccc} & & X \otimes \left( \sum_{i \in I} Y_i \right) \\ & \nearrow \varphi_i & \uparrow \varphi \\ X \otimes Y_i & \xrightarrow{\iota_{X \otimes Y_i}} & \bigoplus_{i \in I} (X \otimes Y_i) \end{array}$$

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

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

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

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

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

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  $\psi'$  es un epimorfismo, existe  $y_i \in Y$  tal que  $\psi'(y_i) = y_i''$  para toda  $i$ . Luego,

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

Como

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

se tiene que  $\text{im}(1_X \otimes \psi) \subset \ker(1_X \otimes \psi')$ . 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

$$\mathbb{Z} \xrightarrow{2 \cdot} \mathbb{Z} \rightarrow \mathbb{Z}/2$$

donde  $2_{\cdot}$  denota la multiplicación por dos, al hacer el producto tensorial con  $Y = \mathbb{Z}/2$  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  $g: Y \times \mathbb{Z} \rightarrow Y$  la función biaditiva dada por  $g(y, \lambda) = \lambda y$ ,  $\lambda \in \mathbb{Z}$ ,  $y \in Y$ . Entonces existe un homomorfismo único  $h: Y \otimes \mathbb{Z} \rightarrow Y$  tal que  $h \circ f = g$ , es decir, el siguiente diagrama conmuta:

$$\begin{array}{ccc} Y \times \mathbb{Z} & \xrightarrow{f} & Y \otimes \mathbb{Z} \\ & \searrow g & \downarrow h \\ & & Y. \end{array}$$

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

$$x = \sum_{i=1}^n (y_i \otimes \lambda_i) = \sum_{i=1}^n (\lambda_i y_i \otimes 1) = \left( \sum_{i=1}^n \lambda_i y_i \right) \otimes 1 = y \otimes 1,$$

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

$$g'': X \times Y \rightarrow X \otimes Y \otimes Z$$

dada por  $g''(x, y) = x \otimes y \otimes w$  para  $w \in Z$  fija, la cual induce un homomorfismo

$$h_w: X \otimes Y \rightarrow X \otimes Y \otimes Z$$

tal que

$$h_w(x \otimes y) = x \otimes y \otimes w.$$

Sea

$$g: (X \otimes Y) \times Z \rightarrow X \otimes Y \otimes Z$$

dada por

$$g(t, w) = h_w(t).$$

La función  $g$  es biaditiva y por lo tanto induce un homomorfismo

$$h: (X \otimes Y) \otimes Z \rightarrow X \otimes Y \otimes Z$$

tal que

$$h((x \otimes y) \otimes w) = x \otimes y \otimes w.$$

Construyamos ahora una función

$$h': X \otimes Y \otimes Z \rightarrow (X \otimes Y) \otimes Z$$

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

$$g': X \times Y \times Z \rightarrow (X \otimes Y) \otimes Z$$

dada por

$$g'(x, y, w) = (x \otimes y) \otimes w.$$

$g'$  es lineal en cada variable, luego induce un homomorfismo

$$h': X \otimes Y \otimes Z \rightarrow (X \otimes Y) \otimes Z$$

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  $f: X \times Y \rightarrow X \otimes Y$ , 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  $i: X \times Y \rightarrow X \otimes Y$  y utilice la unicidad para mostrar que  $i$  es suprayectiva.)

**4.3** Sea  $g: X \times (\sum_{i \in I} Y_i) \rightarrow \sum_{i \in I} (X \otimes Y_i)$  dada por  $g(x, (y_i)) = (x \otimes y_i)$  como en la Proposición 4.5. Compruebe que  $g$  es biaditiva. También compruebe que

$\varphi \circ h = 1_{X \otimes (\sum_{i \in I} Y_i)}$  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  $X' \xrightarrow{\varphi} X \xrightarrow{\varphi'} X''$  es una sucesión exacta de grupos abelianos que se **escinde** (es decir,  $X \cong X' \oplus X''$ ) y  $Y$  un grupo abeliano, entonces

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

es una sucesión exacta que se escinde (es decir,  $X \otimes Y \cong X' \otimes Y \oplus X'' \otimes Y$ ).

# Capítulo 4

En este capítulo se expondrá con todo detalle algunas aplicaciones de la Teoría de Grupos a la Teoría Musical. Se explicarán algunos aspectos básicos de la Teoría Matemática de la Música y, en el proceso, se pretende dar elementos a lectores de diversos antecedentes, tanto en la Matemática como en la Música. Por este motivo los ejemplos siguen de algunos aspectos teóricos sobresalientes de los capítulos previos; los aspectos y términos musicales son introducidos conforme se vayan necesitando para que un lector sin formación musical pueda entender la esencia de cómo la Teoría de Grupos es empleada para explicar ciertas relaciones musicales ya establecidas. Asimismo, para el lector con conocimiento de la Teoría Musical, este capítulo provee elementos concretos, así como motivación, para comenzar a comprender la Teoría de Grupos.

Una meta de la Teoría Musical es describir las posibilidades de un sistema de tonos. El tono es el sonido que se escucha y que, usualmente, se asocia con las frecuencias de vibración. Tradicionalmente, el estudio de los intervalos entre tonos se hacía usando las razones de frecuencia de las potencias de los enteros pequeños. La Teoría Matemática de la Música moderna ofrece una manera independiente de entender el sistema de tonos, considerando los intervalos como transformaciones. El surgimiento histórico de las estructuras algebraicas en la Musicología llevó a la Teoría Transformacional, que se concentra en las operaciones que forman grupos matemáticos. En este capítulo vamos explorar y desarrollar aspectos de la Teoría Neo-Riemanniana, en particular la dualidad los grupos TI y PLR. El contenido de este capítulo está basado en [CFS] y [DP].

## 4.1. Antecedentes Musicales

Los doce tonos de nuestro sistema moderno llevan los nombres de las primeras 7 letras del abecedario<sup>1</sup>. Cada letra representa una frecuencia distinta y las letras se repiten cuando se duplica la frecuencia del tono. El rango de tonos que comienza con una frecuencia hasta su doble, se conoce como una **octava**. Convencionalmente se divide a la octava en 12 intervalos iguales, de modo que obtenemos un conjunto de tonos tales que la frecuencia de cada uno resulta de multiplicar por  $\sqrt[12]{2}$  la del anterior<sup>2</sup>. Esto se conoce como la afinación de **temperamento igual o equitemperada**. Previo a la afinación de temperamento igual, los músicos usaban (entre otras) la afinación justa, que es un sistema con notas que tienen frecuencias que están relacionadas por razones de números enteros. En la afinación equitemperada, la diferencia en frecuencia entre cada nota se llama **semitono**. Con sólo 7 letras y 12 notas, el símbolo  $\sharp$  es usado para denotar un tono que es un semitono por arriba del original y el símbolo  $\flat$  para denotar un tono que es un semitono por debajo del original. Por ejemplo, si hablamos del tono G, entonces la nota que está por arriba un semitono sería  $G\sharp$  y la nota un semitono por abajo sería  $G\flat$ . El conjunto completo de doce notas se llama la **escala cromática** y se denota, musicalmente, como sigue:

$$C, C\sharp, D, D\sharp, E, F, F\sharp, G, G\sharp, A, A\sharp, B.$$

Como se mencionó anteriormente, dos notas sucesivas difieren por un semitono. La nota que está un semitono por arriba de G es  $G\sharp$ , aunque también esa misma nota está un semitono por debajo de A y por ello puede ser denotada con  $A\flat$ . Esta propiedad de las notas de poseer múltiples nombres en la afinación bien temperada, se conoce como la **equivalencia enarmónica**. Esto se muestra, junto con los valores de la frecuencia de cada tono (comenzando con la nota C central<sup>3</sup> y las once notas que la siguen), en la cuadro 4.1.

Como todos los múltiplos de una cierta frecuencia son representados por la misma letra, es matemáticamente conveniente representar este conjunto de doce notas por los enteros módulo 12 ( $\mathbb{Z}_{12}$ ), donde cada elemento es una clase y representa un conjunto infinito de números. De acuerdo con la literatura sobre

<sup>1</sup>La Teoría Matemática de la Música usa la notación científica del tono. Debe tenerse en mente que, generalmente, en los países de habla romance se acostumbra hacer las identificaciones do=C, re=D, mi=E, fa=F, sol=G, la=A y si=B.

<sup>2</sup>El cerebro humano interpreta las distancias entre tonos de manera logarítmica. Es decir, la distancia (en octavas) entre un tono con frecuencia  $F_1$  y otro con frecuencia  $F_2$  se percibe como

$$|\log_2(F_1) - \log_2(F_2)|.$$

Es por eso que si  $F_2 = 2F_1$ , entonces la distancia es

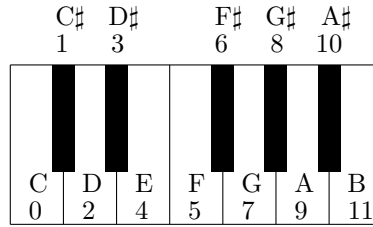
$$|\log_2(F_1) - \log_2(F_2)| = |\log_2(F_1) - \log_2(2F_1)| = |\log_2(\frac{F_1}{2F_1})| = |\log_2 \frac{1}{2}| = |-1| = 1.$$

El lector podrá comprobar que al dividir la distancia entre  $F_1$  y  $2F_2$  en doce partes iguales, las frecuencias de los tonos resultantes son iguales a multiplicar  $F_1$  por potencias sucesivas de  $2^{\frac{1}{12}}$ .

<sup>3</sup>En la notación científica del tono, el llamado C central se ubica en la cuarta octava. Por ello se denota con  $C_4$ .

Nota	Frecuencia (Hz)	Nota	Frecuencia (Hz)
C <sub>4</sub>	261.63	F <sub>4</sub> <sup>♯</sup> /G <sub>4</sub> <sup>♭</sup>	369.99
C <sub>4</sub> <sup>♯</sup> /D <sub>4</sub> <sup>♭</sup>	277.18	G <sub>4</sub>	392.00
D <sub>4</sub>	293.66	A <sub>4</sub> <sup>♭</sup> /G <sub>4</sub> <sup>♯</sup>	415.30
E <sub>4</sub> <sup>♭</sup> /D <sub>4</sub> <sup>♯</sup>	311.10	A <sub>4</sub>	440.00
E <sub>4</sub>	329.63	B <sub>4</sub> <sup>♭</sup> /A <sub>4</sub> <sup>♯</sup>	466.16
F <sub>4</sub>	349.23	B <sub>4</sub>	493.88

Cuadro 4.1: Frecuencias correspondientes a las notas en la octava central.

Figura 4.1: Notas asignadas a los elementos de  $\mathbb{Z}_{12}$ .

la Teoría Matemática de la Música, asignaremos los números a las letras como se indica en la figura F:Asig.

Esta asignación no es rígida y es válido asignar el 0 a cualquiera de las 12 notas. Para los fines de este capítulo, estamos interesados en conjuntos de notas que se tocan simultáneamente. Tales conjuntos de notas se conocen como **acordes**. Nos concentraremos, en particular, en el grupo de acordes conocidos como **tríadas**, es decir, conjuntos de 3 notas se tocan simultáneamente. Ahora bien, hay  $\binom{12}{3} = 220$  subconjuntos de de 3 notas del conjunto de 12 notas. Sin embargo, nos limitaremos a estudiar a los conjuntos de 3 elementos que se conocen como acordes mayores y menores.

Las tres notas en una tríada son conocidas como la fundamental o raíz, la tercera y la quinta (respectivamente). A cada tríada se le nombra según su fundamental (o raíz). No obstante, en nuestro trabajo, las tríadas son conjuntos y el orden no importa (salvo para identificar a la raíz, claro está). Los acordes mayores y menores se definen como sigue:

**1.1 Definición.** Diremos que el acorde  $\{a, b, c\} \in \wp(\mathbb{Z}_{12})$  es un acorde **mayor** si  $b = a + 4$  y  $c = a + 7$ .

Los acordes mayores en este orden están en la posición fundamental (o posición raíz) y son designados con mayúsculas, como  $G^{\sharp} = \{8, 0, 3\}$ . En el caso de  $G^{\sharp}$ , la fundamental es  $G^{\sharp} = 8$ , la tercera es  $B^{\sharp} = 0$ , y la quinta es  $D^{\sharp} = 3$ .

No obstante esta observación musical, en el trabajo matemático con las



tríadas (que son conjuntos de tres elementos) insistimos en que el orden no importa: a veces será más apropiado referirse a  $G\sharp$  como, digamos,  $\{3, 0, 8\}$ . Lo mismo es cierto para los acordes menores que se definen a continuación.

**1.2 Definición.** Diremos que el acorde  $\{a, b, c\} \in \wp(\mathbb{Z}_{12})$  es un acorde **menor** si  $b = a + 3$  y  $c = a + 7$ .

Los acordes menores en este orden también están en la posición de fundamental y serán denotados con letras minúsculas, como  $f = \{5, 8, 0\}$ . Ahora que hemos definido los elementos, nos referiremos a ellos como **tríadas de clases** de tonos.

**1.3 Definición.** El conjunto completo de los 24 acordes mayores y menores se denotará con  $\mathcal{M}$ . Específicamente,

$$\mathcal{M} = \{\{x, x + 3, x + 7\}, \{X, X + 4, X + 7\} | x, X \in \mathbb{Z}_{12}\}.$$

Volvemos a resaltar que los acordes son conjuntos y que por ello no están ordenados. En otras palabras: si el conjunto  $\{5, 8, 0\}$  se escribe en otro orden, digamos  $\{0, 8, 5\}$ , el significado es el mismo pues de ambas maneras representa al acorde de F menor. El acorde de F menor se forma tocando las notas F, Ab, y C simultáneamente. Si tomamos  $\{0, 8, 5\}$ , todavía estamos indicando que las notas C, Ab, y F serán tocadas juntas, lo cual significa que se toca el acorde de F menor. De esta forma, la posición fundamental del acorde (como en las definiciones 1.1 y 1.2) muestra cómo se incluyen las componentes del acorde, pero las notas individuales pueden distribuirse de múltiples maneras sin cambiar la identidad del acorde.

Hay un detalle respecto al término “tríada de clases de tono”. Debe quedar claro con qué elementos estamos trabajando ya que, hasta ahora, nos hemos referido a la tríada de clases de tono como tríada, a secas. Sin embargo, un elemento  $x$  en  $\mathcal{M}$  es una tríada, donde  $x = \{a, b, c\}$ , y  $a, b, c \in \mathbb{Z}_{12}$ . Esta notación se usa porque es cómoda y sencilla, pero para ser más precisos debemos recordar que  $\mathbb{Z}_{12}$  es un conjunto de clases:

$$\mathbb{Z}_{12} = \{[0], [1], \dots, [11]\},$$

donde

$$\begin{aligned} [0] &= \{\dots, -24, -12, 0, 12, 24, \dots\}, \\ &\vdots \\ [11] &= \{\dots, -13, -1, 11, 23, \dots\}. \end{aligned}$$

Así es que, cuando se lee  $a \in \mathbb{Z}_{12}$ , se quiere decir realmente que  $[a] \in \mathbb{Z}_{12}$ . Llamamos estas clases de tono porque, como ya se mencionó, cada nota de C a B representa para nosotros todos los tonos que son múltiplos de él, de la misma manera en que cada clase en  $\mathbb{Z}_{12}$  representa todos los números módulo 12 de que son múltiplos. En consecuencia, cuando se lee,  $x = \{a, b, c\}$ , realmente se tiene

$[x] = \{[a], [b], [c]\}$ . Por lo tanto, se extiende esta idea de clases de tono hasta tríadas de clases de tono, donde todos los elementos en  $\mathcal{M}$  también son clases. Como ejemplo, tómese el acorde de C mayor,  $x = \{0, 4, 7\}$ . Si se ve a C mayor como una clase de tríadas, debemos representarlo de la siguiente manera:

$$C = [x] = \{[0], [4], [7]\} = \{\dots, \{-12, -8, -5\}, \{0, 4, 7\}, \{12, 16, 19\}, \dots\}.$$

Ahora que hemos aclarado la diferencia entre elementos básicos y clases, en aras de la simplicidad, continuaremos denotando  $[x]$  simplemente con  $x$ .

## 4.2. Las Transformaciones T e I

La transposición, en la Teoría Musical, se refiere al proceso de trasladar un tono, o un conjunto de tonos, por un intervalo constante. La definición musical de esta transformación se traduce directamente en una definición de transformación matemática.

**2.1 Definición.** Sea  $x \in \mathcal{M}$ , donde  $x = \{a, b, c\}$ . Una **transposición** es una función  $T_n : \mathcal{M} \rightarrow \mathcal{M}$  dada por

$$T_n(x) = x + n = \{a + n, b + n, c + n\},$$

donde  $n \in \mathbb{Z}$ .

Se puede aplicar  $T_n$  solamente a los 24 elementos (tríadas) en  $\mathcal{M}$ , pero hay una cantidad infinita de transposiciones de cualquier tríada, ya que  $n \in \mathbb{Z}$ . No obstante, después de haber transpuesto cualquier tríada 12 veces, se obtiene la misma sucesión de tríadas de nuevo. Por ejemplo:

$$\begin{aligned} T_0(C) &= T_0(\{0, 4, 7\}) = \{0, 4, 7\} \\ T_1(C) &= T_1(\{0, 4, 7\}) = \{1, 5, 8\} \\ &\vdots \\ T_{12}(C) &= T_{12}(\{0, 4, 7\}) = \{0, 4, 7\} = T_0(C) \\ T_{13}(C) &= T_{13}(\{0, 4, 7\}) = \{1, 5, 8\} = T_1(C) \\ &\vdots \end{aligned}$$

Se ve entonces que  $T_0$  se comporta como la función identidad y que, por cada tríada, no hay más que 12 transposiciones distintas.

Geométricamente, podemos ver las transposiciones como las rotaciones de un triángulo a través de 12 puntos igualmente distribuidos en un círculo. Los tres vértices de un triángulo representan los tonos de una tríada. Por ejemplo, en la esquina superior izquierda de la figura 4.2 se ubica el acorde de C mayor  $\{0, 4, 7\}$ . Después se rotan los tres vértices, o tonos, hacia la derecha, uno por uno. La figura 4.2 presenta el proceso de aplicar  $T_n(\{0, 4, 7\})$ , para toda  $0 \leq n < 12$ , al acorde de C mayor.

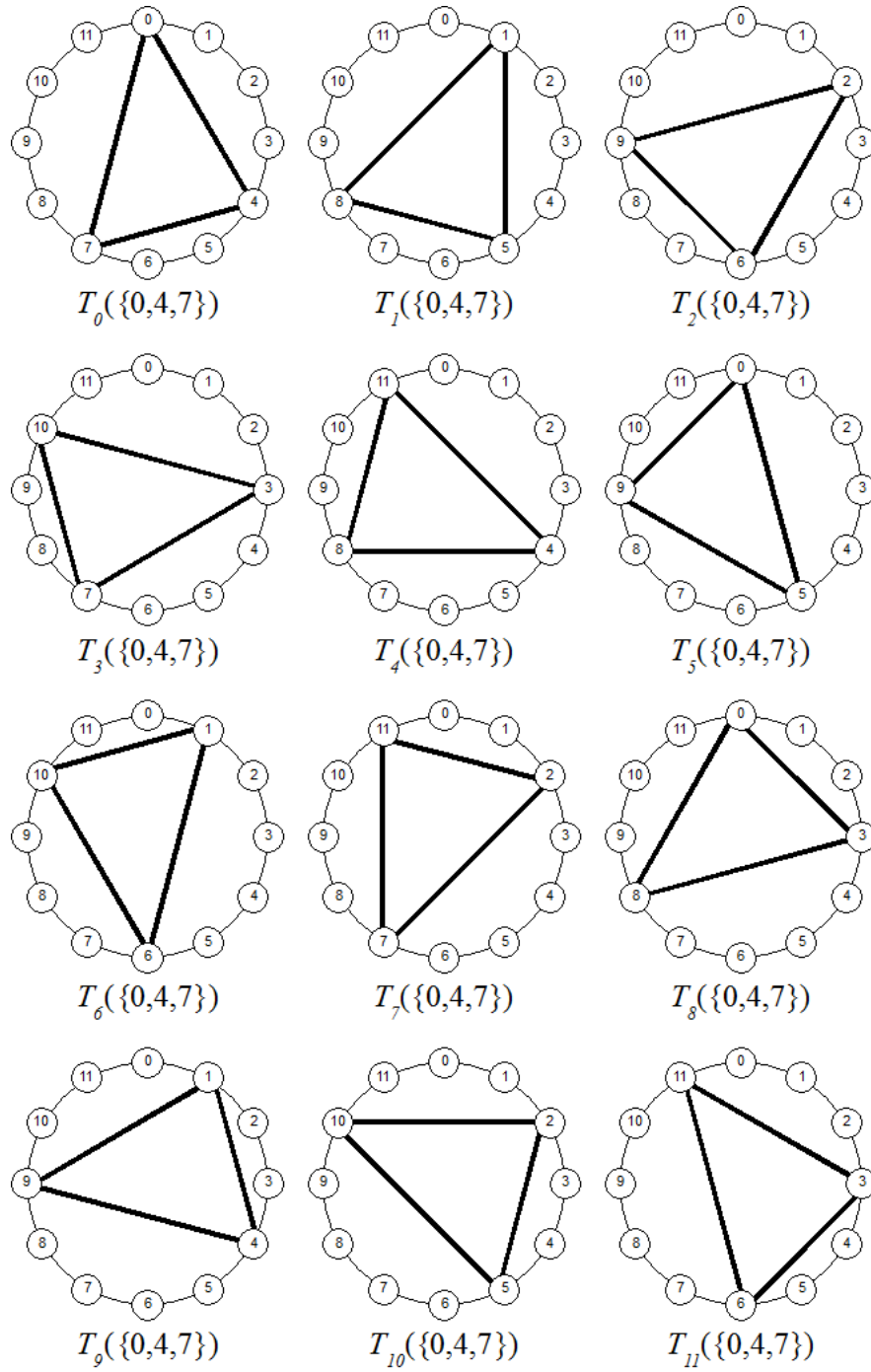


Figura 4.2: Las doce transposiciones de la tríada de  $C$  mayor  $\{0, 4, 7\}$ .

**2.2 Definición.** Sea  $x \in \mathcal{M}$ , donde  $x = \{a, b, c\}$ . Una **inversión** es una función  $I_n : \mathcal{M} \rightarrow \mathcal{M}$  dada por

$$I_n(x) = -x + n = \{-A + n, -B + n, -C + n\}$$

donde  $n \in \mathbb{Z}$ .

Como en el caso de las transposiciones, hay 24 tríadas para invertir y un número infinito de inversiones de cada tríada. Sin embargo, una vez más, cuando invertimos una tríada, y luego transponemos 12 veces, obtenemos nuevamente la misma sucesión de tríadas. Por ejemplo:

$$\begin{aligned} I_0(C) &= I_0(\{0, 4, 7\}) = \{0, 8, 5\} \\ I_1(C) &= I_1(\{0, 4, 7\}) = \{1, 9, 6\} \\ &\vdots \\ I_{12}(C) &= I_{12}(\{0, 4, 7\}) = \{0, 8, 5\} = I_0(C) \\ I_{13}(C) &= I_{13}(\{0, 4, 7\}) = \{1, 9, 6\} = I_1(C) \\ &\vdots \end{aligned}$$

Se ve otra vez que para cada tríada no hay más que 12 inversiones distintas. En contraste con la representación geométrica de la transposición, la representación correspondiente a la inversión es relativamente más descriptiva. Todas las inversiones pueden ser ilustradas como reflexiones de triángulos respecto al eje vertical que pasa por el 0 y el 6 en el círculo. La figura 4.3 no presenta a primera vista las 12 inversiones de  $\{0, 4, 7\}$ . Más bien, a fin de ilustrar la reflexión, la figura presenta la forma invertida de cada tríada mayor. Sin embargo, cada una de tales tríadas es, en última instancia, una transposición de la tríada original  $\{0, 4, 7\}$ . Dicho de otra manera, si se reflejan cada una de las tríadas de la figura 4.2 se obtienen las de la figura 4.3.

**2.3 Proposición.** Para toda  $n, k \in \mathbb{Z}$ , tal que  $n \equiv k \pmod{12}$ ,

$$T_n = T_k \quad \text{y} \quad I_n = I_k$$

**Demostración.** Como  $n \equiv k \pmod{12}$ , entonces  $n = 12q + k$ , para algún  $q \in \mathbb{Z}$ . Por lo tanto

$$T_n = T_{12q+k} = T_{12q} \circ T_k = (T_0)^q \circ T_k = (i)^q \circ T_k = T_k$$

donde  $i$  es la transformación identidad (o la traslación por 0) y

$$I_n = I_{12q+k} \stackrel{*}{=} T_{12q} \circ I_k = (T_0)^q \circ I_k = (i)^q \circ I_k = I_k;$$

la igualdad marcada con un asterisco la demostraremos en el lema 2.5. ♦

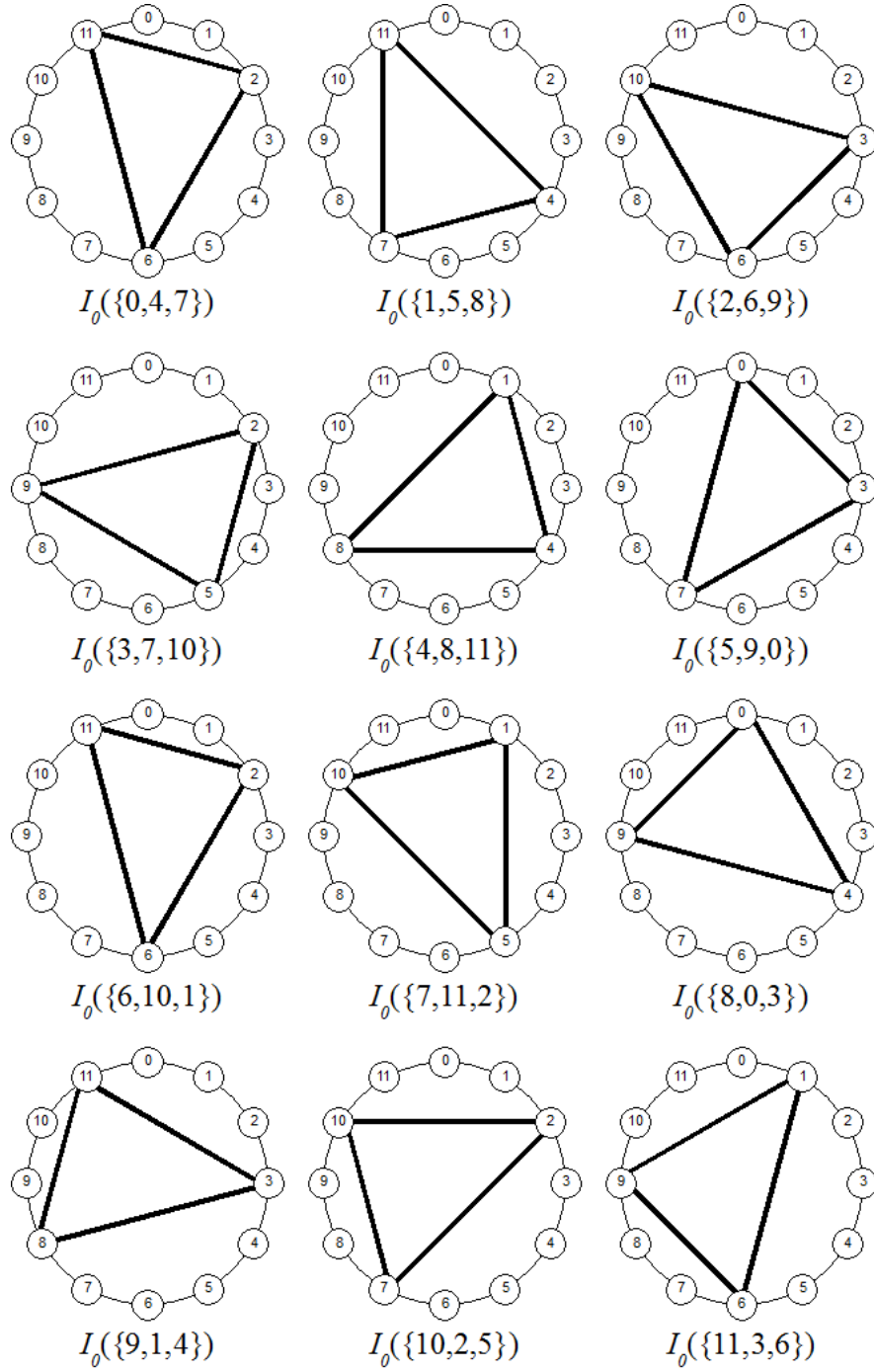


Figura 4.3: Las doce inversiones de la tríada de C mayor  $\{0, 4, 7\}$ .

**2.4 Definición.** El conjunto de todas las funciones de transposición e inversión se denota  $TI$ , y se define como:

$$TI = \{T_n, I_n | n = 0, \dots, 11\}.$$

Resulta que podemos representar todos estos elementos de una forma más compacta si analizamos las cuatro posibles composiciones de las funciones de  $T$  e  $I$ .

**2.5 Lema.** Se tienen las siguientes relaciones en el conjunto  $TI$ :

$$T_m \circ T_n = T_{m+n \text{ mód } 12},$$

$$T_m \circ I_n = I_{m+n \text{ mód } 12},$$

$$I_m \circ T_n = I_{m-n \text{ mód } 12},$$

$$I_m \circ I_n = T_{m-n \text{ mód } 12}.$$

**Demostración.** Para el primer inciso tenemos

$$\begin{aligned} T_m \circ T_n &= T_m(T_n(\{a, b, c\})) \\ &= T_m(\{a + n, b + n, c + n\}) \\ &= \{a + n + m, b + n + m, c + n + m\} \\ &= \{a + (m + n), b + (m + n), c + (m + n)\} \\ &= T_{m+n \text{ mód } 12} \end{aligned}$$

mientras que para el segundo

$$\begin{aligned} T_m \circ I_n &= T_m(I_n(\{a, b, c\})) \\ &= T_m(\{-a + n, -b + n, -c + n\}) \\ &= \{-a + n + m, -b + n + m, -c + n + m\} \\ &= \{-a + (m + n), -b + (m + n), -c + (m + n)\} \\ &= I_{m+n \text{ mód } 12}. \end{aligned}$$

La demostración de las otras dos igualdades se deja como ejercicio para el lector. ♦

Si se aplican consecutivamente las funciones del conjunto  $TI$  a cualquier tríada en  $\mathcal{M}$ , se reproduce todo el conjunto  $\mathcal{M}$ . Reiteramos que las figuras 4.2 y 4.3 muestran el resultado de aplicar todas las funciones de  $T$  e  $I$  a  $C = \{0, 4, 7\}$ .

Se deja al lector, en los ejercicios, mostrar que las funciones en  $T$  e  $I$  están bien definidas.

**2.6 Teorema.** El conjunto  $TI$  forma un grupo bajo composición.

**Demostración.**

1. Para toda  $f, g \in TI$ ,  $f \circ g = h \in TI$ , por el lema 2.5. Por lo tanto,  $TI$  está cerrado bajo composición.
2. Se satisface lo siguiente:

$$T_0 \circ T_n = T_{0+n} = T_n,$$

$$T_n \circ T_0 = T_{n+0} = T_n,$$

$$T_0 \circ I_n = I_{0+n} = I_n,$$

$$I_n \circ T_0 = I_{n-0} = I_n.$$

Por lo tanto,  $T_0 = i \in TI$  (i.e.  $T_0$  es el elemento identidad).

3. Por un lado, las relaciones

$$T_n \circ T_{12-n} = T_{n+12-n} = T_{12} = T_0,$$

$$T_{12-n} \circ T_n = T_{12-n+n} = T_{12} = T_0,$$

implican  $T_n^{-1} = T_{12-n}$ , mientras que  $I_n \circ I_n = T_{n-n} = T_0$ . muestra que  $I_n^{-1} = I_n$ .

4. Por las propiedades de la composición de funciones, la operación  $\circ$  es asociativa.

Así es que  $TI$  es un grupo bajo composición. ♦

## Problemas.

**2.1.** Muestre que las operaciones en  $T$  están bien definidas. Es decir, si  $[x]$  es una tríada de clases de tonos en  $\mathcal{M}$ , para toda  $x_1, x_2 \in [x]$  tenemos que:

$$T_n(x_1) = T_n(x_2), \quad \text{i.e.} \quad T_n(\{a_1, b_1, c_1\}) = T_n(\{a_2, b_2, c_2\}).$$

**2.2.** Demuestra que las operaciones en  $I$  están bien definidas. Es decir, si  $[x]$  es una tríada de clases de tonos en  $\mathcal{M}$ , para toda  $x_1, x_2 \in [x]$  tenemos que:

$$I_n(x_1) = I_n(x_2), \quad \text{i.e.} \quad I_n(\{a_1, b_1, c_1\}) = I_n(\{a_2, b_2, c_2\}).$$

**2.3.** Demuestre las últimas dos igualdades de Lema 2.5.

## 4.3. Las Transformaciones P, L y R

Aunado a las transformaciones  $T$  e  $I$  que se aplican al conjunto  $\mathcal{M}$ , también se tienen las funciones paralela (P), intercambio de la séptima, o *leittonwechsel* (L) y relativa (R). Análogamente a lo ocurrido con las funciones  $T$  e  $I$ , hay descripciones musicales, con la Teoría de Grupos, así como geométricas, de las funciones P, L y R. Las descripciones y definiciones de las tres no serán separadas

como fue el caso con las funciones T e I y se proveerán varios ejemplos después de la definición formal.

Dos tríadas son **paralelas** si tienen la misma letra como nombre, pero su paridad es opuesta (por **paridad** se entiende si el acorde es mayor o menor). Por ejemplo, la tríada paralela de F mayor  $F = \{5, 9, 0\}$  es F menor  $f = \{5, 8, 0\}$ . Ambas tríadas se denotan con la letra F, pero una es mayor y la otra menor.

Dos tríadas son **relativas** si son de paridad opuesta y la raíz de la que es menor se encuentra tres semitonos por debajo de la raíz de la tríada mayor. Para ilustrar, se toma F mayor  $\{5, 9, 0\}$  y se cuenta tres semitonos por debajo de 5, lo cual da 2. A continuación, se construye un acorde menor comenzando con 2. Este es el acorde de D menor,  $\{2, 5, 9\}$ , por lo que D menor es la relativa de F mayor.

Finalmente, el **intercambio de la séptima** (L) también es de paridad opuesta y, en este caso, simplemente la raíz de la tríada original se reemplaza con su “séptima”. Una vez más se usa F- mayor  $\{5, 9, 0\}$  para ilustrar. La raíz de F es 5, que se reemplaza con su séptima, que es 4. El único acorde menor con tonos 4, 9, y 0 es A menor,  $\{4, 0, 9\}$ , que es el intercambio de la séptima de F.

Continuamos ahora con las definiciones matemáticas de P, L y R, después de las cuales siguen más ejemplos.

**3.1 Definición.** Sean  $x, Y \in \mathcal{M}$ , donde  $x = \{a, b, c\}$  es una tríada menor y  $Y = \{A, B, C\}$  es una tríada mayor, entonces

$$\begin{aligned} P(x) &= P(\{a, b, c\}) = \{a, b + 1, c\}, \\ P(Y) &= P(\{A, B, C\}) = \{A, B - 1, C\}, \\ L(x) &= L(\{a, b, c\}) = \{c + 1, a, b\}, \\ L(Y) &= L(\{A, B, C\}) = \{B, C, A - 1\}, \\ R(x) &= R(\{a, b, c\}) = \{b, c, a - 2\}, \\ R(Y) &= R(\{A, B, C\}) = \{C + 2, A, B\}. \end{aligned}$$

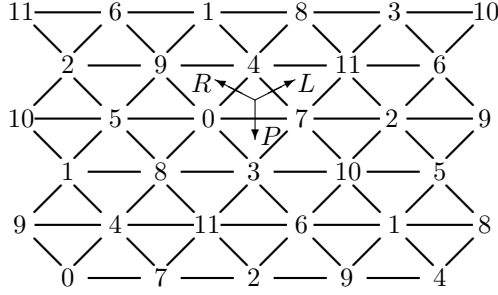
Por ejemplo,

$$\begin{aligned} P(c) &= P(\{0, 3, 7\}) = \{0, 4, 7\} = C \text{ y } P(F) = P(\{5, 9, 0\}) = \{5, 8, 0\} = f, \\ L(e) &= L(\{4, 7, 11\}) = \{0, 4, 7\} = C \text{ y } L(G) = L(\{7, 11, 2\}) = \{11, 2, 6\} = b, \\ R(b) &= R(\{11, 2, 6\}) = \{2, 6, 9\} = D \text{ y } R(A) = R(\{9, 1, 4\}) = \{6, 1, 9\} = f\sharp. \end{aligned}$$

Ahora se exploran las funciones que forman el conjunto de P, L y R y se comienza con la representación geométrica. Lo mismo que con las funciones T e I, hay una representación interesante de las funciones P, L y R sobre un entramado de triángulos conocido como *Tonnetz*.

La palabra *Tonnetz* significa “red de tonos” en alemán. Aunque esta configuración es un invento de Leonhard Euler, fue Hugo Riemann quien exploró su capacidad para trazar el movimiento armónico, o el movimiento de un tono o tríada a otra. Por varios motivos, el *Tonnetz* tiene múltiples variaciones, pero aquí se usa la versión mostrada en la figura 4.4. Nótese que los vértices son clases



Figura 4.4: El *Tonnetz* de Oettingen-Riemann.

de tonos y los triángulos representan tríadas mayores y menores. Como ya se mencionó, las transformaciones P, L, y R preservan 2 tonos cuando son aplicadas a cualquier tríada de  $\mathcal{M}$ . Por lo tanto, la rotación del triángulo alrededor de cualquiera de sus aristas arroja otro triángulo que es equivalente a una de las tres tríadas que producirían P, L, o R. Nótese que si se expande el diagrama con más vértices, éstos comienzan a repetirse vertical y horizontalmente y, en efecto, se produce un enrejado que está sobre un toro.

Ahora analizaremos las composiciones de P, L, y R y las potencias de las composiciones, para determinar los elementos del conjunto. Nótese que P, L, y R son involutivas. En otras palabras:

$$P^2 = L^2 = R^2 = i.$$

Se demuestra esto para la función P. Las funciones L y R se comportan de la misma manera.

$$P \circ P(\{a, b, c\}) = P(\{a, b+1, c\}) = \{a, (b+1)-1, c\} = \{a, b, c\} = i(\{a, b, c\})$$

Si se aplica R a cualquier tríada, luego L al resultado y repetimos esto, se producirá la siguiente sucesión de tríadas (de nuevo, las mayúsculas representan las tríadas mayores y las minúsculas las menores).

$$C, a, F, d, Bb, g, Eb, c, Ab, f, Db, bb, Gb, eb, B, g\sharp, E, c\sharp, A, f\sharp, D, b, G, e, C \quad (4.1)$$

Esta sucesión resulta ser una progresión famosa de la Novena Sinfonía de Beethoven, observada por Cohn [C]. Veamos el primer paso en la construcción de esta sucesión. Inicialmente se toma  $C = \{0, 4, 7\}$  y se aplican las funciones R y L. Obtenemos primero

$$R(\{0, 4, 7\}) = \{4, 0, 9\} = a.$$

Así es que llevamos a C a su relativo menor, que es a. Luego resulta

$$L \circ R(\{0, 4, 7\}) = L(\{4, 0, 9\}) = \{5, 9, 0\} = F,$$

lo cual muestra que se lleva a su intercambio de séptima, que es  $F$  mayor. Si se continúa de esta manera, finalmente se producirá la fila de tríadas exhibidas arriba. Es más, cuando las funciones  $R$  y  $L$  son aplicadas a cualquier tríada mayor de  $\mathcal{M}$  en ese orden, resultará la misma sucesión cíclica de tríadas. Por otro lado, la sucesión se produce al revés si se aplica a cualquier tríada menor. En general, podemos observar primero que

$$\begin{aligned}(L \circ R)^3(\{A, B, C\}) &= (L \circ R)^2(L \circ R(\{A, B, C\})) \\ &= (L \circ R)^2(\{B + 1, C + 2, A\}) \\ &= (L \circ R)(C + 3, A + 2, B + 1) \\ &= \{A + 3, B + 3, C + 3\}\end{aligned}$$

y usar este patrón cuatro veces para obtener

$$\begin{aligned}(L \circ R)^{12}(\{A, B, C\}) &= (L \circ R)^9((L \circ R)^3(\{A, B, C\})) \\ &= (L \circ R)^9(\{A + 3, B + 3, C + 3\}) \\ &= (L \circ R)^6((L \circ R)^3(\{A + 3, B + 3, C + 3\})) \\ &= (L \circ R)^6(\{A + 6, B + 6, C + 6\}) \\ &= (L \circ R)^3((L \circ R)^3(\{A + 6, B + 6, C + 6\})) \\ &= (L \circ R)^3(\{A + 9, B + 9, C + 9\}) \\ &= \{A + 12, B + 12, C + 12\} \\ &= \{A, B, C\} = i(\{A, B, C\}).\end{aligned}$$

Análogamente, si se aplica  $(L \circ R)^{12} = (L \circ R) \circ (L \circ R)^{11}$  a una tríada menor, se obtiene la misma tríada. El siguiente paso en el proceso de calcular el efecto de las potencias de  $L \circ R$  es  $R \circ (L \circ R)^{13}$ . Primero tenemos

$$R \circ (L \circ R)^{12}(\{A, B, C\}) = \{C + 2, B, A\} = R(\{A, B, C\}).$$

Si ahora se calcula  $L \circ R \circ (L \circ R)^{12} = (L \circ R)^{13}$  se obtiene

$$(L \circ R)^{13}(\{A, B, C\}) = \{A + 1, C + 2, B\} = L \circ R(\{A, B, C\})$$

y vuelve a repetirse el patrón.

De esta manera se constata que  $(L \circ R)^{12}$  se comporta como la identidad y se puede afirmar que

$$(L \circ R)^{12} = i = (L \circ R)^0.$$

Se observa de nuevo que una potencia arbitraria de la función siempre tendrá el mismo efecto que una potencia con exponente en el conjunto

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}.$$

Se formaliza este hecho en una proposición.

**3.2 Proposición.** Para  $n, k \in \mathbb{Z}$  tales que  $n \equiv k \pmod{12}$

$$(L \circ R)^n = (L \circ R)^k$$

y

$$R \circ (L \circ R)^n = R \circ (L \circ R)^k.$$

**Demostración.** Recordando que  $(L \circ R)^{12} = (L \circ R)^0 = i$ , tenemos que

$$\begin{aligned} (L \circ R)^n &= (L \circ R)^{12q+k} \\ &= (L \circ R)^{12q} (LR)^k \\ &= ((L \circ R)^0)^q (L \circ R)^k \\ &= i^q (LR)^k = (L \circ R)^k. \end{aligned}$$

La segunda igualdad se sigue inmediatamente de la primera. ♦

**3.3 Definición.** El conjunto de las funciones paralela, relativa e intercambio de la séptima se denota con PLR. Específicamente,

$$\text{PLR} = \{(L \circ R)^n, R \circ (L \circ R)^n | n = 0, \dots, 11\}.$$

Es curioso que las funciones P y L no aparezcan mencionados explícitamente en la definición del conjunto PLR, pero podemos generar todo el conjunto  $\mathcal{M}$  sin emplearlas. Además, tanto P como L, sí están representadas porque el lector puede demostrar que

$$P = R \circ (L \circ R)^3 \tag{4.2}$$

y

$$L = R \circ (L \circ R)^{11}. \tag{4.3}$$

Estas igualdades se cumplen independientemente de que se apliquen a una tríada mayor o menor.

Otro asunto preocupante es que las funciones de la forma  $R \circ L$  introdujeran funciones distintas adicionales al conjunto. Sin embargo, como las funciones P, L y R son involutivas, cuando se aplica la función L primero, seguido de R, de forma consecutiva, también se obtiene la sucesión mencionada, pero al revés. El cuadro 4.2 muestra las relaciones entre las funciones  $L \circ R$  y  $R \circ L$ .

Ahora podemos concluir que la lista de todas las funciones  $(L \circ R)^n$  y  $R \circ (L \circ R)^m$  es mucho más exhaustiva de lo que aparenta. Contiene un conjunto de composiciones que incluyen las funciones P, L y R así como las composiciones de  $L \circ R$  y  $R \circ L$ . Más aún, estas 24 funciones distintas transforman cualquier elemento de  $\mathcal{M}$  en otro elemento distinto de  $\mathcal{M}$ .

En lo subsecuente, denotaremos a las composiciones  $L \circ R$  y  $R \circ L$  simplemente como  $LR$  y  $RL$ , respectivamente.

**3.4 Lema.** El conjunto PLR es cerrado bajo la composición  $\circ$ .

$R \circ (RL)^0 = R = L \circ (LR)^{11}$	$L \circ (LR)^6 = L \circ (RL)^5$
$LR = (RL)^{11}$	$(LR)^7 = (RL)^5$
$R \circ (RL) = L \circ (LR)^{10}$	$L \circ (LR)^7 = L \circ (RL)^4$
$(LR)^2 = (RL)^{10}$	$(LR)^8 = (RL)^4$
$R \circ (RL)^2 = L \circ (LR)^9$	$L \circ (LR)^8 = L \circ (RL)^3$
$(LR)^3 = (RL)^9$	$(LR)^9 = (RL)^3$
$R \circ (RL)^3 = L \circ (LR)^8$	$L \circ (LR)^9 = L \circ (RL)^2$
$(LR)^4 = (RL)^8$	$(LR)^{10} = (RL)^2$
$R \circ (RL)^4 = L \circ (LR)^7$	$L \circ (LR)^{10} = L \circ (RL)$
$(LR)^5 = (RL)^7$	$(LR)^{11} = RL$
$R \circ (RL)^5 = L \circ (LR)^6$	$L \circ (LR)^{11} = L \circ (RL)^0 = L$
$(LR)^6 = (RL)^6$	$(LR)^0 = (RL)^0$

Cuadro 4.2: Equivalencias entre las funciones  $LR$  y  $RL$ .

**Demostración.** Como se tienen dos tipos funciones principales en el conjunto,  $((LR)^n$  y  $R \circ (LR)^m$ ), se tienen cuatro composiciones posibles que deben examinarse, para asegurarse de que permanezcan en el conjunto PLR:

$$R \circ (LR)^n \circ R \circ (LR)^m, \quad (4.4)$$

$$(LR)^n \circ (LR)^m, \quad (4.5)$$

$$R \circ (LR)^n \circ (LR)^m, \quad (4.6)$$

$$(LR)^n \circ R \circ (LR)^m. \quad (4.7)$$

Hay que recordar siempre que  $L$  y  $R$  son involutivas, esto es, que  $L^2 = R^2 = i$ . Veamos primero el caso de la composición (4.4). Si  $m = n = 0$ , su pertenencia a PLR es clara porque

$$R \circ (LR)^0 \circ R \circ (LR)^0 = R \circ i \circ R \circ i = R^2 = i = LR^0.$$

Supongamos que  $R \circ (LR)^n \circ R \circ (LR)^n = i$  para  $n = 1, \dots, k$ . Entonces

$$\begin{aligned}
R \circ (LR)^{k+1} \circ R \circ (LR)^{k+1} &= R \circ (LR)^k \circ L \circ R \circ R \circ (LR)^{k+1} \\
&= R \circ (LR)^k \circ L \circ R^2 \circ (LR)^{k+1} \\
&= R \circ (LR)^k \circ L \circ (LR)^{k+1} \\
&= R \circ (LR)^k \circ L \circ L \circ R \circ (LR)^k \\
&= R \circ (LR)^k \circ L^2 \circ R \circ (LR)^k \\
&= R \circ (LR)^k \circ R \circ (LR)^k = i
\end{aligned}$$

por hipótesis de inducción, y en consecuencia también está en PLR. Si  $m > n$ , entonces

$$\begin{aligned}
R \circ (LR)^n \circ R \circ (LR)^m &= (R \circ (LR)^n \circ R \circ (LR)^n) \circ (LR)^{m-n} \\
&= i \circ (LR)^{m-n} = (LR)^{m-n}
\end{aligned}$$

mientras que si  $m < n$

$$\begin{aligned}
 R \circ (LR)^n \circ R \circ (LR)^m &= R \circ (LR)^{n-m} \circ (LR)^m \circ R \circ (LR)^m \\
 &= R \circ (LR)^{n-m-1} \circ L \circ (R \circ (LR)^m \circ R \circ (LR)^m) \\
 &= R \circ (LR)^{n-m-1} \circ L \circ i \\
 &= R \circ (LR)^{n-m-1} \circ L \\
 &= (RL)^{n-m} = (LR)^{11(n-m)}
 \end{aligned}$$

(pues por el cuadro 4.2 sabemos que  $RL = (LR)^{11}$ ) y ambos resultados pertenecen a PLR. Para (4.5) tenemos que

$$(LR)^n \circ (LR)^m = (LR)^{n+m} = (LR)^{n+m \bmod 12} \in \text{PLR}$$

usando el lema 3.2. El caso de (4.6) es una consecuencia directa de (4.5). Resta elucidar qué sucede con (4.7). Puesto que

$$\begin{aligned}
 (LR)^n \circ R \circ (LR)^m &= L \circ (R \circ (LR)^{n-1} \circ R \circ (LR)^m) \\
 &= R \circ (LR)^{11} \circ (R \circ (LR)^{n-1} \circ R \circ (LR)^m)
 \end{aligned}$$

usando el primer caso concluimos que también permanece en PLR. ♦

Se deja al lector, como ejercicio, mostrar que las operaciones P, L y R están bien definidas y que todas las composiciones posibles de P, L y R están en el conjunto PLR.

**3.5 Teorema.** El conjunto PLR forma un grupo bajo composición. En particular,

$$(R(LR)^n)^{-1} = R(LR)^n \quad \text{y} \quad ((LR)^n)^{-1} = (LR)^k$$

donde  $k = -n \bmod 12$ .

**Demostración.** El lema 3.4 demuestra que todas las composiciones posibles, incluyendo las inversas, permanecen en el conjunto PLR.

Así, todas las funciones P, L y R cumplen con todas las propiedades de grupo, ya que la asociatividad es una propiedad de las funciones. Aunque sabemos que los inversos existen, es de interés ver los inversos de los generadores del grupo PLR. Por la demostración del lema 3.4, para toda función de la forma  $R \circ (LR)^n$ , se tiene  $R \circ (LR)^n \circ R \circ (LR)^n = i$ . Por lo tanto,  $(R \circ (LR)^n)^{-1} = R \circ (LR)^n$ .

En cuanto a todas las funciones de la forma  $(LR)^n$ ,

$$((LR)^n)^{-1} = (LR)^{-n} = (LR)^{-n \bmod 12} = (LR)^k.$$

donde  $k = -n \bmod 12$ . ♦

$R \mapsto I_0$	$R \circ (LR)^4 \mapsto I_8$	$R \circ (LR)^8 \mapsto I_4$
$LR \mapsto T_1$	$(LR)^5 \mapsto T_5$	$(LR)^9 \mapsto T_9$
$R \circ (LR) \mapsto I_{11}$	$R \circ (LR)^5 \mapsto I_7$	$R \circ (LR)^9 \mapsto I_3$
$(LR)^2 \mapsto T_2$	$(LR)^6 \mapsto T_6$	$(LR)^{10} \mapsto T_{10}$
$R \circ (LR)^2 \mapsto I_{10}$	$R \circ (LR)^6 \mapsto I_6$	$R \circ (LR)^{10} \mapsto I_2$
$(LR)^3 \mapsto T_3$	$(LR)^7 \mapsto T_7$	$(LR)^{11} \mapsto T_{11}$
$R \circ (LR)^3 \mapsto I_9$	$R \circ (LR)^7 \mapsto I_5$	$R \circ (LR)^{11} \mapsto I_1$
$(LR)^4 \mapsto T_4$	$(LR)^8 \mapsto T_8$	$(LR)^0 \mapsto T_0$

Cuadro 4.3: El isomorfismo  $\phi : \text{PLR} \mapsto \text{TI}$ .**Problemas.**

**3.1.** Exhiba una trayectoria en el *Tonnetz* tal que una sucesión de funciones R y L transforme la tríada  $\{5, 9, 0\}$  en si misma, después de pasar por todas las otras tríadas de  $\mathcal{M}$  en el proceso.

**3.2.** Muestre que las operaciones P, L y R están bien definidas. Es decir, si  $[x]$  es una tríada de clases de tono en  $\mathcal{M}$  entonces, para toda  $x_1, x_2 \in [x]$  tenemos:

$$\begin{aligned}
 P(x_1) &= P(x_2), & \text{i.e.} & & P(\{a_1, b_1, c_1\}) &= P(\{a_2, b_2, c_2\}), \\
 L(x_1) &= L(x_2), & \text{i.e.} & & L(\{a_1, b_1, c_1\}) &= L(\{a_2, b_2, c_2\}), \\
 R(x_1) &= R(x_2), & \text{i.e.} & & R(\{a_1, b_1, c_1\}) &= R(\{a_2, b_2, c_2\}).
 \end{aligned}$$

**4.4. El Isomorfismo entre PLR y TI**

Ahora exhibiremos un isomorfismo explícito entre los grupos TI y PLR aunque, como ambos son isomorfos al grupo de simetrías del dodecágono (véase los ejercicios 4.2 y 4.3), son isomorfos por transitividad.

El isomorfismo entre los grupos TI y PLR que nos interesa no manda (como se podría pensar) una función en uno de los grupos a una función en el otro, tal que ambas transformen una tríada  $x$  en una misma tríada  $y$ . Considérese la transformación denotada por  $\phi$ , en el cuadro 4.3. Este es, precisamente, el isomorfismo que se verificará en el teorema 4.1.

El isomorfismo se construye de la siguiente forma. Primero se identifican los generadores y las identidades de los grupos TI y PLR. En otras palabras, los generadores de TI son  $T_1$  e  $I_0$ , con las relaciones

$$(T_1)^{12} = i \quad \text{y} \quad (I_0)^2 = i.$$

Asimismo, los generadores del grupo PLR son LR y R, con las relaciones

$$(LR)^{12} = i \quad \text{y} \quad R^2 = i.$$

Tales hechos nos sugieren hacer lo siguiente: llevar  $T_1$  a  $LR$  e  $I_0$  a  $R$ . La identidad  $T_0$ , necesariamente, se lleva a la identidad  $(LR)^0$ . Las otras funciones

revelan un patrón entre las potencias de RL y los subíndices de las funciones T e I.

**4.1 Teorema.** Existe un homomorfismo biyectivo  $\phi : \text{PLR} \rightarrow \text{TI}$  tal que

$$\phi((LR)^x) = T_x, \quad \phi(R \circ (LR)^x) = I_n,$$

donde  $n = -x \text{ mód } 12$ .

**Demostración.** Usando el cuadro 4.3 podemos concluir que la función es biyectiva. A continuación se hace una evaluación puntual de todas las posibles combinaciones de los generadores del grupo PLR. Se mostrará que para toda  $g, h \in \text{PLR}$  y para toda  $x \in \mathcal{M}$ ,

$$\phi(g \circ h)(x) = \phi(g)(\phi(h)(x)).$$

Sea  $x = \{a, b, c\} \in \mathcal{M}$ , y sean  $g = LR$  y  $h = R$ . Entonces el lado izquierdo de la ecuación es

$$\begin{aligned} \phi(g \circ h)(\{a, b, c\}) &= \phi((LR) \circ R)(\{a, b, c\}) \\ &= \phi(L \circ R \circ R)(\{a, b, c\}) \\ &= \phi(L)(\{a, b, c\}) && \text{(pues } R^2 = i) \\ &= \phi(R \circ (LR)^{11})(\{a, b, c\}) && \text{(usando (4.3))} \\ &= I_1(\{a, b, c\}) && \text{(por el cuadro 4.2)} \\ &= \{-a + 1, -b + 1, -c + 1\}, \end{aligned}$$

mientras que el lado derecho resulta

$$\begin{aligned} \phi(g)(\phi(h)(\{a, b, c\})) &= \phi(LR)(\phi(R)(\{a, b, c\})) \\ &= T_1(I_0(\{a, b, c\})) && \text{(por el cuadro 4.2)} \\ &= I_{1+0}(\{a, b, c\}) && \text{(por el lema 2.5)} \\ &= I_1(\{a, b, c\}) \\ &= \{-a + 1, -b + 1, -c + 1\}. \end{aligned}$$

A continuación, sean  $g = R$  y  $h = LR$ , entonces el lado izquierdo de la ecuación resulta ser

$$\begin{aligned} \phi(g \circ h)(\{a, b, c\}) &= \phi(R \circ LR)(\{a, b, c\}) \\ &= I_{11}(\{a, b, c\}) && \text{(por el cuadro 4.2)} \\ &= \{-a + 11, -b + 11, -c + 11\} \end{aligned}$$

mientras que el lado derecho resulta ser

$$\begin{aligned} \phi(g)(\phi(h)(\{a, b, c\})) &= \phi(R)(\phi(LR)(\{a, b, c\})) \\ &= I_0(T_1(\{a, b, c\})) && \text{(por el cuadro 4.2)} \\ &= I_{0-1}(\{a, b, c\}) && \text{(por el lema 2.5)} \\ &= I_{-1}(\{a, b, c\}) \\ &= I_{11}(\{a, b, c\}) \\ &= \{-a + 11, -b + 11, -c + 11\}. \end{aligned}$$

Ahora sean  $g = LR$  y  $h = LR$ , entonces el lado izquierdo de la ecuación es

$$\begin{aligned}
 \phi(g \circ h)(\{a, b, c\}) &= \phi((LR) \circ (LR))(\{a, b, c\}) \\
 &= \phi((LR)^2)(\{a, b, c\}) \\
 &= T_2(\{a, b, c\}) && \text{(por el cuadro 4.2)} \\
 &= \{a + 2, b + 2, c + 2\}
 \end{aligned}$$

mientras que el lado derecho es

$$\begin{aligned}
 \phi(g)(\phi(h)(\{a, b, c\})) &= \phi(LR)(\phi(LR)(\{a, b, c\})) \\
 &= T_1(T_1(\{a, b, c\})) && \text{(por el cuadro 4.2)} \\
 &= T_{1+1}(\{a, b, c\}) && \text{(por el lema 2.5)} \\
 &= T_2(\{a, b, c\}) \\
 &= \{a + 2, b + 2, c + 2\}.
 \end{aligned}$$

Finalmente, sean  $g = R$  y  $h = R$ , entonces el lado izquierdo de la ecuación es

$$\begin{aligned}
 \phi(g \circ h)(\{a, b, c\}) &= \phi(R \circ R)(\{a, b, c\}) \\
 &= \phi(i)(\{a, b, c\}) && \text{(pues } R^2 = i) \\
 &= \phi((LR)^0)(\{a, b, c\}) && \text{(por el cuadro 4.2)} \\
 &= T_0(\{a, b, c\}) && \text{(por el cuadro 4.2)} \\
 &= \{a, b, c\}
 \end{aligned}$$

mientras que el lado derecho es

$$\begin{aligned}
 \phi(g)(\phi(h)(\{a, b, c\})) &= \phi(R)(\phi(R)(\{a, b, c\})) \\
 &= I_0(I_0(\{a, b, c\})) && \text{(por el cuadro 4.2)} \\
 &= T_{0+0}(\{a, b, c\}) && \text{(por el lema 2.5)} \\
 &= T_0(\{a, b, c\}) \\
 &= \{a, b, c\}.
 \end{aligned}$$

Así es que  $\phi(g \circ h)(x) = \phi(g)(\phi(h)(x))$  para toda  $g, h \in \text{PLR}$  y para toda  $x \in \mathcal{M}$ . Esto demuestra que  $\phi$  es un isomorfismo. ♦

## Problemas.

### 4.1. Dado el lema

Sea  $x \in \{(LR)^n, R \circ (LR)^n\}$ , y  $y = a \circ x$ , donde  $a \in \{P, L, R\}$ .  
Entonces  $y = a \circ x \in \text{PLR}$ .



demuestre por inducción que todas las posibles composiciones de P, L y R están en el conjunto PLR. (Sugerencia: exprese  $P$  de la forma  $R \circ (LR)^3$  y  $L$  de la forma  $R \circ (LR)^{11}$  y, junto con  $R$ , se verifica que para  $n = 1$ ,  $x \in \text{PLR}$  en los tres casos. Luego, suponga que  $x$  tiene longitud a lo más  $k$ ).

**4.2.** Muestre que el grupo TI es isomorfo al grupo diedral de orden  $n = 12$ , es decir, que

$$(T_1)^n = i, \quad (I_0)^2 = i, \quad (4.8)$$

$$I_0 \circ T_1 = T_1^{n-1} \circ I_0, \quad (4.9)$$

$$\text{TI} = \{i, T_1, T_2, \dots, T_{n-1}, I_0, I_1, \dots, I_{n-1}\}. \quad (4.10)$$

**4.3.** Muestre que el grupo PLR es isomorfo al grupo diedral de orden  $n = 12$ , es decir, que

$$(LR)^n = i, \quad R^2 = i, \quad (4.11)$$

$$R \circ (LR) = (LR)^{n-1} \circ R, \quad (4.12)$$

$$\text{PLR} = \{i, (LR), (LR)^2, \dots, (LR)^{11}, R, R \circ (LR), \dots, R \circ (LR)^{11}\}. \quad (4.13)$$

## 4.5. La Dualidad de los Grupos TI y PLR

Sabemos del capítulo 3, definición 2.3, lo que significa que un grupo  $G$  actúa sobre un conjunto  $X$ .

**5.1 Lema.** El conjunto  $\mathcal{M}$  es un TI-conjunto. En otras palabras, el grupo TI actúa sobre  $\mathcal{M}$ .

**Demostración.** Definimos las acciones de  $T_m, I_n \in \text{TI}$  sobre  $x \in \mathcal{M}$  a través de la evaluación, es decir,

$$\phi(T_m, x) = T_m * x = T_m(x) \quad \text{y} \quad \phi(I_n, x) = I_n * x = I_n(x).$$

Puesto que para cualesquiera funciones  $f, g \in \text{TI}$  se satisface

$$(f \circ g) * x = (f \circ g)(x) = f(g(x)) = f * (g * x)$$

y, además,  $i * x = T_0 * x = T_0(x) = x = i(x)$ , se sigue que TI actúa sobre  $\mathcal{M}$ . ♦

**5.2 Lema.** El conjunto  $\mathcal{M}$  es un PLR-conjunto. En otras palabras, el grupo PLR actúa sobre  $\mathcal{M}$ .

**Demostración.** Definiendo la acción a través de la evaluación, la demostración es esencialmente la misma que la del lema anterior. ♦

También del capítulo 3, recordemos la definición de la órbita de  $X$  bajo  $G$ .

**5.3 Lema.** Para toda  $x \in \mathcal{M}$ , la órbita  $\text{TI}x$  de  $x$  es  $\mathcal{M}$ .

**Demostración.** Como se ilustra en las figuras 4.2 y 4.3, cuando todas las funciones que se aplican a una sola tríada, se genera la totalidad del conjunto  $\mathcal{M}$ . Aún y cuando la tabla sólo muestre las funciones aplicadas al acorde de C mayor, se puede verificar fácilmente que las funciones actúan de manera igual sobre cualquier tríada mayor o menor. Así es que la órbita del grupo TI es:

$$\text{TI}x = \{f * x \mid f \in \text{TI}\} = \mathcal{M}.$$

♦

Dejamos como ejercicio la demostración de que para toda  $x \in \mathcal{M}$ , la órbita  $\text{PLR}x$  también es  $\mathcal{M}$ . Recordemos del capítulo 3 la definición de subgrupo de isotropía, o estabilizador, así como el teorema órbita-estabilizador (teorema 2.8).

**5.4 Lema.** Sea  $x \in \mathcal{M}$ . Entonces el estabilizador de  $x$  bajo PLR es

$$\text{PLR}_x = \{f \in \text{PLR} \mid f * x = x\} = i = (LR)^0$$

**Demostración.** Usamos el teorema 3.2.8. para ver que

$$|\text{PLR}_x| = \frac{|\text{PLR}|}{|\text{PLR}x|}.$$

Pero  $|\text{PLR}| = 24$  pues hay 24 funciones in PLR y  $|\text{PLR}x| = 24$  dado que  $\text{PLR}x = \mathcal{M}$ . Esto nos da

$$|\text{PLR}_x| = \frac{24}{24} = 1.$$

Naturalmente,  $i * x = x$ , así que  $i \in \text{PLR}_x$  y es el único miembro del conjunto. Por lo tanto, el estabilizador es trivial. ♦

Dejamos como ejercicio la demostración de que si  $x \in \mathcal{M}$ , entonces el estabilizador de  $x$  bajo TI es

$$\text{TI}x = \{f \in \text{TI} \mid f * x = x\} = i = T_0.$$

**5.5 Definición.** Una acción del grupo  $G$  en el conjunto  $X$  es **libre** si para cualesquiera  $g, h \in G$  y  $x \in X$  se cumple que  $g * x \neq h * x$ . Esta condición es equivalente a que  $g * x = x$  si, y sólo si,  $g$  es el elemento identidad de  $G$ .

**5.6 Corolario.** Los grupos TI y PLR actúan libremente sobre  $\mathcal{M}$ .

**Demostración.** Ya hemos establecido que para toda  $x \in \mathcal{M}$  los estabilizadores son precisamente  $\text{TI}_x = i$  y  $\text{PLR}_x = i$ . Por lo tanto, las acciones de los grupos TI y PLR sobre  $\mathcal{M}$  satisfacen la definición de acción libre. ♦

**5.7 Definición.** Una acción del grupo  $G$  en el conjunto  $X$  es **transitiva** si para cualesquiera  $x, y \in X$  existe  $g \in G$  tal que  $g * x = y$ .

**5.8 Definición.** Una acción del grupo  $G$  en el conjunto  $X$  es **regular** si es transitiva y libre.

Ahora demostraremos que los grupos TI y PLR actúan regularmente sobre  $\mathcal{M}$ .

**5.9 Proposición.** Las acciones de los grupos TI y PLR sobre  $\mathcal{M}$  son regulares, es decir, son transitivas y libres.

**Demostración.** Podemos deducir la regularidad de las figuras 4.2 y 4.3 y la ecuación (4.1). Primeramente, se ve que todas las funciones actuando sobre cualquier  $x$  producen la totalidad del conjunto  $\mathcal{M}$ . En otras palabras, para toda  $x$  y  $y$  en  $\mathcal{M}$  siempre existe una función  $g$  tal que  $g(x) = y$ . Más aún, esto sucede sin que ocurra una repetición de tríadas, lo cual significa que sólo una función transforma cualquier tríada en cualquier otra tríada. Por lo tanto,  $g$  es única.

Por otro lado, se puede usar lo encontrado arriba para inferir la regularidad. Puesto que para todo  $x$  se cumple que  $TIx = \mathcal{M}$ , entonces dados  $z, y \in \mathcal{M}$  se cumple que existen  $f, g \in TI$  tales que  $f * x = z$  y  $g * x = y$ . Esto quiere decir que

$$f^{-1}(z) = f^{-1} * (f * x) = (f^{-1} \circ f) * x = i * x = x$$

y que

$$(g \circ f^{-1}) * z = g * (f^{-1}(z)) = g * x = y$$

por lo que  $g \circ f^{-1}$  es un elemento del grupo que envía a  $z$  en  $y$  a través de la acción. Finalmente, si existen  $g_1, g_2 \in TI$  tales que  $g_1 * x = g_2 * x$  entonces  $(g_2^{-1} \circ g_1) * x = x$ . Pero si el estabilizador de  $x$  es trivial, así que  $g_2^{-1} \circ g_1 = i$  y por ello  $g_2 = g_1$ . Esto demuestra que la acción de  $TI$  es regular. El caso de PLR es análogo. ♦

Recuérdese la definición de centralizador de un grupo del capítulo 3. El concepto de centralizador se basa en la conmutatividad, por lo que examinaremos la conmutatividad entre los elementos de TI y PLR.

**5.10 Lema.** Todos los elementos de los grupos PLR y TI conmutan.

**Demostración.** Basta mostrar la conmutatividad de los generadores de cada grupo, o sea, que

$$T_1 \circ (LR) = (LR) \circ T_1, \quad (4.14)$$

$$T_1 \circ R = R \circ T_1, \quad (4.15)$$

$$I_0 \circ (LR) = (LR) \circ I_0, \quad (4.16)$$

$$I_0 \circ R = R \circ I_0. \quad (4.17)$$

Se deja como ejercicio completar la demostración de este lema. ♦

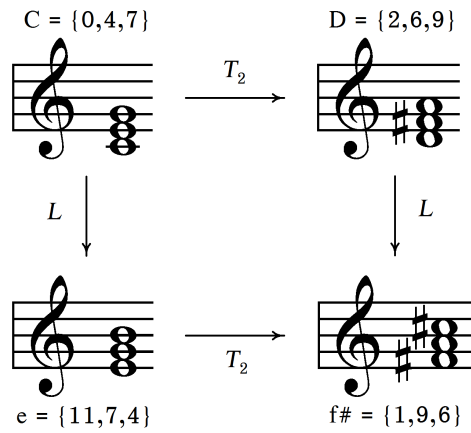


Figura 4.5: Ilustración musical de  $T_2 \circ L(C) = L \circ T_2(C)$ .

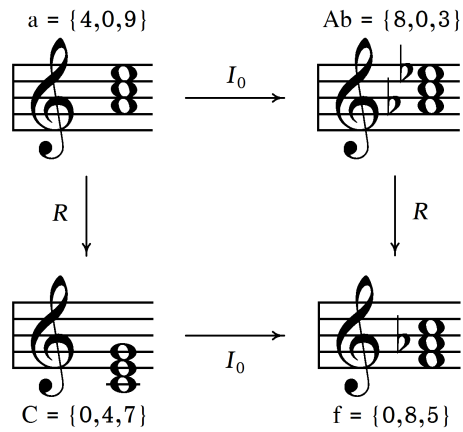


Figura 4.6: Ilustración musical de  $I_0 \circ R(a) = R \circ I_0(a)$ .

Las figuras 4.5 y 4.6 proporcionan ejemplos musicales de la conmutatividad con el uso de los diagramas conmutativos.

Puesto que las relaciones de conmutatividad son válidas cuando se evalúan en cualquier elemento de  $\mathcal{M}$ , para toda  $f$  en TI y para toda  $g$  en PLR vale el diagrama conmutativo

$$\begin{array}{ccc} \mathcal{M} & \xrightarrow{f} & \mathcal{M} \\ g \downarrow & & \downarrow g \\ \mathcal{M} & \xrightarrow{f} & \mathcal{M}. \end{array}$$

Por ejemplo,

$$\begin{array}{ccc} \mathcal{M} & \xrightarrow{T_n} & \mathcal{M} \\ L \downarrow & & \downarrow L \\ \mathcal{M} & \xrightarrow{T_n} & \mathcal{M} \end{array}$$

significa que  $L \circ T_n = T_n \circ L$ .

La naturaleza conmutativa de los grupos TI y PLR nos lleva a la última noción que se requiere para la dualidad.

Como los grupos TI y PLR son transformaciones de  $\mathcal{M}$  en sí mismo, son grupos de permutaciones y, por lo tanto, subgrupos del grupo simétrico en  $\mathcal{M}$  (i.e.  $\text{Sym}(\mathcal{M})$ , que es el grupo de todas las biyecciones de  $\mathcal{M}$  en sí mismo bajo la composición de funciones). Recuérdese la definición de centralizador del capítulo 3. Examinaremos los centralizadores de cada grupo dentro del grupo más grande  $\text{Sym}(\mathcal{M})$ .

**5.11 Lema.** Se cumple que

$$C_{\text{Sym}(\mathcal{M})}(\text{TI}) = \text{PLR} \quad \text{y} \quad C_{\text{Sym}(\mathcal{M})}(\text{PLR}) = \text{TI}.$$

**Demostración.** Primero, considérese el centralizador del grupo TI,

$$C_{\text{Sym}(\mathcal{M})}(\text{TI}) = \{g \in \text{Sym}(\mathcal{M}) \mid fg = gf, \forall f \in \text{TI}\}.$$

Por el lema 5.10 tenemos que para toda  $g \in \text{PLR}$  y  $f \in \text{TI}$ ,  $f \circ g = g \circ f$ . Entonces PLR está contenido en  $C_{\text{Sym}(\mathcal{M})}(\text{TI})$ . Debemos verificar que no existen otras funciones aparte de las del grupo PLR en  $C_{\text{Sym}(\mathcal{M})}(\text{TI})$ . Comenzamos por investigar el estabilizador de  $x$  en  $C_{\text{Sym}(\mathcal{M})}(\text{TI})$ . Supóngase que  $h \in C_{\text{Sym}(\mathcal{M})}(\text{TI})$  y que fija a  $x \in \mathcal{M}$ . Sea  $g \in \text{TI}$ . Entonces

$$\begin{aligned} h(x) &= x, \\ g(h(x)) &= g(x), \\ h(g(x)) &= g(x), \end{aligned}$$

donde la última igualdad se sigue del hecho de que  $h$  está en el centralizador. Por la proposición 5.9 sabemos que TI actúa regularmente y, de esta manera, para toda  $y \in \mathcal{M}$  existe  $g$  tal que  $y = g(x)$ . Esto muestra que para toda  $x, y \in \mathcal{M}$

$$h(y) = h(g(x)) = g(x) = y.$$

Luego  $h(y) = y$  para toda  $y \in \mathcal{M}$ . Sin embargo, el único elemento en  $C_{\text{Sym}(\mathcal{M})}(\text{TI})$  que fija cualquier elemento en  $C_{\text{Sym}(\mathcal{M})}(\text{TI})$  es  $i$  y, por lo tanto,  $h$  es el elemento identidad. Así es que  $C_{\text{Sym}(\mathcal{M})}(\text{TI})_x = i$ .

Aplicando a  $C_{\text{Sym}(\mathcal{M})}(\text{TI})_x$  el teorema 2.8 del capítulo 3 (de la órbita-estabilizador), obtenemos

$$|C_{\text{Sym}(\mathcal{M})}(\text{TI})_x| = \frac{|C_{\text{Sym}(\mathcal{M})}(\text{TI})|}{|C_{\text{Sym}(\mathcal{M})}(\text{TI})_x|} = |C_{\text{Sym}(\mathcal{M})}(\text{TI})| \leq |\mathcal{M}| = 24,$$

pues la órbita de  $x$  bajo  $C_{\text{Sym}(\mathcal{M})}(\text{TI})$  está contenida en  $\mathcal{M}$ . Por otro lado,  $\text{PLR} \subseteq C_{\text{Sym}(\mathcal{M})}(\text{TI})$ , así que

$$24 = |\text{PLR}| \leq |C_{\text{Sym}(\mathcal{M})}(\text{TI})|.$$

Combinando estas desigualdades, vemos que  $|C_{\text{Sym}(\mathcal{M})}(\text{TI})| = 24$  y necesariamente el centralizador de TI es el grupo PLR. Queda por mostrar que el centralizador del grupo PLR es el grupo TI. Sin embargo, sólo es necesario voltear los papeles del grupo TI con el grupo PLR, desde el comienzo de la demostración, para mostrar que  $C_{\text{Sym}(\mathcal{M})}(\text{PLR}) = \text{TI}$ . ♦

**5.12 Definición.** Sean  $H$  y  $K$  subgrupos del grupo simétrico  $\text{Sym}(X)$  (i.e.  $H$  y  $K$  son grupos de permutaciones sobre el conjunto  $X$ ). Entonces  $H$  y  $K$  se dicen **duales** si cada uno actúa regularmente sobre  $X$  y uno es el centralizador del otro en  $\text{Sym}(X)$ .

Los múltiples lemas y teoremas ya vistos se usan para deducir la dualidad de los grupos TI y PLR.

**5.13 Teorema.** Los grupos TI y PLR son duales.

**Demostración.** Se sigue de la proposición 5.9 y el lema 5.11. ♦

La dualidad entre los grupos TI y PLR ya existía en la música antes de que fuera formalizada matemáticamente. Consideremos la progresión de acordes de la figura 4.7, que aparece en 28 variaciones del Canon en D de Johann Pachelbel. Se puede ver la dualidad claramente por medio del siguiente diagrama conmutativo:

$$\begin{array}{ccc} \text{D} & \xrightarrow{T_7} & \text{A} \\ R \downarrow & & \downarrow R \\ \text{b} & \xrightarrow{T_7} & \text{f}\sharp. \end{array}$$

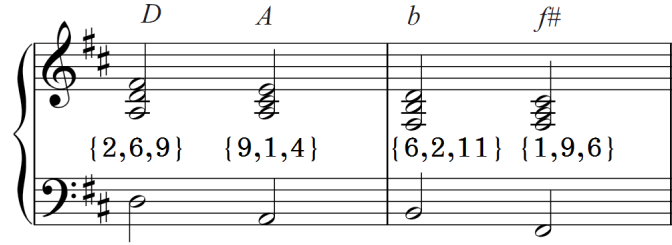


Figura 4.7: Progresión de acordes del Canon en D de Pachelbel.

Como se ha estudiado la dualidad entre los grupos TI y PLR, la composición de las funciones TI y PLR es lo que más interesa. Por este motivo, las funciones que se presentan horizontalmente estarán en un grupo diferente de las que corren vertical. El objeto es encontrar la transformación entre cada triada, consciente de que hay que buscar dos funciones, una de TI y otra de PLR. Asimismo, siempre tiene que haber un cambio en paridad, por la naturaleza de las transformaciones. En la figura 4.7, la paridad de las triadas horizontales es la misma, y las triadas verticales son de paridad opuesta. Es claro que las funciones T mantienen la paridad de la triada sobre la cual se actúa y, por lo tanto, la función horizontal debe ser una transposición. La transformación vertical tiene que cambiar la paridad de la triada y debe, por lo tanto, ser un número impar de composiciones de funciones en PLR (porque ya usamos una función del grupo TI). El acorde mayor D se encuentra a siete semitonos de A y, por lo mismo, las transformaciones horizontales son  $T_7$ . Ahora debemos encontrar una función, o composición de funciones, del grupo PLR que transforme A mayor en F# menor y que transforme D mayor en B menor. Tanto A como D son tres semitonos arriba de la triada en que se deben transformar (lo cual quiere decir que son los mayores relativos de sus respectivos menores). Así es que la función vertical tiene que ser R.

### Problemas.

**5.1.** Demuestre que para toda  $x \in \mathcal{M}$ , la órbita de  $x$  bajo PLR es  $\mathcal{M}$ .

**5.2.** Demuestre que si  $x \in \mathcal{M}$ , el estabilizador  $\text{TI}x$  es

$$\text{TI}x = \{f \in \text{TI} \mid f * x = x\} = T_0.$$

**5.3.** Complete la demostración del lema 5.10 (que todos los elementos de los grupos PLR y TI conmutan).

# Bibliografía y Referencias

- [A] Armstrong, M. A. *Groups and Symmetry*. UTM. Springer. 1988.
- [B-M] Birkhoff, G. y MacLane, S. *Algebra*. Macmillan. 1968.
- Bourbaki, N. *Algebra I*. Addison Wesley. 1973.
- [C] Cohn, R. *Neo-Riemannian operations, parsimonious trichords and their Tonnetz representations*. Journal of Music Theory, 41 (1997), 1-66.
- [CFS] Crans, A., Fiore, T. y Satyendra, R. *Musical Actions of Dihedral Groups*. [http://arxiv.org/PS\\_cache/arxiv/pdf/0711/0711.1873v2.pdf](http://arxiv.org/PS_cache/arxiv/pdf/0711/0711.1873v2.pdf), 2008.
- [DP] Du Plessis, J. *Transformation Groups and Duality in the Analysis of Musical Structure*. Tesis de maestría, Universidad Estatal de Georgia (EU), 2008.
- [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.
- [L1] Lluís-Puebla, E. *Álgebra Homológica, Cohomología de Grupos y K-Teoría Algebraica Clásica*. Segunda Edición. Publicaciones Electrónicas. Sociedad Matemática Mexicana. Serie: Textos. Vol. 5. 2005.
- [L2] Lluís-Puebla, E. *Álgebra Lineal, Álgebra Multilineal, y K-Teoría Algebraica Clásica*. Segunda Edición. Publicaciones Electrónicas. Sociedad Matemática Mexicana. Serie: Textos. Vol. 9. 2008.
- [M] Mazzola, G. *The Topos of Music*. Birkhäuser-Verlag. 2002.
- 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

$\mathbb{Z}$ , 7	$(x)$ , 32
$\mathbb{Z}_3$ , 9	$\cdots \rightarrow G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i}$
$\Delta_3$ , 11	$\rightarrow G_{i+1} \xrightarrow{f_{i+1}} \cdots$ , 38
$xfy$ , 12	$\{C_n\}_{n \in \mathbb{Z}}$ , 41
$\Sigma_n$ , 13	$G/H$ , 42
$(V, +, \mu)$ , 13	$x \equiv_i y \pmod{H}$ , 43
$(G, +)$ , 13	$x \equiv_d y \pmod{H}$ , 43
$+: G \times G \rightarrow G$ , 13	$H \triangleleft G$ , 44
$+(u, v)$ , 13	$H_n(C)$ , 47
$O \in G$ , 13	$H^n(C)$ , 48
$I_s$ , 14	$\text{In}(G)$ , 53
$R$ , 14, 97	$\text{Aut}(G)$ , 53
$RI_s$ , 14	$HN$ , 54
$\mathcal{T}(n)$ , 14	$\text{coim } g$ , 54
$ST_s$ , 15	$\text{coker } g$ , 54
$o(G)$ , 16	$\prod_{i \in I} H_i$ , 54
$ G $ , 16	$\bigoplus_{i \in I} G_i$ , 54
$e^t$ , 17	$\wp(S)$ , 55
$(\Lambda, +, \cdot)$ , 19	$G_1 \times G_2$ , 55
$(A, +, \mu, \cdot)$ , 20	$\prod_{i \in I}^d G_i$ , 57
$\mathcal{I}$ , 20	$\sum_{i \in I} G_i$ , 57
$T^k(V)$ , 23	$\chi(C)$ , 63
$\bigwedge^k V$ , 23	$\beta_n(C)$ , 63
$\cong$ , 26	$(i_1, i_2, \dots, i_r)$ , 65
$\mapsto$ , 27	$Gx$ , 67
$\twoheadrightarrow$ , 27	$G_x$ , 67
$\ker f$ , 27	$C_H(x)$ , 67
$\text{im } f$ , 27	$C_G(x)$ , 67
$H < G$ , 27	$N_H(K)$ , 67
$\text{Hom}(X, Y)$ , 28	$N_G(K)$ , 67
$D_n$ , 30	$hKh^{-1}$ , 71
$V$ , 30	
$\text{Hom}(G, G')$ , 31	

$sg(\sigma)$ , 71  
 $(X|R)$ , 75  
 $X \otimes Y$ , 79  
 $\sharp$ , 88  
 $\flat$ , 88  
 $\mathcal{M}$ , 90  
 $T_n$ , 91

$I_n$ , 93  
TI, 95  
 $P$ , 97  
 $L$ , 97  
PLR, 100  
 $\text{Sym}(M)$ , 110

# Índice Analítico

- acción, 18
  - de un grupo en un conjunto, 66
  - por conjugación, 67
  - libre, 107
  - regular, 108
  - transitiva, 108
- acorde, 68, 89
  - aumentado, 69
  - de la escala, 47
  - mayor, 89
  - menor, 90
  - paridad del, 97
- afinación equitemperada, 88
- alfabeto, 72
- álgebra, 20
  - de Grassmann, 23
  - tensorial, 23
  - exterior, 23
  - graduada, 23
- álgebras
  - asociativas, 22
  - conmutativas, 22
  - con uno, 22
- anillo, 19
  - conmutativo, 19
  - con división, 19
  - con identidad, 19
  - con uno, 19
- automorfismo, 27, 49
  - exterior, 53
  - interior, 49, 53
- base del grupo abeliano libre, 76, 77
- cadena, 41
- cadenas de grado  $n$ , 47
- campo, 19
- característica de Euler-Poincaré, 63
- centralizador, 67
- cerrado, 12
- ciclo de longitud  $r$ , 65
- clase conjugada, 67
- clase de automorfismo, 53
- clase de homología, 47
- clase lateral, 42
  - derecha, 44
  - izquierda, 44
- cocadena, 42
- codominio, 7
- coeficientes de torsión, 61, 63
- coimagen, 54
- composición, 8
- congruente
  - por la derecha, 43
  - por la izquierda, 43
- conjugado, 67
- conmutador, 48
- conmutativo, 14
- conúcleo, 54
- diagrama, 40
  - conmutativo, 40
- diferenciales, 47
- dominio, 7
  - entero, 19
- elemento de identidad, 13, 25
  - derecho, 24

- izquierdo, 24
  - elementos relacionados, 67
  - endomorfismo, 27
  - epimorfismo, 27
  - equivalencia enarmónica, 88
  - escala, 47
    - cromática, 10, 47, 88
    - de  $C$  mayor, 10
    - de  $F$  mayor, 10
  - espacio tensorial de grado  $k$ , 23
  - estabilizador, 67
  - estable, 12
  - estructura algebraica, 12
- factores invariantes, 62
- fronteras, 47
- función, 7
  - biaditiva universal, 80
- $G$ -conjunto, 66
- generador, 32
- generadores, 75
- grupo, 12, 13, 24
  - abeliano, 24
  - libre, 75, 76
  - libre de rango  $r$ , 62
  - libre generado por, 76
- afín general, 68
- cíclico
  - de orden  $n$ , 32
  - generado por, 32
  - infinito, 32
- cociente, 42
- conmutativo, 14, 24
- con operadores, 18
- cuatro de Klein, 30
- de cohomología, 48
- de homología, 47
- diedral, 30, 75
- dual, 111
- finitamente generado, 61
- libre en el conjunto  $X$ , 73
- libre generado por los elementos
  - del conjunto  $X$ , 75
- orden de, 16
- simple, 46
- grupoide, 14
- grupos de orden menor que 16, 77
- grupos isomorfos, 27
- homología de la cadena, 47
- homólogos, 47
- homomorfismo
  - de anillos, 19
  - de grupos, 17
  - de  $\Lambda$ -módulos, 19
  - identidad, 30
  - inducido por, 29, 49
  - trivial, 27, 30
- identidad izquierda, 24
- imagen, 8, 27
- índice, 46
- intercambio de la séptima, 97
- intervalo de contrapunto, 20
  - orientación, 20
- inversión, 93
  - respecto a un tono, 14
- inverso, 14, 25, 26
  - derecho, 24
  - izquierdo, 24
- inyección canónica, 59
- isomorfismo, 26, 27
- juego completo de residuos módulo, 9
- ley de composición, 8
- magma, 14
- módulo
  - finitamente generado, 20
  - izquierdo, 19
  - libre, 20
  - proyectivo, 20
- monomorfismo, 27
- morfismo
  - cero, 37
  - de cadenas, 41
  - de cocadenas, 42
  - trivial, 37
- motivo, 14, 55
- multiplicación, 20

- normalizador, 67
- núcleo, 27
- número de Betti, 63
- octava, 10, 88
- operación
  - binaria, 8, 12
  - inducida, 12
  - $n$ -aria, 12
  - nula, 12
  - ternaria, 12
  - unaria, 12
- operador, 18
- operadores frontera, 47
- órbita, 65, 67
- orden, 16
- palabra, 72
  - reducida, 73
- permutación
  - impar, 71
  - par, 71
- $p$ -grupo, 71
- presentación, 75
  - libre, 75
- presentaciones isomorfas, 75
- Primer Teorema de Isomorfismo, 50
- Primer Teorema de Sylow, 71
- producto, 55
  - directo
    - externo, 54
    - externo débil, 57
    - interno, 58
  - tensorial, 78
- propiedad universal del producto directo, 57
- propiedades del producto tensorial, 84
- proyección, 55
  - canónica, 43, 44, 60
  - natural, 44
- $p$ -subgrupo de Sylow, 71
- rango, 62
  - finito, 77
  - infinito, 77
- red de subgrupos, 35
- relaciones, 75
- retrogradación, 14
  - con inversión, 14
- Segundo Teorema de Isomorfismo, 52
- Segundo Teorema de Sylow, 71
- semigrupo, 14
- semitono, 34, 88
- signo de una permutación, 71
- simetría afín, 68
- sistema algebraico, 12
- subgrupo, 27
  - conjugado, 71
  - de isotropía, 67
  - impropio, 28
  - normal, 44
  - propio, 28
  - trivial, 28
- sucesión
  - exacta, 38
    - corta, 38
    - corta escindible, 86
  - semiexacta, 37
- suma directa
  - completa, 54
  - externa, 57
- Teorema
  - de Cauchy, 72
  - de Lagrange, 45
  - primero de isomorfismo, 50
  - primero de Sylow, 71
  - segundo de isomorfismo, 52
  - segundo de Sylow, 71
  - tercero de isomorfismo, 53
  - tercero de Sylow, 71
- Tercer Teorema de Isomorfismo, 53
- Tercer Teorema de Sylow, 71
- Tonnetz*, 97
- tono, 10
- translación, 66, 71
- transposición, 65, 91
- triada, 89
  - de clases de tonos, 90
  - paralela, 97
  - relativa, 97

## **Los Autores**

### **Octavio A. Agustín-Aquino**

Octavio Alberto Agustín Aquino estudió la Licenciatura en Matemáticas Aplicadas en la Universidad Tecnológica de la Mixteca (Huajuapán de León, Oaxaca) y la Maestría en Ciencias Matemáticas en la Universidad Nacional Autónoma de México. Actualmente es estudiante del Doctorado en Ciencias Matemáticas en la UNAM bajo la dirección conjunta de Emilio Lluís Puebla, Guerino Mazzola y Rodolfo San Agustín Chi. Su investigación está encaminada a extender la teoría matemática del contrapunto desarrollada por Guerino Mazzola.

### **Janine du Plessis**

Janine du Plessis es originaria de Sudáfrica y realizó sus Estudios Profesionales y de Maestría en Matemática en la Universidad Estatal de Georgia (Georgia State University), donde realizó su tesis bajo la dirección de Mariana Montiel. También llevó a cabo estudios de Música en la misma universidad. Ayudó a fortalecer el Club de Matemáticas y Estadística en el Departamento de Matemáticas y Estadística de GSU y ha trabajado activamente con alumnos a todos los niveles para infundirles interés en la Matemática y sus diferentes aplicaciones. Ha organizado actividades en la Escuela Sabatina de la Universidad para estudiantes sobresalientes y ha trabajado en escuelas preparatorias en Atlanta. Actualmente enseña matemáticas en Herzing College mientras hace sus planes para continuar sus estudios de doctorado.

### **Emilio Lluís-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 más de treinta 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 Cátedra 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.

### **Mariana Montiel**

Mariana Montiel realizó sus Estudios Profesionales y de Maestría en Matemática en la Universidad Nacional Autónoma de México. En 2005 obtuvo su Doctorado en Matemática en Estados Unidos. Es catedrática de la Universidad Estatal de Georgia (Georgia State University) en el Departamento de Matemáticas y Estadística desde 2006. Su investigación se enfoca hacia la Teoría Matemática de la Música y las Matemáticas como un Sistema Semiótico, con énfasis en el aspecto del lenguaje.

Ha dirigido tesis y proyectos de investigación en México y Estados Unidos en el área de la Teoría Matemática de la Música. Ha publicado artículos y colaborado en libros en torno a la aplicación de la Teoría de Categorías a la Teoría Matemática de la Música. Actualmente desarrolla cursos multidisciplinarios para estudiantes de Matemáticas, Ciencias de la Computación y Música, en torno al software RUBATO Composer, producto de investigadores de América y Europa.

Ha recibido varias becas y subsidios de fundaciones e instituciones de México y Estados Unidos como Conacyt, Telmex, la Fundación UNAM, la Universidad de New Hampshire y la Fundación para la Investigación de la Universidad Estatal de Georgia. Colabora internacionalmente y hace traducciones de artículos sobre Matemática y Educación Matemática. Algunas de sus publicaciones se encuentran en editoriales con distribución mundial, como Birkhuser y Springer Verlag. Nova Science Publishers está por publicar su trabajo de colaboración con colegas de las universidades de Navarra y Barcelona.



## 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 (en particular en la Música) 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 está basado en el de “Teoría de Grupos: un primer curso” de Emilio Lluís-Puebla publicado en esta misma serie. Contiene el material correspondiente al curso sobre la materia que se imparte en la Facultad de Ciencias de la Universidad Nacional Autónoma de México, aunado a material optativo introductorio a un curso básico de la Teoría Matemática de la Música.

Este texto sigue el enfoque de los otros textos del Emilio Lluís-Puebla 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 cuatro capítulos. 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. A lo largo de los primeros tres capítulos se incluyen ejemplos representativos (no numerados) de las aplicaciones de la Teoría de Grupos a la Teoría Matemática de la Música, para estudiantes que ya tienen conocimiento de la Teoría Musical.

En el capítulo 4 se exponen con detalle más aplicaciones de la Teoría de Grupos a la Teoría Musical. Se explican algunos aspectos básicos de la Teoría Matemática de la Música y, en el proceso, se pretende dar elementos a lectores de diversos antecedentes, tanto en la Matemática como en la Música. Por este motivo, los ejemplos se siguen de algunos aspectos teóricos sobresalientes de los capítulos previos; los aspectos y términos musicales son introducidos conforme se van necesitando para que un lector sin formación musical pueda entender la esencia de cómo la Teoría de Grupos es empleada para explicar ciertas relaciones musicales ya establecidas. Asimismo, para el lector con conocimiento de la Teoría Musical, este capítulo provee elementos concretos, así como motivación, para comenzar a comprender la Teoría de Grupos.