

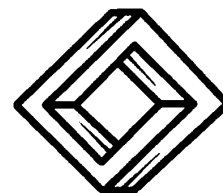
**Publicaciones Electrónicas
Sociedad Matemática Mexicana**

Álgebra Moderna

Emilio Lluis-Puebla

www.smm.org.mx

Serie: Textos. Vol. 22 (2021)



Álgebra Moderna

Emilio Luis-Puebla

Universidad Nacional Autónoma de México



Publicaciones Electrónicas
Sociedad Matemática Mexicana

Índice General

Prefacio	5
Introducción	7
I Estructuras Algebraicas y Propiedades Elementales	15
I.1 Operaciones Binarias	15
I.2 Estructuras Algebraicas	22
I.3 Propiedades Elementales de Grupos	28
I.4 Grupos Cíclicos	39
II Grupos Cociente, Teoremas de Isomorfismo y Productos	43
II.1 Sucesiones Exactas	43
II.2 Grupos Cociente	49
II.3 Teoremas de Isomorfismo	57
II.4 Productos	64
III Grupos Libres, Producto Tensorial y Teoremas de Sylow	71
III.1 Grupos Abelianos Finitamente Generados	71
III.2 Permutaciones y Órbitas	75
III.3 Grupos Libres	85
III.4 Producto Tensorial	92
III.5 Teoremas de Sylow	101
IV Teoría de Anillos	111
IV.1 Anillos	111
IV.2 Propiedades Elementales y Teoremas de Isomorfismo	118

IV.3 Polinomios y Campo de Cocientes	127
V Teoría de Campos y	
Teoría de Galois	139
V.1 Extensiones de Campos	139
V.2 Automorfismos y más sobre extensiones	151
V.3 Teoría de Galois	160
Bibliografía y Referencias	169
Lista de Símbolos	171
Índice Analítico	175

Prefacio

El éxito de la Teoría de Grupos es impresionante y extraordinario. Es la rama más poderosa e influyente de toda la Matemática. Influye en casi todas las disciplinas científicas, artísticas y en la propia Matemática de una manera fundamental. Lo que realmente se ha hecho en la Teoría de Grupos, es extraer lo esencial de diversas situaciones donde ocurre. Dado un conjunto no vacío, definimos una operación binaria en él, tal que cumpla ciertos 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.

Con respecto a la Teoría de Galois, ha sido mi intención la de llegar al Teorema Principal de la manera más corta y elegante posible. He visto que el exponer demasiado material hace muy tedioso el curso a los alumnos y al profesor, además de que algunos alumnos pierden de vista el objetivo dentro de un mar de definiciones y proposiciones. Creo haber logrado este objetivo mediante un material equilibrado.

Este texto está diseñado para un curso de un semestre sobre Álgebra Moderna en el posgrado de matemática o bien para un curso de dos semestres en la licenciatura de matemática. Consta de cinco capítulos con diversas secciones cada uno. Contienen una serie de problemas que se resuelven con creatividad utilizando el material expuesto, mismos que constituyen una parte

fundamental del mismo. Tienen también como finalidad, la de permitirle al estudiante crear y redactar matemática. En III.5 se incluye la demostración de los Teoremas de Sylow basados en las notas de Guerino Mazzola [M] desarrolladas por Marco Larrea-Schiavon [L]. En la licenciatura de matemática se puede repartir el contenido en dos cursos semestrales, viendo los tres primeros capítulos hasta III.4 en el primero y la sección III.5 junto con los dos últimos capítulos en el segundo semestre.

Este libro es producto del trabajo escrito y revisado a lo largo de varios años del material correspondiente a mi curso sobre la materia que he impartido en la Facultad de Ciencias de la Universidad Nacional Autónoma de México. Después de haber ofrecido por muchos años el curso con excelentes textos, algunos citados en la Bibliografía, y de los cuales he sido inspirado, decidí escribir uno que siga el enfoque de mis libros [L1] y [L2]. Es decir, escogí una presentación moderna donde introduzco el lenguaje de diagramas conmutativos y propiedades universales, tan requerido en la Matemática actual, así como en la Física y en la Ciencia de la Computación, entre otras disciplinas.

Ciudad Universitaria.
Septiembre de 2021.

Introducción

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

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

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

Es muy común la creencia de que un matemático es una persona que se dedica a realizar enormes sumas de números naturales durante todos los

días de su vida. También, la gente supone que un matemático sabe sumar y multiplicar los números naturales muy rápidamente. Si pensamos un poco acerca de este concepto que la mayoría tiene acerca de los matemáticos, podríamos concluir que no se requieren matemáticos ya que una calculadora de bolsillo realiza este trabajo.

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

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

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

Para contar fue necesario representar los números de alguna forma, por ejemplo, los dedos de la mano. Después, el ábaco constituyó un paso todavía ligado a contar con los dedos, el cual todavía se utiliza en algunas partes del planeta. Posteriormente la máquina aritmética de Pascal inventada en 1642 permitía efectuar sumas y restas mediante un sistema muy ingenioso de engranes. En la actualidad, las calculadoras de bolsillo o teléfonos móviles 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 remembranza 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, estas 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 las clases de tonos en la Música) o por un número primo p obteniendo conceptos y resultados importantes) y para la propia Teoría de Grupos (grupo diédrico y simétrico). Al observar esto, lo que realmente se ha hecho en la Teoría de Grupos, es extraer lo esencial de ellos, a saber, dado un conjunto no vacío, definimos una operación binaria en él, tal que cumpla ciertas axiomas, postulados o propiedades, es decir, que posea una estructura, (la estructura de grupo). Existen varios conceptos ligados al de estructura, uno de los más importantes es el de isomorfismo.

El concepto de estructura y de los relacionados con éste, como el de isomorfismo, juegan un papel decisivo en la Matemática actual. Las teorías generales de las estructuras importantes son herramientas muy poderosas. Siempre que alguien pruebe que sus objetos de estudio satisfacen los axiomas de cierta estructura, obtiene, de inmediato, todos los resultados válidos para esa teoría en sus objetos. Ya no tiene que comprobar cada uno de ellos

particularmente. Un uso actual en la Matemática, de las estructuras y los isomorfismos, es el de clasificar las diversas ramas de ella (no es importante la naturaleza de los objetos, pero sí lo es el de sus relaciones).

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

Como es frecuente en la Matemática, los intentos por resolver un problema específico dan lugar a una Teoría Matemática. En este caso, los intentos por encontrar soluciones por radicales de ecuaciones algebraicas dan como resultado varias de las ramas de la Matemática: la Teoría de Grupos, la Teoría de Anillos y la Teoría de Galois entre otras. En [A-L11] y [A-L12] el lector puede encontrar otros ejemplos de esta situación. La Teoría de Galois es una interacción entre grupos, campos y polinomios, entre el Álgebra Lineal y la Teoría de Grupos.

Se sabe de la escuela secundaria cómo encontrar por el método de radicales las soluciones de un polinomio cuadrático, con coeficientes en \mathbb{R} , de la forma $f(t) = at^2 + bt + c$, con $a \neq 0$. Esto lo sabían los antiguos babilonios alrededor del año 1600 A.C. Las raíces están dadas mediante la fórmula $(-b \pm \sqrt{b^2 - 4ac})/2a$. Esta solución está en una tableta de barro que sobrevive hasta la fecha. Este método es válido para cualquier polinomio con coeficientes en un campo de característica diferente de 2 cuyas raíces están en la cerradura algebraica de ese campo. Lo mismo sucede para polinomios de grado 3 y 4 (del Ferro, Tartaglia, Ferrari y Cardano en 1545) sobre los números racionales. Los matemáticos trataron por cientos de años de encontrar una fórmula por radicales para polinomios de grado 5 (Lagrange en 1770

y Ruffini en 1799 probaron que los métodos para grados 3 y 4 fallan para grado 5). Fue Abel en 1824 y 1826 quien probó que esto no puede necesariamente resolverse por radicales. En fin, la solución de ecuaciones polinomiales ha sido un problema matemático por más de 3500 años.

Galois asoció a cada ecuación, un grupo, llamado ahora, de Galois en honor a él. Este grupo consiste de un subconjunto de permutaciones de las soluciones. A partir de las propiedades del grupo de Galois se pueden deducir propiedades de una ecuación, sin hacer mención de ella. Vagamente, la idea principal de la Teoría de Galois es la de considerar las permutaciones de las raíces de un polinomio que tienen la característica de que permutadas siguen satisfaciendo cualquier ecuación algebraica que satisfagan originalmente. Estas permutaciones de las raíces forman un grupo, el grupo de Galois.

El concepto que abarca a los polinomios y a los campos es el de anillo conmutativo. Comenzamos el Capítulo IV estudiando el sistema algebraico de los anillos. La palabra anillo fue introducida por David Hilbert. Alrededor del año 1921, Emmy Noether fundamenta la Teoría de Anillos Conmutativos. También estudiamos dos tipos de anillos importantes, los dominios enteros y los campos. El concepto de campo (o cuerpo) fue considerado por Dedekind en 1871, por Kronecker en 1881, y por ambos alrededor de 1850 en sus clases. Pero fue Weber en 1893 quien proveyó de una definición como la que actualmente usamos. El concepto de ideal fue introducido por Kummer alrededor de 1850 y utilizado como ahora lo conocemos por Dedekind.

En 1881 Leopold Kronecker proveyó una extensión de un campo adjuntado una raíz de un polinomio irreducible. En 1894 Dedekind fue el primer matemático en desarrollar el concepto de automorfismo de campos, lo llamó permutaciones del campo. Fue Emil Artin en 1926 quien desarrolló la relación entre campos y grupos con mucho detalle y enfatizó que la Teoría de Galois no debería tener como meta la de determinar las condiciones de solubilidad de ecuaciones algebraicas sino la de explorar las relaciones entre las extensiones de campos y los grupos de automorfismos y es esta última intención la que se sigue en el presente texto.

Con respecto a la notación para una extensión de campos he preferido denotar con $K' \rightsquigarrow K$ una extensión imitando una torre rotada 90 grados a la derecha, es decir, una torre acostada de campos ya que esto facilita visualizar específicamente los campos y su respectiva inclusión en otros.

Algunos piensan que la Matemática es un juego simple que sola y fríamente interesa al intelecto. Esto sería el olvidar, asienta Poincaré, la sensación de la belleza matemática, de la armonía de los números y las formas, así como de la elegancia geométrica. Esta es ciertamente una sensación de placer estético que todo verdadero matemático ha sentido y por supuesto que pertenece al campo de la emoción sensible. La belleza y la elegancia matemática consisten en 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 por qué el que carece de ella nunca será un verdadero creador, concluye Poincaré.

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

Capítulo I

Estructuras Algebraicas y Propiedades Elementales

I.1 Operaciones Binarias

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

Recordemos algunos conceptos elementales.

Primero, recuerde el conjunto de los números enteros

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

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

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

es una función, mientras que la asociación

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

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 $(x, y) \longmapsto f(x, y)$.

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

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

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

Si la operación binaria f la denotamos simplemente como $+$ (la suma usual en \mathbb{Z}) entonces $(3, 2) \longmapsto +(3, 2) = 3 + 2$ que es igual a 5. Si la

operación binaria f la denotamos como \cdot (la multiplicación usual en \mathbb{Z}), entonces $(3, 2) \mapsto \cdot(3, 2) = 3 \cdot 2$ 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:

⋮	⋮	⋮
-6	-5	-4
-3	-2	-1
0	1	2
3	4	5
6	7	8
9	10	11
⋮	⋮	⋮

[0]	[1]	[2]
-----	-----	-----

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

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

con

$$\begin{aligned} (1, 1) &\mapsto +(1, 1) = 1 + 1 = 2 \\ (0, 1) &\mapsto +(0, 1) = 0 + 1 = 1 \\ (1, 0) &\mapsto +(1, 0) = 1 + 0 = 1 \\ (2, 1) &\mapsto +(2, 1) = 2 + 1 = 0 \end{aligned}$$

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

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:

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

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

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

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

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

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

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

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

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

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

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

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

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 Δ_3 con su operación binaria respectiva, poseen la estructura de grupo. Como se puede ver en el caso de (Δ_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 Δ_3 con la operación binaria definida en el Ejemplo 1.3 es un grupo.

1.5 Sea S_3 el conjunto de las permutaciones de 1, 2, 3. Calcule el número de elementos de S_3 . Defina una operación binaria en S_3 y construya su tabla.

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

1.7 Construya una tabla que represente la suma de todos los elementos de \mathbb{Z}_6 y compárela con las tablas de S_3 y Δ_3 . Observe que las tablas de S_3 y Δ_3 son la misma salvo por el orden y el nombre de los elementos. Compruebe que éstos dos últimos son grupos y establezca una función biyectiva entre sus elementos. Observe que la tabla de \mathbb{Z}_6 le permite comprobar que es un grupo, pero que su tabla es totalmente diferente a las otras dos.

I.2 Estructuras Algebraicas

En esta sección definiremos varias estructuras algebraicas algunas de las cuales ya han sido implícitamente estudiadas. Tiene como finalidad la de **presentar un breve panorama** de algunas de las estructuras algebraicas (no el del estudio propio de la categoría de grupos) y así situar al lector en una mejor posición para comprender los objetos de estudio de la Teoría de Grupos. Supondremos que el lector ya conoce los fundamentos del Álgebra Lineal como en (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 μ nos quedaremos con un conjunto con una operación binaria $+$ que cumple las cuatro axiomas usuales. Entonces diremos que $(V, +)$ es un **grupo conmutativo bajo $+$** . Formalmente, **con esta notación y en este contexto** (en la próxima sección daremos otra versión de la definición de grupo más general) **repetimos**, para ligarla con el estudio de espacios vectoriales, la definición de grupo introducida en la sección anterior:

2.1 Definición. Un **grupo** es una pareja $(G, +)$ donde G es un conjunto no vacío y

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

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 $(\mathbb{Z}, +)$, $(n\mathbb{Z}, +)$, $n \in \mathbb{Z}$, $(\mathbb{Q}, +)$, $(\mathbb{Q}^* = \mathbb{Q} - \{0\}, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R}^* = \mathbb{R} - \{0\}, \cdot)$, $(\mathbb{C}, +)$, $(\mathbb{C}^* = \mathbb{C} - \{0\}, \cdot)$, $(\mathbb{Z}_n, +)$, (Δ_3, \circ) , (S_3, \circ) , (S_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).

Recordemos que podemos denotar la operación binaria en un conjunto con cualquier símbolo, por ejemplo, $+$, $*$, \circ , \diamond , \star , θ , \bullet , Δ , 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 , $o(\Delta_3, \circ) = 6$, $|S_3| = 6$, $o(S_n) = n!$. Si $|G|$ es infinito (finito) diremos que G es infinito (finito). Así, \mathbb{Z} es (constituye un grupo) infinito (bajo la suma usual).

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 $f(u \diamond v) = f(u) \star f(v)$.

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

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

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

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

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

La ley distributiva puede expresarse como

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

i.e.,

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

2.7 Observación. En un grupo G con operadores en Ω , cada elemento de Ω (llamado **operador**) define un endomorfismo (i.e. un homomorfismo de $G \rightarrow G$) 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 Λ es un conjunto, $+$ y \cdot son operaciones binarias tales que

- (i) $(\Lambda, +)$ es un grupo conmutativo
- (ii) (Λ, \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) (Λ, \cdot) es un semigrupo conmutativo, entonces $(\Lambda, +, \cdot)$ se llamará **anillo conmutativo**.

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

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

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

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

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

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

Muchos de los resultados para los espacios vectoriales son válidos para los Λ -módulos, basta tomar $K = \Lambda$ un anillo conmutativo con 1. En particular, relacionamos dos Λ -módulos mediante un **homomorfismo de Λ -módulos**.

Los Λ -módulos son generalizaciones de los conceptos de grupo conmutativo y de espacio vectorial, y son los objetos de estudio del Álgebra Homológica (véase L11). Imitando a los espacios vectoriales, si un Λ -módulo posee una *base*, lo llamaremos **Λ -módulo libre**. No todo Λ -módulo posee base, es decir, no todo Λ -módulo es libre, pero todo espacio vectorial o K -módulo es libre, es decir, sí posee una base. Diremos que un Λ -módulo es **projectivo** si es sumando directo de un libre y que es **finitamente generado** si posee un conjunto finito de generadores.

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

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

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

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

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

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

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

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

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

espacio tensorial de grado k de V . Si definimos una multiplicación

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

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

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 monooides.

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

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

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

I.3 Propiedades Elementales de Grupos

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

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

donde, por abuso o conveniencia de notación se escribe

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

tal que

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

Diremos que el grupo es **conmutativo** o **abeliano** si además satisface

- (iv) $xy = yx$, para toda $x, y \in G$, es decir, si su operación binaria es conmutativa.

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

Podemos ver el concepto de grupo como un caso especial del de grupos con operadores en \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. \blacklozenge

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 $e = e'$. \blacklozenge

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

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

luego, $(xy)^{-1} = y^{-1}x^{-1}$. ♦

Recordemos la definición de homomorfismo de grupos de la sección anterior con la notación siguiente: Sean $(G, +)$ y (G', \cdot) dos grupos. Un **homomorfismo de grupos** es una función $f: G \rightarrow G'$ 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 $im f$, 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 $f : G \rightarrow G'$; si $im f = G'$ diremos que f es un **epimorfismo** y lo denotamos $f : G \twoheadrightarrow G'$ y si f es tal que $\ker f = \{e\}$ e $im f = G'$ entonces diremos que f es un **isomorfismo**. Dicho de otra manera, f es un monomorfismo cuando es inyectiva; es un epimorfismo cuando es suprayectiva y es un isomorfismo cuando es biyectiva (Problema 3.13). Llamaremos **endomorfismo** a un homomorfismo $f : G \rightarrow G$ 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, $im f = \{e'\}$. 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, $x + y \in \cap H_i$, $e \in \cap H_i$, $x^{-1} \in \cap H_i$.♦

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

Ahora, veamos que $f^{-1}(H') = \{x \in G \mid f(x) \in H'\}$ 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 $im f$ es un subgrupo de G' y $ker f$ es un subgrupo de G .

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

Denotemos con $Hom(X, Y)$ el conjunto de homomorfismos del grupo abeliano X en el grupo abeliano Y . Sean $f, g : X \rightarrow Y$ 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 $Hom(X, Y)$ un grupo abeliano, (Problema 3.21).

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

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

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

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

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

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

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

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

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:

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

Problemas

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

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

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

3.4 Pruebe la Proposición 3.15.

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

3.6 Compruebe las afirmaciones del Ejemplo 3.16.

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

3.8 Sea $G = G' = K^n$ donde K es denota un campo. Pruebe que $f: G \rightarrow G'$ 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) $1 \rightarrow Z_2$

(ii) $Z_2 \xrightarrow{\times 2} Z_4$

(iii) $Z_4 \rightarrow Z_2$

(iv) $Z_2 \rightarrow 1$

(v) $Z_2 \rightarrow Z_2 \times Z_2$

(vi) $Z_2 \times Z_2 \rightarrow Z_2$

(vii) $Z_4 \rightarrow Z_2 \times Z_2$

3.12 Denotemos con $Hom(G, G')$ el conjunto de homomorfismos del grupo G en el grupo abeliano G' . Defina $f + g: G \rightarrow G'$ 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) $f(\lambda x, y) = \lambda f(x, y) = f(x, \lambda y)$ para toda $x \in X, y \in Y$ y $\lambda \in \mathbb{Z}$.
- (ii) f nunca es inyectiva a menos que $X = Y = 0$.

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

3.21 Considere $Hom(X, Y)$ el conjunto de homomorfismos del grupo abeliano X en el grupo abeliano Y . Sean $f, g : X \rightarrow Y$ 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

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

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

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

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

dada por $\varphi^*(g) = g \circ \varphi$. Pruebe que φ^* 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 $1_{Y*} : \text{Hom}(X, Y) \longrightarrow \text{Hom}(X, Y)$ es la identidad de $\text{Hom}(X, Y)$, y $(\psi' \circ \psi)_* = \psi'_* \circ \psi_*$.

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

I.4 Grupos Cíclicos

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

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

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

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

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

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

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

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

dada por

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

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

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

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

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

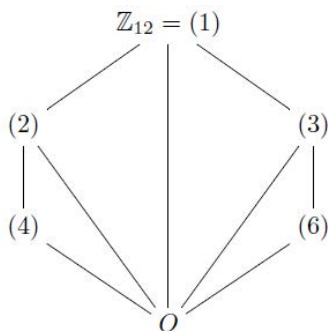
También, si N es un subgrupo no trivial de (x) podemos tomar el menor entero positivo m tal que $x^m \in N$. Como $e = x^n = x^{mq}$, $m \mid n$ y (x) consta de $m = n/q$ elementos. Finalmente, si $o(G) = n$, entonces x^j es un generador de G si, y sólo si $(n, j) = 1$, (Problema 4.7).

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

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

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 II

Grupos Cociente, Teoremas de Isomorfismo y Productos

II.1 Sucesiones Exactas

En esta sección estudiaremos sucesiones finitas e infinitas de homomorfismos

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

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

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

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

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

1.2 Proposición. Una sucesión de grupos

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

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.

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

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

la escribiremos indistintamente como

$$G' \twoheadrightarrow G \twoheadrightarrow G''$$

donde \twoheadrightarrow denota inyectividad y \twoheadrightarrow suprayectividad.

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

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

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

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 $g(x'') = h''(x'')$. Como f es suprayectiva, existe $z \in G$ tal que $f(z) = x''$. Luego,

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

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

$$\begin{array}{ccccccc} e & \longrightarrow & Z_2 & \xrightarrow{\times 2} & Z_4 & \longrightarrow & Z_2 & \longrightarrow & e \\ \parallel & & \parallel & & & & \parallel & & \parallel \\ e & \longrightarrow & Z_2 & \longrightarrow & Z_2 \times Z_2 & \longrightarrow & Z_2 & \longrightarrow & e \end{array}$$

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

Sea $\{C_n\}_{n \in \mathbb{Z}}$ 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:

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

Problemas

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

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

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

II.2 Grupos Cociente

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

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

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

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 . Recuerdese 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

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

y

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

respectivamente.

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

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

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

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

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

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

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

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

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

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

por lo tanto, H es normal.♦

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

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

dada por

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

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

Demostración. Es inmediato comprobar que G/H cumple las axiomas de grupo con $eH = H$ como elemento de identidad y $x^{-1}H$ como inverso de xH . Como $p(xy) = (xy)H = (xH)(yH) = p(x)p(y)$ y p es suprayectiva, entonces es un epimorfismo. Finalmente,

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

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.♦

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

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

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

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

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

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

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

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

Demostración. Supongamos que (x) es de orden n . Si h es un homomorfismo y x genera (x) , como $h(x^r) = [h(x)]^r$ (Problema I.4.1), $h(x)$ genera $im\ h$ pues $e = h(e) = h(x^n) = [h(x)]^n = e$. ♦

2.12 Teorema. (Teorema de Cauchy para Grupos Abelianos Finitos). Sea G un grupo abeliano finito y p un primo tal que $p \mid |G|$. Entonces existe un elemento en G de orden p .

Demostración. La demostración es por inducción sobre el orden de G . Si $|G| = 1$ entonces $G = \{e\}$. Si $|G| = 2$, el único primo que divide a $|G|$ es 2. Si tomamos el elemento a de G que no es el neutro es inmediato notar que $o(a) = 2$.

Sea $|G| = n$, p un primo tal que $p \mid |G|$ y $a \in G$ un elemento distinto del neutro. El orden de a es un entero mayor a 1 divisible por un primo q , digamos $o(a) = qt$ para alguna $t \in \mathbb{N}$. Sea $b = a^t$. Es claro que $o(b) = q$ pues $b^q = a^{qt} = e$. Si $q = p$ entonces b es un elemento de orden p .

Supongamos que $q \neq p$. Sea N el subgrupo cíclico generado por b . N es normal en G , pues G es abeliano. Además $|N| = q$. Entonces $|G/N| = |G|/|N| = n/q$. Sabemos que $q \neq p$ y $p \mid n$, entonces, $p \mid (n/q)$. Además como $n/q < n$ entonces, por hipótesis de inducción G/N tiene un elemento de orden p . Sea cN tal elemento. Observemos que $c^p N = (cN)^p = N$ entonces $c^p \in N$, por lo tanto $c^{pq} = (c^p)^q = e$, pues N es de orden q , lo que implica que $o(c) \mid pq$.

Hay, por lo tanto, cuatro casos: $o(c) = 1$, $o(c) = q$, $o(c) = p$ o $o(c) = pq$. c no puede tener orden 1 pues si así fuera, el orden de cN sería 1 y no p . Tampoco puede tener orden q pues se tendría que $(cN)^q = c^q N = N$ y como cN tiene orden p entonces $p \mid q$ lo cual no puede suceder pues p y q son primos distintos. Por lo tanto quedan solamente dos casos: que $o(c) = p$ o que $o(c) = pq$. En el primer caso c es el elemento buscado de orden p . En el segundo caso el elemento buscado es c^q . ♦

2.13 Corolario. Sea G un grupo abeliano finito y p un primo tal que $p^k \mid |G|$ donde $k \in \mathbb{N}$. Entonces G tiene un subgrupo H de orden p^k .

Demostración. La demostración es por inducción sobre k . Para $k = 1$ el teorema anterior nos proporciona el resultado deseado. Si $p^k \mid |G|$ entonces $p^{k-1} \mid |G|$, y por hipótesis de inducción G tiene un subgrupo H' de orden p^{k-1} .

Como G es abeliano, $H' \triangleleft G$, además $|G/H'| = |G|/|H'| = |G|/p^{k-1}$. Como $p^k || G|$, entonces p divide a $|G/H'|$.

Por el teorema de Cauchy para grupos abelianos, G/H' tiene un subgrupo \overline{H} de orden p . Entonces existe un subgrupo H de G que contiene a H' tal que $\overline{H} = H/H'$. Esto implica que el orden de H es p^k . (Problema 2.13). \blacklozenge

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

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

Problemas

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

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

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

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

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

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

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

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

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

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

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

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

2.13 Proporcione los detalles de la demostración del Corolario 2.13.

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** , $H^n(C)$.

2.16 Sea G un grupo abeliano y $m \in \mathbb{N}$. Demuestre que $o(g) | m$ sí, y sólo si, $g^m = e$ y que $H = \{g \in G | o(g) | m\}$ es un subgrupo de G .

II.3 Teoremas de Isomorfismo

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

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

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

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

3.2 Proposición. Sean $H \triangleleft G$ 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

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

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:

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

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:

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



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 $g^* : G/H \longrightarrow G'$ 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, $xH \in \ker g^*$ sí, y sólo si $g(x) = e$, lo cual sucede si, y sólo si $x \in \ker g$. Así, $\ker g^* = \{xH \mid x \in \ker g\} = \ker g/H$. Claramente $\text{im } g = \text{im } g^*$. 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 isomórfica a $G/\ker g$. Además, nos dice que cualquier epimorfismo $g : G \rightarrow G'$ 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,

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

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

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

Entonces $\text{im } f = \ker g$, 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,

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

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 $g : G \rightarrow G'$ 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

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

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

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

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

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

Generalizaremos el concepto de clase lateral:

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

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

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

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

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

Demostración. Como $N \triangleleft G$, se tiene que $(H \cap N) \triangleleft H$ puesto que si $h \in H$ y $x \in H \cap N$, por un lado, $h x h^{-1} \in H$ pues H es subgrupo de G . Por otro lado, como $N \triangleleft G$ entonces $h N h^{-1} = N$ para toda $h \in H$. Luego, si $x \in N$, $h x h^{-1} \in N$. Como $h x h^{-1} \in H$ y $h x h^{-1} \in N$, $h x h^{-1} \in H \cap N$. Así, $h(H \cap N)h^{-1} \subset H \cap N$ y por lo tanto, $(H \cap N) \triangleleft H$. Definamos

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

Veamos que f está bien definido: supongamos que $x_1 y_1 = x y$, 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 f es un homomorfismo. Como $N \triangleleft G$, $x_1 y_2 = y_2 x_3$. Luego, $f((x_1 y_1)(x_2 y_2)) = f((x_1 x_2)(y_3 y_2)) = x_1 x_2(H \cap N) = x_1(H \cap N)x_2(H \cap N) = f((x_1 y_1)f(x_2 y_2))$.

Como $\ker f = \{xy \in HN \mid x \in H \cap N\} = (H \cap N) = N$ y como $f(xe) = x(H \cap N)$ 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

$$h(xy) = ((xy)N)(H/N) = ((xN)(yN))(H/N) \\ = [(xN)(H/N)][(yN)(H/N)] = h(x)h(y),$$

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

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

◆

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 $In(G)$. Pruebe que es un grupo bajo la composición.

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

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

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

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

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

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

$$e \rightarrow \ker g \rightarrow G \rightarrow G'' \rightarrow \text{co ker } g \rightarrow e$$

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 inyectivo (escribábase como repaso) si, y sólo si, $\ker g = e$ y que es suprayectivo si, y sólo si, $\text{co ker } g = e$.

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

II.4 Productos

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

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

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

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

el cual tiene una estructura de grupo dada por

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

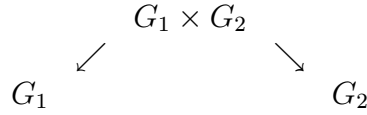
Si utilizamos la notación aditiva, escribiremos $\bigoplus_{i \in I} G_i$ y la llamaremos **suma directa completa**.

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 $h : I \longrightarrow \bigcup_{i \in I} X_i$ 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



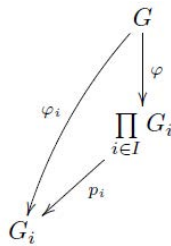
Observe que toda función $h : \{1, 2\} \rightarrow G_1 \cup G_2$ tal que $h(1) \in G_1$ y $h(2) \in G_2$ determina un elemento $(x_1, x_2) = (h(1), h(2)) \in G_1 \times G_2$ y que inversamente, una pareja $(x_1, x_2) \in G_1 \times G_2$ determina una función $h : \{1, 2\} \rightarrow G_1 \cup G_2$ dado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

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

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

$$\begin{aligned}
 g \mapsto h_g : & \quad I \rightarrow \cup G_i \\
 & \quad i \mapsto h_g(i) = \varphi_i(g) \in G_i
 \end{aligned}$$

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

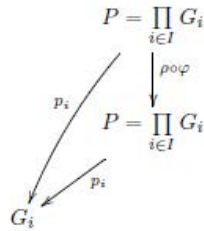
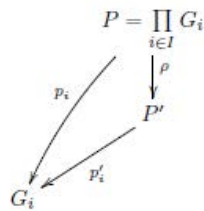
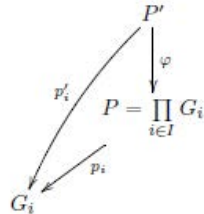


Supongamos que $\varphi' : G \rightarrow \prod_{i \in I} G_i$ es otro homomorfismo tal que $p_i \circ \varphi' = \varphi_i$ para toda $i \in I$. Pero

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

Luego $\varphi = \varphi'$. ♦

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



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

Esta **propiedad universal del producto directo** determina al producto $\prod_{i \in I} G_i$ 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.

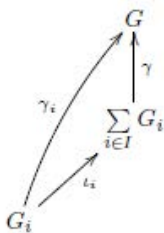
4.2 Teorema. Sea G un grupo abeliano. Consideremos una familia de grupos abelianos aditivos $\{G_i\}$ y una familia de homomorfismos $\{\gamma_i : G_i \rightarrow G\}_{i \in I}$. Entonces existe un homomorfismo único $\gamma : \sum_{i \in I} G_i \rightarrow G$ tal que

$\gamma \circ \iota_i = \gamma_i$ 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

$$\begin{array}{ccc} \gamma : \sum_{i \in I} G_i & \longrightarrow & G \\ 0 & \mapsto & 0 \\ \{g_i\} & \mapsto & \gamma(\{g_i\}) = \gamma_{i_1}(g_{i_1}) + \dots + \gamma_{i_s}(g_{i_s}) = \sum_{j=1}^s \gamma_{i_j}(g_{i_j}) \end{array} \quad \text{mediante}$$

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



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 $\eta : \sum_{i \in I} G_i \rightarrow G$ es tal que $\eta \circ \iota_i = \gamma_i$ para toda $i \in I$ entonces

$$\eta(\{g_i\}) = \eta(\sum \iota_i(g_i)) = \sum \eta \iota_i(g_i) = \sum \eta_{\iota_j}(g_{\iota_j}) = \sum_{j=1}^s \gamma_{i_j}(g_{i_j}) = \gamma(\sum \iota_i(g_i)) = \gamma(\{g_i\}).$$

Luego $\eta = \gamma$ y por lo tanto γ 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 $g = x_1 y_1$

entonces $xy = x_1y_1$. Luego $x^{-1}x_1 = yy_1^{-1}$. Como este elemento está en la intersección de H y N , $x^{-1}x_1 = yy_1^{-1} = e$. Luego $x = x_1$ y $y = y_1$.

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

4.4 Definición. Diremos que un grupo G es un **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. Sea G un grupo abeliano tal que $|G| = mn$ donde $\text{mcd}(m, n) = 1$, $H = \{g \in G \mid o(g) \mid m\}$ y $K = \{g \in G \mid o(g) \mid n\}$. Entonces $G \cong H \times K$, donde $|H| = m$ y $|K| = n$.

Demostración. Veamos que $H \cap K = \{e\}$ y $HK = G$. $H \cap K = \{e\}$ pues, si $g \in H \cap K$ entonces $o(g) \mid m$ y $o(g) \mid n$. Es decir, $1 = \text{mcd}(m, n) \geq o(g) \geq 1$. Por lo tanto $o(g) = 1$ y $g = e$.

$HK = G$ pues claramente $HK \subset G$ y si $g \in G$, como $\text{mcd}(m, n) = 1$, existen $a, b \in \mathbb{Z}$ tales que $1 = am + bn$. Luego $g = g^1 = g^{am+bn} = g^{am}g^{bn}$. Como $(g^{am})^n = (g^{mn})^a = e$ y $(g^{bn})^m = (g^{mn})^b = e$. Esto implica que $g^{am} \in K$ y $g^{bn} \in H$. Por lo tanto $g \in HK$.

Sabemos que $\text{mcd}(m, n) = 1$ y como $|H||K| = |G|$, es posible ver al orden de H como el producto de un divisor de m por uno de n , es decir, $|H| = m'n'$ donde $m' \mid m$ y $n' \mid n$. Sea p un primo (o el número 1) tal que $p \mid n'$, p también divide al orden de H entonces, por el teorema de Cauchy para grupos abelianos, H tiene un elemento de orden p , es decir, existe $x \in H$ tal que $o(x) = p$. Entonces $o(x) \mid n$, pero por definición de H , $o(x) \mid m$. Es decir, $x \in H \cap K = e$.

por lo tanto $p = 1$. Por lo tanto, no existe ningún número primo que divide a n' . Luego $n' = 1$, lo que implica que $|H||m$. Similarmente $|K||n$. Pero $nm = |G| = |H||K|$, entonces $|H| = m$ y $|K| = n$. ♦

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

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

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

el homomorfismo $0 : X_i \rightarrow Y$ es tal que $0 = \varphi \iota_i$. Luego, $\varphi = 0$. Por lo tanto, $\ker \rho = \{0\}$. Veamos que ρ es un epimorfismo: sea $(\varphi_i)_{i \in I} \in \prod_{i \in I} Hom(X_i, Y)$. Entonces tenemos $\varphi_i : X_i \rightarrow Y$ 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 $\iota_j : G_j \rightarrow \prod_{i \in I} G_i$ dado por $\iota_j(g) = \{g_i\}_{i \in I}$ donde

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

es un monomorfismo de grupos llamado **inyección canónica**, que $\iota_i(G_i) \triangleleft \prod_{i \in I} G_i$ 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 $\{G_i\}$, $\prod_{i \in I} G_i = \{(x_1, \dots, x_n) \mid x_i \in G_i\}$ 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 $\mathbb{Z}_i \times \mathbb{Z}_j \cong \mathbb{Z}_{ij}$ sí, y sólo si el máximo común divisor $(i, j) = 1$.

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

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

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 III

Grupos Libres, Producto Tensorial y Teoremas de Sylow

III.1 Grupos Abelianos Finitamente Generados

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

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

Esto quiere decir que G es de la forma

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

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

Esto quiere decir que G es de la forma

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

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

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

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

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

Aunque ya en un curso de Álgebra Lineal (como el de [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 éstos teoremas preferimos posponerlas para un curso posterior de Teoría de Módulos y ver

éstos teoremas como caso especial de los teoremas correspondientes para módulos finitamente generados sobre un anillo de ideales principales y así poder exponer otros temas usualmente excluidos del programa. El lector interesado puede ver la demostración en [B-M, Cap. X] o [H, Cap. II y IV]. Veamos a continuación cómo se utilizan.

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

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

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

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

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

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

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

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

$$\mathbb{Z}_3 \times \mathbb{Z}_6 \times \mathbb{Z}_{30}$$

$$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{60}$$

$$\mathbb{Z}_2 \times \mathbb{Z}_{270}$$

$$\mathbb{Z}_6 \times \mathbb{Z}_{90}$$

$$\mathbb{Z}_3 \times \mathbb{Z}_{180}$$

$$\mathbb{Z}_{540}$$

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.

III.2 Permutaciones y Órbitas

Consideremos el conjunto S_n consistente de todas las permutaciones del conjunto $I_n = \{1, \dots, n\}$, es decir, S_n consiste de todas las funciones biyectivas de I_n en I_n . En I.2 vimos que S_n es un grupo bajo la operación binaria \circ y que $|S_n| = n!$ Recordemos S_3 y su tabla correspondiente como en I.1. Sus elementos son

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

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

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

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

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

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

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

Hemos escrito para $I_n = \{1, \dots, n\}$ 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 σ 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 σ un elemento de S_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 σ . 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 σ 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 σ se puede escribir como producto de ciclos ajenos. ♦

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

2.2 Corolario. Toda permutación $\sigma \in S_n$ 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 S_n -conjunto con la acción $a : S_n \times I_n \longrightarrow I_n$ 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 $a(g, x) = gx = y$ para alguna $g \in G$.

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

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

es un subgrupo de G .

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

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

Observación. Sea $a : G \times X \longrightarrow X$ una acción, es fácil notar que la función dada por $a_g(x) = a(g, x)$ es una biyección para cada $g \in G$.

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** .

Veamos esto último de la siguiente manera: Sea G un grupo y denotemos con ϑ el conjunto de todos los subgrupos de G . Hagamos de ϑ un G -conjunto haciendo actuar a G sobre ϑ por conjugación, es decir, definamos una acción $a : G \times \vartheta \rightarrow \vartheta$ tal que $a(g, H) = g H g^{-1} = \{g h g^{-1} \mid h \in H\}$.

Sea H un subgrupo de un grupo G . Al subgrupo de isotropía de H bajo la acción de conjugación, $G_H = \{g \in G \mid g H g^{-1} = H\}$, lo llamaremos el **normalizador de H en G** y lo denotaremos $N_G[H]$.

Observación. Sea $H < G$. Las siguientes propiedades del normalizador de H en G son inmediatas:

(i) Sea $T < G$ tal que $H \triangleleft T$, entonces, si $t \in T$ se tiene que $t H t^{-1} = H$. Esto implica que $T \subset N_G[H]$.

(ii) Es inmediato notar que $H \triangleleft G$ sí, y sólo si, $N_G[H] = G$. (Problema 2.7).

2.8 Teorema. Sea X un G -conjunto con $a : G \times X \rightarrow X$. 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

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

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

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

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

2.8 suele llamarse **Teorema de la órbita-estabilizador**.

2.9 Corolario. Si $o(G)$ es finito, entonces $o(O_G(x)) = o(G)/o(G_x)$.

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

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

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

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 $r = o(G)n$. ♦

Sea X un G -conjunto finito bajo una acción a . Sea $R = \{x_1, x_2, \dots, x_r\}$ tal que cada elemento x_i esté contenido en una (única) órbita $O_G(x_i)$, (es decir, elegimos un elemento de cada una de las r órbitas de tal forma que no repitamos órbitas procurando pasar por todas ellas). A R lo llamaremos un

sistema de representación de X . Como las órbitas forman una partición de X (pues son clases de equivalencia), tenemos que

$$|X| = \sum_{i=1}^r |O_G(x_i)| = \sum_{i=1}^r |Gx_i| \quad (*)$$

Usando el Teorema de la órbita-estabilizador, podemos escribir la ecuación anterior de la siguiente manera

$$|X| = \sum_{i=1}^r (G : G_{x_i}) \quad (*)$$

donde para cada $x \in R$ tenemos que $(G : G_x)$ es el índice del subgrupo de isotropía de x en G .

Puede que haya órbitas que tengan un solo elemento, es decir, $O_G(x) = \{a(g, x) | g \in G\} = \{x\}$. Sea $X_G = \{x \in X | a(g, x) = x \text{ para toda } g \in G\}$ entonces, X_G es precisamente la unión de todas las órbitas de un solo elemento. Si hay s órbitas de un solo elemento, podemos reescribir la ecuación anterior de la siguiente manera.

$$|X| = |X_G| + \sum_{i=s+1}^r (G : G_{x_i}) \quad (*)$$

Hagamos de G un G -conjunto mediante conjugación, es decir $a : G \times G \rightarrow G$ es tal que $a(g, \gamma) = g\gamma g^{-1}$. Sea $g \in G$. Es inmediato notar que el subgrupo de isotropía de g bajo conjugación es el centralizador de g , es decir,

$$G_g = \{x \in G | gxg^{-1} = x\} = \{x \in G | gx = xg\} = C_G(g).$$

Reescribiendo la ecuación anterior, ahora con la acción de conjugación, obtenemos

$$|G| = |G_G| + \sum_{i=s+1}^r (G : C_G(x_i))$$

Finalmente, notemos que $G_G = \{g' \in G | a(g, g') = gg'g^{-1} = g' \text{ para toda } g \in G\} = \{g' \in G | gg' = g'g \text{ para toda } g \in G\} = Z(G)$. Reemplazando en la ecuación anterior obtenemos la siguiente ecuación

$$|G| = |Z(G)| + \sum_{i=s+1}^r (G : C_G(x_i)) \quad (*)$$

donde $\{x_{s+1}, x_{s+2}, \dots, x_r\}$ es un sistema de representación completo fuera del centro de G . Las ecuaciones anteriores marcadas con $*$ se llaman *ecuaciones de clases*. A la última ecuación la llamaremos **ecuación de clases conjugadas**.

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

$$\begin{aligned} \omega : G &\longrightarrow S_X \\ g &\longmapsto \omega(g) = \sigma_g(x) = gx \end{aligned}$$

es un homomorfismo.

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

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

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

2.12 Corolario. (Cayley) Si G es un grupo entonces existe un monomorfismo $G \longrightarrow S_G$, 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 S_n .

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

$$\begin{aligned} \omega : G &\longrightarrow S_G \text{ dada por} \\ g &\longmapsto \omega(g) = \sigma_g(x) = gx \end{aligned}$$

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, ω es un monomorfismo. Como caso particular, si $o(G) = n$ entonces $S_G = S_n$.

Otra redacción es la siguiente: Propondremos a

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

como candidato a subgrupo de S_G . $\sigma_g : G \longrightarrow G$ es claramente una permutación de G pues si $\sigma_g(x) = \sigma_g(y)$ entonces $gx = gy$ y $x = y$, además, si

$x \in G$ entonces $\sigma_g(g^{-1}x) = gg^{-1}x = x$. Es inmediato comprobar que H es un subgrupo de S_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

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

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. ♦

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 $(h, K) \mapsto hKh^{-1}$. Pruebe que hKh^{-1} es un subgrupo de G isomorfo a K . hKh^{-1} se dice que es un **subgrupo conjugado** de K .

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

2.4 Pruebe que si σ es una permutación de S_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** $\sigma \in S_n$ como

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

Pruebe que si σ' es otra permutación, entonces $sg(\sigma' \circ \sigma) = sg(\sigma')sg(\sigma)$ y que si τ es una transposición, entonces $sg(\tau) = -1$. Diremos que una permutación

es **par** o **impar** si su signo es 1 o -1 respectivamente. Concluya que si $n > 1$, el conjunto de las permutaciones pares de I_n forman un subgrupo A_n de S_n llamado **grupo alternante de grado n**.

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

2.7 (i) Sea $H < G$, $T < G$ tal que $H \triangleleft T$. Pruebe que si $t \in T$, entonces $tHt^{-1} = H$; lo que implica que $T \subset N_G[H]$.

(ii) Pruebe que $H \triangleleft G$ sí, y sólo si, $N_G[H] = G$.

III.3 Grupos Libres

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

$$K \times K \rightarrow K \\ ((x_1, \dots, x_r), (y_1, \dots, y_s)) \mapsto (x_1, \dots, x_r, y_1, \dots, y_s)$$

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

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

Ahora definamos una operación binaria en L con las siguientes condiciones: si alguno de los elementos x ó y es 1 entonces su producto es x ó 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 $f : X \rightarrow L$ es una función tal que, para cualquier función $g : X \rightarrow G$, G un grupo cualquiera, existe un homomorfismo único $h : L \rightarrow G$ tal que el siguiente triángulo es conmutativo:

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

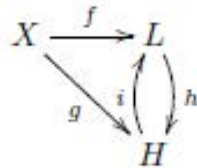
Definamos una función $f : X \rightarrow L$ mediante $f(x) = x^1 \in L$. Supongamos que $g : X \rightarrow G$ es cualquier función de X en un grupo G . Definamos una función $h : L \rightarrow G$ mediante

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

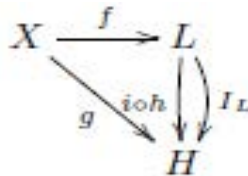
Es fácil comprobar que h es un homomorfismo de grupos tal que $h \circ f = g$. Aún más, si $h' : L \rightarrow G$ es otro homomorfismo de grupos tal que $h' \circ f = g$. Entonces para la palabra $k = x_1^{\eta_1} x_2^{\eta_2} \cdots x_n^{\eta_n}$ tendríamos que $h'(k) = h'(x_1)^{\eta_1} h'(x_2)^{\eta_2} \cdots h'(x_n)^{\eta_n} = g(x_1)^{\eta_1} g(x_2)^{\eta_2} \cdots g(x_n)^{\eta_n}$. 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 $f : X \rightarrow L$ 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 $g : X \rightarrow G$ 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 $g : X \rightarrow H$ con $i \circ g = f$ donde i denota la inclusión de H en L . Como L es libre, existe un homomorfismo $h : L \rightarrow H$ tal que $h \circ f = g$.

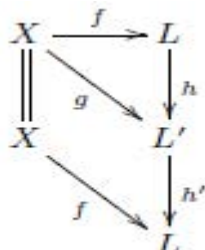


Considere el diagrama

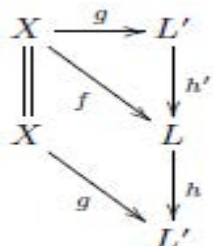


Es claro que $I_L \circ f = f$, y $i \circ h \circ f = i \circ g = f$. Por la unicidad, $i \circ h = I_L$. Luego, i debe ser suprayectiva. Así, $H = L$ y $f(X)$ genera L .

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



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



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 $g : X \rightarrow G$ **se extiende a** un homomorfismo único $h : L \rightarrow G$. 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 $g : X \rightarrow G$ se extiende a un homomorfismo $h : L \rightarrow G$. h es suprayectiva puesto que X genera G y $X = g(X) \subset h(L)$. Si N es el núcleo de h , por el primer teorema del isomorfismo, $G \cong L/N$. Podemos resumir esto en el siguiente

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

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

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

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

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

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

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

3.9 Definición. Un grupo abeliano libre en el conjunto X es una pareja (L, f) donde L es un grupo abeliano y $f : X \rightarrow L$ es una función tal que, para cualquier función $g : X \rightarrow G$, G un grupo abeliano cualquiera, existe un homomorfismo único $h : L \rightarrow G$ 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 ó y es 1 entonces su producto es x ó 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 $\sum_{j \in X} G_j \cong (L, f)$.

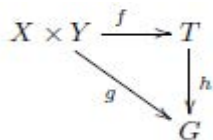
(iv) Concluya que un grupo abeliano es de rango m si, y sólo si, es isomorfo a la suma directa de m grupos cíclicos infinitos.

III.4 Producto Tensorial

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

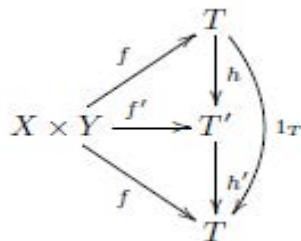
4.1 Definición. Sean X y Y grupos abelianos. El **producto tensorial** de X y Y es la pareja (T, f) , donde T es un grupo abeliano y $f: X \times Y \rightarrow T$ es una función biaditiva, tal que si, G es un grupo abeliano y $g: X \times Y \rightarrow G$ es biaditiva, entonces existe un homomorfismo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

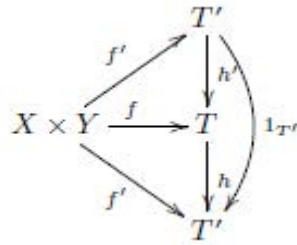
La condición $g = h \circ f$ se puede representar mediante el diagrama



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



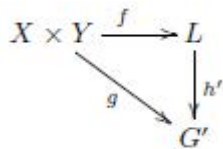


Por ser T un producto tensorial, como $1_T: T \rightarrow T$ es tal que $1_T \circ f = f$ se tiene que también que $h' \circ h \circ f = f$. Luego, por la unicidad, tenemos que $h' \circ h = 1_T$. De manera semejante, por ser T' un producto tensorial, como $1_{T'}: T' \rightarrow T'$ es tal que $1_{T'} \circ f' = f'$ 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 $X \otimes Y$.

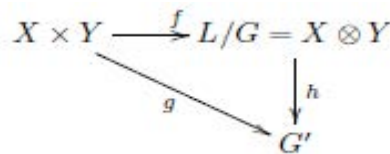
Ahora veamos que, dados dos grupos abelianos, siempre existe su producto tensorial.

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 que $X \otimes Y$ es, efectivamente, un producto tensorial. Sea G' un grupo abeliano cualquiera. Consideremos el triángulo



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:



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

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

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

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 éstas afirmaciones en el siguiente diagrama:

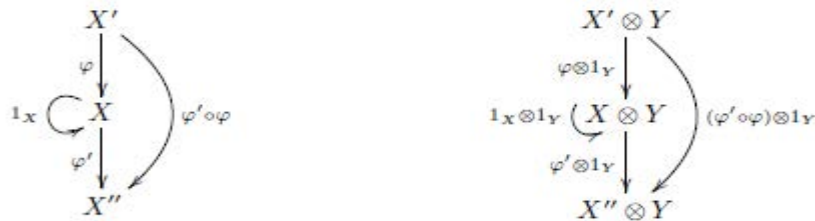


Análogamente tenemos la siguiente

4.4 Proposición. Sean $\varphi: X' \rightarrow X$ y $\varphi': X \rightarrow X''$ homomorfismos de grupos abelianos y Y 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) $(\varphi' \otimes 1_Y) \circ (\varphi \otimes 1_Y) = ((\varphi' \circ \varphi) \otimes 1_Y)$. ♦

Podemos escribir éstas afirmaciones en el siguiente diagrama:



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

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

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

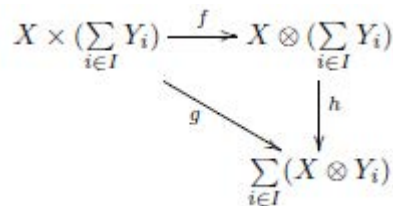
(ii) Sean X y Y grupos abelianos y $X = \sum_{i \in I} X_i$. Entonces

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

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

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

tal que el siguiente diagrama conmuta:



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

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

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 $i \in I$

$$\begin{array}{ccc} & & X \otimes (\sum_{i \in I} Y_i) \\ & \nearrow \varphi_i & \uparrow \varphi \\ X \otimes Y_i & \xrightarrow{1_{X \otimes Y_i}} & \sum_{i \in I} (X \otimes Y_i) \end{array}$$

Es fácil comprobar que $\varphi \circ h = 1_{X \otimes (\sum_{i \in I} Y_i)}$ y que $h \circ \varphi = 1_{\oplus_{i \in I} (X \otimes Y_i)}$. 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 ψ' es un epimorfismo, existe $y_i \in Y$ tal que $\psi'(y_i) = y_i''$ para toda i . Luego,

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

Como

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

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

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).♦

El resultado 4.6 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

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

la cual es equivalente a

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

pero 2_* no es inyectivo.

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

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

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 biaditiva, 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 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.

III.5 Teoremas de Sylow

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. En esta sección, p_i denotará un número primo.

5.1 Teorema. Sea G un grupo abeliano finito tal que $|G| = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$ donde $p_i \neq p_j$ para $i \neq j$ y $n_i > 0$. Entonces

$$G \cong S_{p_1}(G) \times S_{p_2}(G) \times \dots \times S_{p_k}(G)$$

donde $S_{p_i}(G) = \{x \in G \mid o(x) \text{ es una potencia de } p_i\}$ y $|S_{p_i}(G)| = p_i^{n_i}$.

Demostración. La demostración es por inducción sobre el número de primos distintos en los que se factoriza el orden de G . Si $|G| = p_1^{n_1}$, por definición, $S_{p_1}(G) \subset G$. Sea $g \in G$. Sabemos que $o(g) \mid |G| = p_1^{n_1}$ lo que implica que $g \in S_{p_1}(G)$. Luego $G = S_{p_1}(G)$.

Supongamos que $|G| = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$. Es claro que $m = p_1^{n_1} p_2^{n_2} \dots p_{k-1}^{n_{k-1}}$ y $n = p_k^{n_k}$ son primos relativos. Por la Proposición II.4.5, $G \cong H \times S_{p_k}(G)$, donde $H = \{x \in G \mid o(x) \mid m\}$ y $|H| = m$. Por hipótesis de inducción

$$H \cong S_{p_1}(G) \times S_{p_2}(G) \times \dots \times S_{p_{k-1}}(G)$$

y, por lo tanto,

$$G \cong S_{p_1}(G) \times S_{p_2}(G) \times \dots \times S_{p_k}(G). \blacklozenge$$

Observe que, por el teorema anterior, $|S_{p_i}(G)| = p_i^{n_i}$.

5.2 Teorema. Sea $|G| = n$ y p un primo tal que $p^k \mid n$ donde $k \in \mathbb{N}$. Entonces existe un subgrupo H de G tal que $|H| = p^k$.

Demostración. La demostración la haremos por inducción sobre el orden de G . El caso $|G| = 1$ es trivial. Si $|G| = 2$ el único primo que divide a $|G|$ es 2, por lo tanto $H = G$ es el subgrupo de orden $p^1 = 2$.

Sea $Z = Z(G)$ el centro de G . Tenemos dos casos: $p \mid |Z|$ o $p \nmid |Z|$.

Si $p \mid |Z|$, como Z es abeliano, entonces, por el teorema anterior, $|S_p(Z)| = p^t$ para alguna $t \in \mathbb{N}$. Como Z es abeliano y $S_p(Z)$ es un subgrupo de Z , tenemos que $S_p(Z) \triangleleft G$. Observe que $|G/S_p(Z)| = |G|/|S_p(Z)| = |G|/p^t < |G|$.

Hay dos posibilidades: Si $p^k \geq p^t$: entonces como $p^k \mid n$, tenemos que $p^{k-t} \mid |G|/p^t = |G/S_p(Z)|$. Luego, por inducción, $G/S_p(Z)$ tiene un subgrupo H' de orden p^{k-t} . Así que existe $H < G$ tal que $H/S_p(Z) = H'$ lo que implica que $|H| = p^{k-t}p^t = p^k$.

Por otro lado, si $p^k < p^t$. En este caso $p^k \mid |S_p(Z)|$, y por II.2.13, $S_p(Z)$ tiene un subgrupo H de orden p^k . H también es un subgrupo de G .

Para el caso en que $p \nmid |Z|$, la ecuación de clases conjugadas nos dice que $|G| = |Z| + \sum_{r \in R} (G : C_G(r))$ donde R es un sistema de representación completo fuera del centro de G . Como $p \nmid |Z|$, debe de haber un r' tal que $p \nmid (G : C_G(r'))$. Como $p^k \mid |G|$ y $p \nmid (G : C_G(r'))$ entonces es inmediato notar que $p^k \mid |C_G(r')|$. Sabemos también que r' está fuera del centro de G luego $C_G(r') \neq G$. Esto implica que $|C_G(r')| < |G|$. Por lo tanto, por hipótesis de inducción $C_G(r')$ tiene un subgrupo H de orden p^k . ♦

El siguiente corolario es inmediato del teorema anterior.

5.3 Corolario. (Teorema de Cauchy) 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 .

Demostración. Por el teorema anterior G tiene un subgrupo H de orden p . Como p es primo, H es cíclico (II.2.10). Luego existe un elemento h que lo genera. Por lo tanto h es de orden p . ♦

5.4 Definición. Un grupo G se dice que es un **p -grupo** (p un número primo), si todos los elementos de G tienen por orden una potencia de p y diremos que P es un **p -subgrupo de Sylow de G** si P es un p -subgrupo máximo de G , es decir, si K es un p -grupo tal que $P < K < G$ entonces $P = K$.

Es decir, P es un p -subgrupo de Sylow de G si $o(P)$ es la mayor potencia de p que divide a $o(G)$.

5.5 Proposición. Sea G un grupo finito. G es un p -grupo si, y sólo si, $|G| = p^s$ para alguna $s \in \mathbb{N}$.

Demostración. Si G es un p -grupo y q un primo distinto de p tal que $q \mid |G|$, por el Teorema de Cauchy, G tiene un elemento de orden q lo cual contradice que G sea un p -grupo. Por lo tanto $|G| = p^s$. Si $|G| = p^s$ para alguna $s \in \mathbb{N}$, y $g \in G$, entonces, el orden de g divide a $|G| = p^s$. Luego, el orden de g es una potencia de p y por lo tanto G es un p -grupo. \blacklozenge

Observaciones:

- 1) Todo subgrupo de un p -grupo es un p -grupo.
- 2) 5.2 nos asegura que siempre existe al menos un p -subgrupo de Sylow.
- 3) Si G es un grupo abeliano finito tal que $p \mid |G|$ entonces, por 5.1, es inmediato notar que G tiene un único p -subgrupo de Sylow $S_p(G)$.
- 4) Si H y K son p -subgrupos de G con $H \triangleleft G$ o $K \triangleleft G$, entonces, por el Segundo Teorema de Isomorfismo, HK también es un p -subgrupo de G .
- 5) Si G es un p -grupo y $H < G$, entonces $(G : H) = p^k$ con $k \in \{0\} \cup \mathbb{N}$.

5.6 Lema. Sea G un grupo finito, p un primo que divide al orden de G y $S < G$ un p -subgrupo de Sylow de G . Si $H < G$ es un p -subgrupo de G tal que $H \subset N_G[S]$ entonces $H \subset S$.

Demostración. Como $N_G[S]$ contiene tanto a S como a H , podemos trabajar ahí. Sabemos que $S \triangleleft N_G[S]$ y, por las observaciones anteriores, SH es un p -grupo. Luego, como $S \subset SH$ y S es un p -subgrupo de Sylow, tenemos que $S = SH$. Por lo tanto, $H \subset S$. \blacklozenge

5.7 Lema. Sea G un grupo finito de orden $p^k m$ donde p es primo y $p \nmid m$. Sea S un p -subgrupo de Sylow de G . Si T es otro p -subgrupo de Sylow de G entonces, T y S son conjugados, es decir, existe $g \in G$ tal que $gSg^{-1} = T$.

Demostración. Sea Φ el conjunto de todos los subgrupos de G . Hagamos de Φ un G -conjunto por conjugación, es decir, la acción $a : G \times \Phi \rightarrow \Phi$ es tal que $a(g, H) = gHg^{-1}$. Consideremos $H \in \Phi$ y notemos que el subgrupo de isotropía de H es el normalizador de H en G , pues

$$G_H = \{g \in G \mid a(g, H) = H\} = \{g \in G \mid gHg^{-1} = H\} = N_G[H].$$

Por el Teorema 2.8, sabemos que,

$$|O_G(H)| = (G : G_H) = (G : N_G[H]) = |G/N_G[H]| = |G|/|N_G[H]|.$$

Como S es un p -subgrupo de Sylow, entonces $|S| = p^k$ y $S < N_G[S]$. Luego $p^k \mid |N_G[S]|$, es decir $|N_G[S]| = p^k n$ para alguna $n \in \mathbb{N}$. Entonces

$$|O_G(S)| = |G|/|N_G[S]| = p^k m/p^k n = m/n$$

donde m/n no tiene a p como factor, es decir, $p \nmid |O_G(S)|$.

Sea T otro p -subgrupo de Sylow de G . Es fácil ver que la acción $a' : T \times O_G(S) \rightarrow O_G(S)$ dada por $a'(t, H) = tHt^{-1}$ está bien definida y hace de $O_G(S)$ un T -conjunto. Utilizando las ecuaciones de clases de III.2, tenemos que

$$|O_G(S)| = \sum_{W \in \Omega} (T : T_W)$$

donde Ω es un sistema de representación de $O_G(S)$. Como T es un p -subgrupo de Sylow tenemos que $(T : T_W) = p^{s_W}$, para $s_W \in \{0\} \cup \mathbb{N}$. Como por hipótesis, $p \nmid |O_G(S)|$ entonces $p \nmid (T : T_{W'})$ para alguna $W' \in \Omega$. Esto puede suceder solamente cuando $(T : T_{W'}) = p^{s_{W'}} = p^0 = 1$, lo que implica que $T = T_{W'}$.

Sabemos que $W' \in O_G(S)$, entonces $W' = gSg^{-1}$ para alguna $g \in G$, en particular, $|W'| = |gSg^{-1}| = |S| = p^k$. Entonces W' es un p -subgrupo de Sylow de G . Luego $T = T_{W'}$. Así $tW't^{-1} = W'$ para toda $t \in T$. Claramente esto implica que $T \subset N_G[W']$. Por el lema anterior, como W' es un p -subgrupo de Sylow, tenemos que $T \subset W'$. Por lo tanto, como T también es un p -subgrupo de Sylow. Entonces, $T = W' = gSg^{-1}$, es decir, T y S son conjugados. ♦

Obsérvese que, si T es un p -subgrupo de Sylow de G entonces gTg^{-1} es un p -subgrupo de Sylow para toda $g \in G$ pues $|T| = |gTg^{-1}|$. Esta observación junto con el lema anterior son de gran importancia para entender cuáles son los p -subgrupos de Sylow de un grupo pues nos dice que solamente es necesario encontrar uno y todos los demás son conjugados de él. Veamos un ejemplo.

5.8 Ejemplo. Consideremos el grupo simétrico S_n . Dicho grupo consta de las permutaciones de un conjunto C de cardinalidad n . Como el grupo simétrico es independiente del conjunto C (pues la única característica es que tenga n elementos), consideraremos para este ejemplo a S_{p^2} como el conjunto de permutaciones de $Z_p \times Z_p$.

Consideremos los siguientes elementos de S_{p^2} .

$$a(i, j) = (i + 1, j)$$

$$b_k(i, j) = \begin{cases} (i, j + 1) & \text{si } k = i \\ (i, j) & \text{si } k \neq i \end{cases}$$

Es fácil notar que $a, b_0, b_1, \dots, b_{p-1}$ son permutaciones y que son elementos de orden p . También es inmediato notar que los elementos b_0, \dots, b_{p-1} conmutan entre sí. Si se colocan los elementos de $Z_p \times \mathbb{Z}_p$ en una tabla, se puede pensar que a es la permutación cíclica de renglones, mientras que b_k es la permutación cíclica del renglón k . Denotemos con G al subgrupo de S_{p^2} generado por $\{a, b_0, \dots, b_{p-1}\}$ y con $A, B_0, B_1, \dots, B_{p-1}$ los subgrupos cíclicos (de orden p) generados por los elementos a, b_0, \dots, b_{p-1} respectivamente. Sea B el producto $B = B_0 \times B_1 \times \dots \times B_{p-1}$. Como B_k es abeliano para cada k , el grupo B también es abeliano.

Veamos que existe una cierta conmutatividad entre a y b_0, b_1, \dots, b_{p-1} . Sea $(l, m) \in Z_p \times \mathbb{Z}_p$

$$\begin{aligned} ab_i a^{-1}(l, m) &= ab_i(l - 1, m) \\ &= \begin{cases} a(l - 1, m + 1) & \text{si } i = l - 1 \\ a(l - 1, m) & \text{si } i \neq l - 1 \end{cases} \\ &= \begin{cases} (l, m + 1) & \text{si } i + 1 = l \\ (l, m) & \text{si } i + 1 \neq l \end{cases} \\ &= b_{i+1}(l, m) \end{aligned}$$

Llamaremos a lo anterior, la **regla de conmutación**. Esta regla se puede escribir también como $b_i a = ab_{i-1}$. La notación de los índices, al igual que la notación de los exponentes de los elementos a, b_0, \dots, b_{p-1} es módulo p .

Sea $g \in G$, como G está generado por el conjunto $C = \{a, b_0, \dots, b_{p-1}\}$, g se puede escribir como un producto de potencias de elementos de C . Sabemos que los elementos b_0, \dots, b_{p-1} conmutan y además, por la regla de la conmutación, es fácil ver que g se puede escribir de la siguiente forma

$$g = a^r b_0^{r_0} \dots b_{p-1}^{r_{p-1}}$$

Dicha forma además, es única (siempre que los exponentes sean menores que p) pues si

$$a^r b_0^{r_0} \dots b_{p-1}^{r_{p-1}} = a^{r'} b_0^{r'_0} \dots b_{p-1}^{r'_{p-1}}$$

entonces,

$$a^{r-r'} = b_0^{r'_0-r_0} \dots b_{p-1}^{r'_{p-1}-r_{p-1}}$$

Observemos que, por las definiciones de a y de b_k en el producto

$$B_0 B_1 \dots B_{p-1}$$

no hay ningún elemento de A excepto la identidad de S_{p^2} , es decir

$$A \cap B_0 B_1 \dots B_{p-1} = \{e\}.$$

Entonces $a^{r-r'} = b_0^{r'_0-r_0} \dots b_{p-1}^{r'_{p-1}-r_{p-1}} = e$ y en particular $a^{r-r'} = e$.

Si $b_0^{r'_0-r_0} \dots b_{p-1}^{r'_{p-1}-r_{p-1}} = e$ entonces, $b_0^{r'_0-r_0} = b_1^{r'_1-r_1} \dots b_{p-1}^{r'_{p-1}-r_{p-1}}$ y similarmente es fácil notar que $B_0 \cap B_1 B_2 \dots B_{p-1} = \{e\}$ y, por lo tanto, $b_0^{r'_0-r_0} = b_1^{r'_1-r_1} \dots b_{p-1}^{r'_{p-1}-r_{p-1}} = e$, lo cual en particular implica que $b_0^{r'_0-r_0} = e$. Siguiendo este mismo argumento obtenemos que

$$a^{r'-r} = b_0^{r'_0-r_0} = b_1^{r'_1-r_1} = \dots = b_{p-1}^{r'_{p-1}-r_{p-1}} = e$$

Esto puede suceder únicamente si $r \equiv r'$, $r_0 \equiv r'_0, \dots, r_{p-1} \equiv r'_{p-1} \pmod{p}$, pues A, B_0, \dots, B_{p-1} son cíclicos de orden p . Como todos los exponentes son menores que p , esto implica que $r = r'$ y $r_i = r'_i$ para toda i . Por lo tanto, la expresión es única.

De esta forma es fácil contar la cantidad de elementos de G , pues hay p^{p+1} formas distintas de escribir sus elementos, es decir, $|G| = p^{p+1}$. Ahora S_{p^2} tiene $p^2!$ elementos y en su descomposición en primos, $p^2!$ tiene exactamente $p+1$ veces a p (pues $p, 2p, 3p, \dots, p^2$ están en el producto $p^2! = 2 \times 3 \times \dots \times p^2$), es decir $|S_{p^2}| = p^2! = p^{p+1}m$ donde $m \in \mathbb{N}$ y $p \nmid m$. Como $|G| = p^{p+1}$, G es un p -subgrupo de Sylow de S_{p^2} . De esta forma cualquier otro p -subgrupo de Sylow es de la forma $\sigma G \sigma^{-1}$ con $\sigma \in S_{p^2}$.

5.9 Teorema. (Teoremas de Sylow) Sea G un grupo finito de orden $p^k m$ donde p es primo y $p \nmid m$. Entonces

- 1) Los p -subgrupos de Sylow de G son los p -subgrupos S tales que $p \nmid (G : S)$.
- 2) Cualesquiera dos p -subgrupos de Sylow de G son conjugados.
- 3) Sea $\sigma_p = |\{S < G \mid S \text{ es un } p\text{-subgrupos de Sylow}\}|$, entonces $\sigma_p \mid |G|$ y $\sigma_p \equiv 1 \pmod{p}$.

4) Todo p -subgrupo de G está contenido en un p -subgrupo de Sylow de G .

Demostración. 1) Sea S un p -subgrupo de Sylow de G , entonces $|S| = p^k$ y $(G : S) = |G|/|S| = p^k m/p^k = m$. Por lo tanto $p \nmid (G : S) = m$.

2) Por el lema anterior se tiene este resultado.

3) Consideremos la acción por conjugación del lema anterior $a : G \times \Phi \rightarrow \Phi$. Sea S un p -subgrupo de Sylow de G . Como todos los p -subgrupos de Sylow son conjugados se tiene que

$$O_G(S) = \{gSg^{-1} | g \in G\} = \{S < G | S \text{ es un } p\text{-subgrupo de Sylow}\}$$

y por el Teorema 2.8,

$$\sigma_p = |O_G(S)| = (G : G_S) = |G|/|G_S|.$$

Por lo tanto $\sigma_p \mid |G|$.

Sea $T \in O_G(S)$. Consideremos la acción por conjugación restringida a $T \times O_G(S)$ (como en el lema anterior) y seleccionemos un sistema de representación Ω de $O_G(S)$ tal que $T \in \Omega$. Si $W \in O_G(S)$, sabemos que $|O_T(W)| = (T : T_W) = p^{s_W}$ con $s_W \geq 0$.

Veamos que si $T \neq W$, entonces T_W está contenido propiamente en T . Supongamos que $T = T_W$, entonces claramente $T \subset N_G[W]$. Por el Lema 5.7 tenemos que $T \subset W$. Como T es un p -subgrupo de Sylow entonces $T = W$, lo cual es falso. Así, $(T : T_W) = p^{s_W}$ con $s_W > 0$. Claramente $(T : T_T) = 1$.

Finalmente utilizando las ecuaciones de clase de III.2 tenemos que

$$\begin{aligned} \sigma_p &= |O_G(S)| \\ &= (T : T_T) + \sum_{W \in \Omega - \{T\}} (T : T_W) \\ &= 1 + \sum_{W \in \Omega - \{T\}} (T : T_W). \end{aligned}$$

Donde $p \mid (T : T_W)$ para todo $W \in \Omega - \{T\}$. Por lo tanto $\sigma_p \equiv 1 \pmod{p}$.

4) Sea Φ el conjunto de todos los p -subgrupos de Sylow de G y sea Q un p -subgrupo de G . Podemos hacer de Φ un Q -conjunto por conjugación. Por las de ecuaciones de clase de III.2, sabemos que

$$|\Phi| = |\Phi_Q| + \sum_{S \in \Omega} (Q : Q_S)$$

donde Ω es un sistema de representación fuera de Φ_Q . Entonces, si $S \in \Omega$, existe $q' \in Q$ tal que $q'Sq'^{-1} \neq S$ y así $(Q : Q_S) = |O_Q(S)| > 1$, pues la órbita $O_Q(S)$ contiene al menos a S y a $q'Sq'^{-1}$. Entonces $p \mid \sum_{S \in \Omega} (Q : Q_S) = |\Phi| - |\Phi_Q|$, lo que implica que

$$|\Phi| \equiv |\Phi_Q| \pmod{p}$$

Por 3) $|\Phi| \equiv 1 \pmod{p}$, luego $|\Phi_Q| \equiv 1 \pmod{p}$, así $|\Phi_Q| > 0$. Sea $H \in \Phi_Q$, entonces $qHq^{-1} = H$ para toda $q \in Q$. Es decir, $Q < N_G[H]$. Además $H \triangleleft N_G[H]$, luego, QH es un p -grupo. Como $H \subset QH$ y H es un p -subgrupo de Sylow, tenemos que $H = QH$ y por lo tanto $Q \subset QH = H$. ♦

5.10 Proposición. Sea G un grupo de orden $p^k m$ donde p y m son primos relativos. Entonces cada subgrupo de orden p^i de G es normal en un subgrupo de orden p^{i+1} para $1 \leq i < k$.

Demostración. Sea H el subgrupo de G de orden p^i . Hagamos de G/H un H -conjunto mediante la acción $a : H \times G/H \rightarrow G/H$ dada por $a(h, gH) = hgH$. Utilizando las ecuaciones de clase de III.2, tenemos que

$$|G/H| = |(G/H)_H| + \sum_{r \in \Omega} (H : H_r)$$

donde Ω es un sistema de representación completo fuera de $(G/H)_H$. Sabemos que $(H : H_r) = p^{k_r}$ para cada $r \in \Omega$, además $k_r > 0$ pues r no está en $(G/H)_H$ entonces, $p \mid (H : H_r)$ para cada $r \in \Omega$. Como $i < k$, p también divide a $|G/H|$, y como $H \in (G/H)_H$ entonces $|(G/H)_H| \geq 1$. De la ecuación anterior es inmediato que $p \mid |(G/H)_H|$.

Veamos que $(G/H)_H = N_G[H]/H$. Sea $gH \in (G/H)_H$, entonces, $gH = hgH$ para toda $h \in H$. Esto pasa si, y sólo si, $ghg^{-1} \in H$ para toda $h \in H$. Es decir, si, y sólo si, $g \in N_G[H]$. Luego $gH \in N_G[H]/H$. Como consecuencia de esto último, $|(G/H)_H| = (N_G[H] : H)$. Así, $p \mid (N_G[H] : H)$. Como $H \triangleleft N_G[H]$, tenemos que $N_G[H]/H$ es un grupo. Luego $H_G[H]/H$ tiene un subgrupo \overline{K} de orden p . Por el teorema de correspondencia $N_G[H]$ tiene un subgrupo K que contiene a H tal que $\overline{K} = K/H$. Claramente $o(K) = p^{i+1}$. Como $H < \rho^{-1}(K) \leq N_G[H]$ y $H \triangleleft N_G[H]$, es inmediato que $H \triangleleft \rho^{-1}(K)$. ♦

Problemas

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

(ii) Pruebe que $S_{p_i}(G) = \{x \in G \mid o(x) \text{ es una potencia de } p_i\}$ es un subgrupo de G .

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

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

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

5.5 Pruebe que solamente existe un grupo de orden 15.

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

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

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

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

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

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

5.12 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).

Como consecuencia de los problemas anteriores se tiene que los **grupos de orden menor que 16** son:

<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.

Capítulo IV

Teoría de Anillos

IV.1 Anillos

En esta sección definiremos varias estructuras algebraicas que son los objetos de estudio de la Teoría de Anillos. Para un breve panorama de algunas estructuras algebraicas incluyendo las de los anillos véase [L13]. Supondremos que el lector ya conoce los fundamentos de la Teoría de Grupos como en [L13] y utilizaremos la notación que ahí se expone.

1.1 Definición. Un **anillo** es una terna $(\Lambda, +, \cdot)$ donde Λ es un conjunto no vacío, $+$ y \cdot son operaciones binarias tales que

- (i) $(\Lambda, +)$ es un grupo conmutativo
- (ii) (Λ, \cdot) es un semigrupo
- (iii) $u(v + w) = uv + uw$ y $(u + v)w = uw + vw$

La propiedad (iii) se llama **ley distributiva**.

Nótese que se ha suprimido el símbolo \cdot , en uv , como es usual en la notación utilizada en la Teoría de Grupos.

1.2 Ejemplos. 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, (Problema 1.1).

Si un anillo $(\Lambda, +, \cdot)$ satisface

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

Si (Λ, \cdot) es un monoide, diremos que $(\Lambda, +, \cdot)$ es un **anillo con identidad** o **con uno**. Denotaremos con 1 a este único elemento neutro del monoide.

Si consideramos un anillo Λ con multiplicación dada por $(u, v) \mapsto uv$ pero definimos su multiplicación como $(u, v) \mapsto vu$, obtendremos un anillo llamado **opuesto de Λ** , denotado ${}^o\Lambda$, que tiene el mismo elemento cero y uno de Λ . Dicho anillo coincide con Λ solamente cuando Λ es conmutativo.

Si el producto de dos elementos distintos de cero de un anillo Λ es el elemento cero del anillo, entonces esos dos elementos se dice que son **divisores de cero**. Si un anillo conmutativo $(\Delta, +, \cdot)$ 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**.

Observe que un anillo con uno es un anillo con división, sí, y sólo si, los elementos distintos de cero forman un grupo bajo la multiplicación (Problema 1.2). Los cuaternios \mathbb{H} constituyen un ejemplo de anillo (no conmutativo) con división (Problema 1.3).

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

1.3 Ejemplos. \mathbb{Z} es un dominio entero, $2\mathbb{Z}$ es un anillo conmutativo sin elemento de identidad para la multiplicación; \mathbb{Z}_n no es dominio entero para toda n , solamente cuando n es primo. \mathbb{Q} , \mathbb{R} y \mathbb{C} son campos bajo las operaciones binarias usuales en cada uno. Las matrices cuadradas sobre cualquiera de los tres campos mencionados son un anillo no conmutativo con uno. Los enteros módulo n son anillos conmutativos con uno y cuando n es primo, son campos. Los divisores de cero del anillo \mathbb{Z}_n son los elementos distintos de cero que no son primos relativos con n , por lo tanto, \mathbb{Z}_p no posee divisores de cero para p primo.

1.4 Definición. Diremos que un subconjunto Γ de un anillo $(\Lambda, +, \cdot)$ es un **subanillo** de Λ si Γ es, a la vez, un anillo estable o cerrado bajo las operaciones binarias inducidas. Lo denotaremos $\Gamma < \Lambda$. Si el subanillo Γ de un anillo Λ es un dominio entero, entonces diremos que Γ es un **subdominio** de Λ . Si el subanillo Γ de un anillo Λ es un campo, entonces diremos que Γ es un **subcampo** de Λ .

De la definición de subanillo es inmediato el siguiente resultado que proporciona una manera de comprobar si un subconjunto de un anillo es un subanillo de él.

1.5 Proposición. Un subconjunto Γ de un anillo $(\Lambda, +, \cdot)$ es un subanillo de Λ si, y sólo si, Γ es estable o cerrado bajo $+$ y \cdot , i.e., si $x - y \in \Gamma$ y $xy \in \Gamma$ para cualesquiera $x, y \in \Gamma$.

Demostración. Véase el Problema 1.4.♦

1.6 Ejemplos. Para todo entero $n \in \mathbb{Z}$, $n\mathbb{Z} < \mathbb{Z}$. $\mathbb{Z} < \mathbb{R} < \mathbb{C}$. Pero como dominios enteros, \mathbb{Z} es un subdominio de \mathbb{R} y $n\mathbb{Z}$ no es un subdominio de \mathbb{Z} para n distinto de 1 y -1 . \mathbb{Q} es un subcampo de \mathbb{R} , pero \mathbb{Z} no es un subcampo de \mathbb{R} .

Es fácil ver que un subanillo no trivial Γ de un dominio entero Λ es un subdominio de Λ sí, y sólo si, Γ contiene al elemento de identidad de Λ (Problema 1.7). Asimismo, es fácil ver que un subanillo Γ de un campo Λ es un subcampo de Λ sí, y sólo si, para todo elemento $x \in \Gamma$, su inverso $x^{-1} \in \Gamma$ (Problema 1.8).

A continuación, veamos un concepto que hace el papel para la Teoría de Anillos equivalente a la de subgrupo normal para la Teoría de Grupos.

1.7 Definición. Un subanillo I de un anillo Λ se llamará **ideal izquierdo** de Λ si para toda $x \in \Lambda$ y para toda $a \in I$ se tiene que $xa \in I$, es decir, $\Lambda I \subset I$. Un subanillo I de un anillo Λ se llamará **ideal derecho** de Λ si para toda $x \in \Lambda$ y para toda $a \in I$ se tiene que $ax \in I$, es decir, $I\Lambda \subset I$. Un subanillo I de un anillo Λ se llamará **ideal de** Λ si es ideal izquierdo e ideal derecho a la vez.

1.8 Ejemplos. El subanillo $n\mathbb{Z}$ es un ideal de \mathbb{Z} . Los subanillos Λ y 0 son los **ideales triviales** de Λ . Los ideales izquierdos de Λ son los ideales derechos de ${}^o\Lambda$.

Observe que si Λ es un anillo e I un ideal de Λ , la parte aditiva de Λ constituye un grupo abeliano y, por lo tanto, I es un subgrupo normal de Λ . Los ideales de un anillo distintos de los triviales se llamarán **ideales propios no triviales**.

1.9 Proposición. Sea Λ un anillo con división. Entonces Λ solamente posee ideales triviales.

Demostración: Sea I un ideal no trivial cualquiera de Λ . Como I es no trivial, posee un elemento $a \in I$ diferente de cero. Por ser I ideal, $1 = aa^{-1} \in I$. Por lo tanto, $\Lambda = 1\Lambda \subset I\Lambda \subset I$. Luego, $I = \Lambda$. ♦

Observe que debido a esta proposición, un campo no puede poseer ideales propios no triviales.

¿Cómo se relacionan dos anillos? Mediante funciones que preserven la estructura de anillos.

1.10 Definición. Si $(\Lambda, \diamond, \star)$ y $(\Lambda', +, \cdot)$ son anillos, un **homomorfismo de anillos** es una función que es un homomorfismo del grupo conmutativo de Λ en el grupo conmutativo de Λ' y que también es un homomorfismo del semigrupo de Λ en el semigrupo de Λ' , es decir,

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

Usualmente utilizaremos, por abuso, la notación $+$ y \cdot para denotar las (posibles) diferentes operaciones binarias de dos anillos relacionados mediante un homomorfismo, quedando la notación imprecisa, pero usual

$$f(x + y) = f(x) + f(y) \text{ y } f(x \cdot y) = f(x) \cdot f(y).$$

o peor aún,

$$f(x + y) = f(x) + f(y) \text{ y } f(xy) = f(x)f(y).$$

Imitando lo correspondiente para grupos [L13] tenemos la siguiente

1.11 Proposición. La composición de dos homomorfismos de anillos es un homomorfismo de anillos.

Demostración. Sean $f : \Lambda' \rightarrow \Lambda$ y $g : \Lambda \rightarrow \Lambda''$ homomorfismos de anillos. Luego $(g \circ f)(x + y) = g(f(x + y)) = g(f(x) + f(y)) = g(f(x)) + g(f(y)) = (g \circ f)(x) + (g \circ f)(y)$. Análogamente, $(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y)$. Por lo tanto $(g \circ f)$ es un homomorfismo de anillos. ♦

1.12 Definición. Sea $f : \Lambda \rightarrow \Lambda'$ un homomorfismo de anillos. Diremos que f es un **isomorfismo**, y escribiremos $f : \Lambda \xrightarrow{\cong} \Lambda'$ si existe un homomorfismo $g : \Lambda' \rightarrow \Lambda$ tal que $g \circ f = 1_\Lambda$ y $f \circ g = 1_{\Lambda'}$.

Es fácil comprobar (Problema 1.11) que, si g existe está determinada en forma única; lo denotaremos con f^{-1} y se llama **inverso** de f . Diremos que dos anillos Λ y Λ' son **isomorfos** si existe un isomorfismo $f : \Lambda \xrightarrow{\cong} \Lambda'$ y escribiremos $\Lambda \cong \Lambda'$.

1.13 Definición. Sea $f : \Lambda \rightarrow \Lambda'$ un homomorfismo de anillos. El **núcleo** de f , denotado $\ker f$, es el conjunto de todos los elementos $x \in \Lambda$ tales que $f(x) = 0$ donde 0 denota la identidad aditiva de Λ' . La **imagen** de f , denotada $\text{im } f$, es el conjunto de $f(x)$ con $x \in \Lambda$.

Observe que solamente vemos el concepto de núcleo de un homomorfismo de anillos como núcleo de la parte de grupo aditivo de los anillos. Aún cuando los anillos sean con uno, no pediremos que la imagen del uno del anillo del dominio vaya a dar al uno del anillo codominio (Problema 1.12).

Si en la definición de homomorfismo se tiene que $\ker f = \{0\}$, diremos que f es un **monomorfismo** y lo denotamos $f : \Lambda \hookrightarrow \Lambda'$; si $\text{im } f = \Lambda'$, diremos que f es un **epimorfismo** y lo denotamos $f : \Lambda \twoheadrightarrow \Lambda'$ y si f es tal que $\ker f = \{0\}$ e $\text{im } f = \Lambda'$, entonces diremos que f es un **isomorfismo**. De otra manera, f es un monomorfismo cuando es inyectiva; es un epimorfismo cuando es suprayectiva y es un isomorfismo cuando es biyectiva. Llamaremos **endomorfismo** a un homomorfismo $f : \Lambda \rightarrow \Lambda$ y diremos que es **automorfismo** si dicha f es biyectiva.

Observe que, como grupos conmutativos, $2 \cdot _ : \mathbb{Z} \rightarrow 2\mathbb{Z}$ dado por $x \mapsto 2x$ establece un isomorfismo de grupos abelianos pero, como anillos no se tiene un isomorfismo.

Diremos que un homomorfismo $f : \Lambda \rightarrow \Lambda'$ es **trivial** si $f(x) = 0$ para todo $x \in \Lambda$. Es decir, $\text{im } f = \{0\}$. Equivalentemente, $f = 0$ si, y sólo si, $\ker f = \Lambda$.

Recuerde que si A es un subconjunto de B , la función $\iota : A \rightarrow B$ dada por $\iota(a) = a \in B$ para toda $a \in A$ se llama **inclusión** de A en B . La

función identidad de un anillo Λ en sí mismo es un homomorfismo llamado **homomorfismo de identidad**.

1.14 Proposición. Sean $f: \Lambda' \rightarrow \Lambda$, $g: \Lambda \rightarrow \Lambda''$ dos homomorfismos de anillos 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 $h(\Lambda') = \Lambda''$. Luego, $\Lambda'' = h(\Lambda') = g(f(\Lambda')) \subset g(\Lambda) \subset \Lambda''$. Por lo tanto, $g(\Lambda) = \Lambda''$. ♦

Problemas.

1.1 (i) Compruebe que los conjuntos con sus operaciones binarias respectivas en el Ejemplo 1.2 son efectivamente anillos.

(ii) Defina operaciones binarias de suma y producto en nZ y pruebe que nZ es un anillo, n entero positivo.

1.2 Pruebe que un anillo con uno es un anillo con división, sí, y sólo si, los elementos distintos de cero forman un grupo bajo la multiplicación.

1.3 Verifique que los cuaternios \mathbb{H} forman un anillo (no conmutativo) con división.

1.4 Pruebe que un subconjunto Γ de un anillo $(\Lambda, +, \cdot)$ es un subanillo de Λ si, y sólo si, Γ es estable o cerrado bajo $+$ y \cdot .

1.5 Compruebe que si G es un grupo abeliano, entonces el conjunto de endomorfismos $End(G, G)$ con la composición es un anillo.

1.6 Compruebe que los anillos $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ son conmutativos y que $End(G, G)$ del Problema 1.5 no lo es.

1.7 Pruebe que un subanillo no trivial Γ de un dominio entero Λ es un subdominio de Λ sí, y sólo si, Γ contiene al elemento de identidad de Λ .

1.8 Pruebe que un subanillo Γ de un campo Λ es un subcampo de Λ sí, y sólo si, para todo elemento $x \in \Gamma$, su inverso $x^{-1} \in \Gamma$.

1.9 Sea Λ un anillo. Pruebe que el conjunto $I = \{x \in \Lambda \mid nx = 0, n \in \mathbb{Z}\}$ es un ideal de Λ .

1.10 Pruebe que $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ dado por $x \longmapsto r$, donde r es el residuo módulo n es un homomorfismo de anillos.

1.11 En la notación la Definición 1.12 pruebe que, si g existe, está determinada en forma única, el cual es denotado con f^{-1} y se llama inverso de f .

1.12 Proporcione un ejemplo en donde bajo un homomorfismo de anillos, $f : \Lambda \rightarrow \Lambda'$, $f(1_\Lambda) \neq 1_{\Lambda'}$.

1.13 Pruebe que, como anillos, $\mathbb{Z}_i \times \mathbb{Z}_j$ es isomorfo a $\mathbb{Z}_{i \times j}$ cuando el máximo común divisor $(i, j) = 1$.

1.14 Encuentre las raíces de la ecuación $x^2 - 7x + 12$ en \mathbb{Z}_8 .

1.15 Pruebe que los inversos izquierdo y derecho de una unidad en un anillo con uno coinciden.

1.16 Demuestre que los divisores de cero del anillo \mathbb{Z}_n son los elementos distintos de cero que no son primos relativos con n , por lo tanto, \mathbb{Z}_p no posee divisores de cero para p primo.

1.17 Demuestre que si Δ es un dominio entero finito, entonces Δ es campo.

IV.2 Propiedades Elementales y Teoremas de Isomorfismo

Veamos algunas propiedades de los anillos.

2.1 Proposición. Sea Λ un anillo. Entonces

(i) $0x = 0 = x0$ para toda $x \in \Lambda$.

(ii) En un anillo Λ vale la ley de cancelación para todo elemento distinto de cero sí, y sólo si, Λ no posee divisores de cero.

(iii) $(-x)y = x(-y) = -(xy)$, para toda $x, y \in \Lambda$.

(iv) $(-x)(-y) = xy$ para toda $x, y \in \Lambda$.

Demostración. (i) Como $0 = 0 + 0$, $0x = (0 + 0)x = 0x + 0x$. Luego, $0x = 0$. Análogamente, $x0 = 0$.

(ii) Supongamos que en Λ vale la ley de la cancelación para todo elemento distinto de cero. Veamos que Λ no tiene divisores de cero. Tomemos el producto de dos elementos distintos de cero tal que su producto sea cero, es decir, $xy = 0$. Por la parte (i), $x0 = 0$. Luego $xy = x0$. Como $x \neq 0$, entonces $y = 0$. Esto contradice el hecho de que $y \neq 0$.

Ahora, supongamos que Λ no tiene divisores de cero. Supongamos que $xa = ya$ para $a \neq 0$. Luego, por la distributividad, $(x - y)a = xa - ya = 0$. Como $a \neq 0$ y Λ no posee divisores de cero, $x - y = 0$. Así, $x = y$.

(iii) Como $xy + (-x)y = (x + (-x))y = 0y = 0$ luego $(-x)y = -(xy)$ pues el inverso es único. Análogamente $xy + x(-y) = x(y + (-y)) = x0 = 0$, luego $x(-y) = -(xy)$.

(iv) Por (iii) $-(x(-y)) = (-x)(-y)$. También, por (iii), $-(x(-y)) = -(-(-xy))$. Luego, $-(-(-xy)) + (-xy) = 0$. Luego, $-(-(-xy)) = xy$. Así, $(-x)(-y) = xy$ para toda $x, y \in \Lambda$.

Sea $(\Lambda, +, \cdot)$ un anillo con uno. Un elemento $x \in \Lambda$ se llama **inverso izquierdo** de un **elemento invertible por la izquierda** $y \in \Lambda$ si $xy = 1$. Análogamente, un elemento $x \in \Lambda$ se llama **inverso derecho** de un **elemento invertible por la derecha** $z \in \Lambda$ si $zx = 1$. Diremos que $y \in \Lambda$ es **invertible** o **unidad** si es a la vez invertible por la izquierda y la derecha.

Es fácil comprobar que los inversos izquierdo y derecho de una unidad en un anillo con uno coinciden y que el conjunto de unidades es un grupo bajo la multiplicación (Problema 2.6).

Observe que si I es un ideal con uno de un anillo conmutativo con uno Λ , se tiene que $\Lambda I \subset I$, es decir $xI \subset I$ para toda $x \in \Lambda$. Si tomamos $y \in I$ una unidad de Λ , entonces consideremos $x = y^{-1}$. Luego, $y^{-1}y = 1 \in I$. Así, $xI \subset I$, para toda $x \in \Lambda$ y $x1 = x \in \Lambda$. Entonces $I = \Lambda$. Además si Λ es un anillo no necesariamente conmutativo con uno e I un ideal que contiene también al uno de Λ , entonces $I = \Lambda$.

2.2 Proposición. Sea $f : \Lambda \longrightarrow \Lambda'$ un homomorfismo de anillos. Entonces $\ker f$ es un ideal de Λ e $\text{im } f$ es un subanillo de Λ' .

Demostración. Por I.3.20 $\ker f$ e $\text{im } f$ son subgrupos de la parte abeliana aditiva de Λ y Λ' respectivamente y fácilmente se puede ver que son subsemigrupos de la parte multiplicativa de Λ y Λ' respectivamente. Para ver que $\ker f$ es un ideal de Λ , sea $x \in \ker f$ y $a \in \Lambda$. Entonces $f(ax) = f(a)f(x) = f(a)0 = 0$. Por lo tanto, $ax \in \ker f$. Análogamente, $xa \in \ker f$. Luego, $\ker f$ es un ideal. ♦

Una consecuencia inmediata es la siguiente: sea $f : \Lambda \longrightarrow \Lambda'$ un homomorfismo no trivial donde Λ es un campo y Λ' un anillo. Por la proposición anterior, $\ker f$ es un ideal de Λ y por 1.9, como Λ es campo, no posee ideales no triviales, es decir, solamente posee al 0 y a Λ como ideales. Como f no es trivial, $\ker f = 0$ y por lo tanto, f es monomorfismo.

Es inmediato comprobar que todo dominio entero finito es un anillo con división (Problema 2.1) y que todo dominio entero conmutativo finito es un campo (Problema 1.17). Observe que todo dominio entero y anillo con

división poseen al menos los elementos de identidad bajo la suma y multiplicación. Por ejemplo, el dominio entero \mathbb{Z} no es un campo pues todo entero distinto de ± 1 no posee inverso.

De manera semejante a I.3.18 se tiene la siguiente

2.3 Proposición. La intersección de subanillos de un anillo es un subanillo.

Demostración. Véase el Problema 2.5.♦

Imitando la definición de [L12, I.2.17] para espacios vectoriales, tenemos

2.4 Definición. Sea S un subconjunto de un anillo Λ . La intersección de todos los subanillos de Λ que contienen a S se llama **subanillo de Λ generado por S** .

Definiciones semejantes se tienen de **subdominio** o **subcampo generado por un subconjunto S** .

2.5 Definición. Diremos que un anillo Λ es de **característica 0** (denotada $\text{car}(\Lambda) = 0$) si $n = 0$ es el único entero tal que $nx = 0$ para toda $x \in \Lambda$. Si Λ no es de característica 0, el menor entero positivo n tal que $nx = 0$ para toda $x \in \Lambda$ se llama **característica** del anillo Λ (denotada $\text{car}(\Lambda) = n$).

2.6 Ejemplos Los anillos \mathbb{Z} , \mathbb{Q} , \mathbb{R} y \mathbb{C} tienen característica 0. El anillo \mathbb{Z}_n tiene característica n .

2.7 Proposición.

(i) Sea Λ un anillo con 1. La característica de Λ es igual al orden del elemento 1. De no ser así, Λ es de característica 0 si el grupo aditivo de Λ es de orden infinito.

(ii) Si Λ no posee divisores de 0, todos los elementos distintos de cero tienen el mismo orden.

(iii) Si Λ es un anillo no trivial sin divisores de cero tal que $\text{car}(\Lambda) \neq 0$, entonces Λ es de característica igual a un número primo.

Demostración. (i) Sea n el orden del 1, es decir, n veces $1+1+\dots+1 = 0$. Entonces, $nx = n(1x) = (n1)x = 0$ para toda $x \in \Lambda$. Así, Λ es de

característica n . Es claro que Λ es de característica 0 si el 1 es de orden infinito.

(ii) Sean x, y cualesquiera dos elementos distintos de cero del anillo Λ y supongamos que x es de orden n . Luego, $x(ny) = n(xy) = (nx)y = 0y = 0$. Por hipótesis, Λ no posee divisores de cero y como x es distinto de cero, se tiene que $ny = 0$. Como y es arbitrario, cualquier elemento distinto de cero tiene orden n .

(iii) Sea $n = \text{car}(\Lambda)$. Como $\Lambda \neq 0$, podemos escoger un elemento $x \neq 0$. Luego, por (ii), x es de orden n . Veamos que n debe ser un número primo. Supongamos que n se factoriza como producto de dos primos $n = pq$. Entonces, $(px)(qx) = pqxx = nxx = 0$. Como Λ no posee divisores de cero, px ó qx debe ser 0. Como x es de orden n , ó p ó q es n y el que queda es 1. Por lo tanto, n es primo. \blacklozenge

Por la proposición anterior podemos decir que un anillo no trivial Λ sin divisores de cero es de característica 0 sí, y sólo si, todo elemento distinto de cero es de orden infinito. De otra manera, la característica $\text{car}(\Lambda)$ es un número primo y todo elemento distinto del cero es de orden p .

Recordando el concepto de espacio vectorial cociente estudiado en el curso de Álgebra Lineal como en [L12, II.4] o en la Teoría de Grupos II.2 y considerando la parte aditiva, se tenía que, para el caso en que Λ es un grupo conmutativo e I un subgrupo de Λ con $x \in \Lambda$, denotábamos con $x + I$ el conjunto $\{x + y | y \in I\}$. Dichos elementos $x + I$ los llamamos **clases laterales** de I en Λ . Como $0 \in I$ y $x = x + 0 \in x + I$, cada $x \in \Lambda$ pertenece a una clase lateral.

Se comprobó que cualesquiera dos clases laterales o son ajenas o son iguales. Se denotó con Λ/I el conjunto de todas las clases laterales de I en Λ y se le dio a Λ/I una estructura de grupo mediante

$$+: \Lambda/I \times \Lambda/I \rightarrow \Lambda/I$$

dada por

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

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 Λ/I . Llamamos a Λ/I , **grupo cociente** de Λ módulo I .

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

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

Finalmente, se consideró $p: \Lambda \rightarrow \Lambda/I$ dada por $x \mapsto x + I$. Si $x, w \in \Lambda$, entonces

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

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

Todo esto se realizó para espacios vectoriales sobre un campo K . Recuerdese de nuevo que la parte aditiva es un grupo conmutativo. Lo mismo sucede para la parte abeliana aditiva de los anillos. Si Λ es un anillo e I un ideal de Λ , la parte aditiva de Λ constituye un grupo abeliano y, por lo tanto, I es un subgrupo normal de Λ .

Ahora, para Λ un anillo e I un ideal de Λ , definamos en el grupo cociente Λ/I una multiplicación

$$\cdot: \Lambda/I \times \Lambda/I \rightarrow \Lambda/I$$

dada por

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

Si tomamos elementos cualesquiera $x, y \in \Lambda$ y $a, b \in I$ entonces,

$$(x + a)(y + b) = xy + xb + ay + ab \in xy + I$$

por la distributividad e I ser un ideal. Luego

$$(x + I)(y + I) \subset xy + I.$$

Así, la clase lateral $xy + I$ no depende de los elementos x e y y únicamente sí depende de las clases laterales $(x + I)$ y $(y + I)$ lo cual nos dice que la multiplicación anterior está bien definida haciendo por lo tanto de Λ/I un anillo. Llamaremos a Λ/I **anillo cociente de Λ sobre su ideal I** . Si Λ

posee elemento de identidad 1, entonces $1+I$ es la identidad en Λ/I . Observe que si Λ es conmutativo, también Λ/I lo es.

Considere $p: \Lambda \rightarrow \Lambda/I$ dada por $x \mapsto x + I$. Si $x, y \in \Lambda$, entonces

$$p(xy) = (xy) + I = (x + I)(y + I) = p(x)p(y).$$

Luego, p es un epimorfismo de anillos, denotado $p: \Lambda \rightarrow \Lambda/I$, con núcleo $I = \ker p$. Así tenemos una sucesión exacta corta [Ll3, II.1]:

$$0 \longrightarrow I \xrightarrow{i} \Lambda \xrightarrow{p} \Lambda/I \longrightarrow 0.$$

Por lo tanto, hemos visto que un subanillo I de un anillo Λ es un ideal de Λ si, y sólo si, existe un homomorfismo de anillos $f: \Lambda \rightarrow \Lambda'$ con núcleo $\ker f = I$.

Sea $f: \Lambda \rightarrow \Lambda'$ un homomorfismo de anillos con ideales $I \subset \Lambda$ e $I' \subset \Lambda'$ tales que $f(I) \subset I'$, entonces $f^*: \Lambda/I \rightarrow \Lambda'/I'$ dado por $f^*(x+I) = f(x)+I'$ es el homomorfismo inducido por f en los grupos abelianos cociente II.3. Como

$$\begin{aligned} f^*((x+I)(y+I)) &= f^*(xy+I) \\ &= f(xy)+I' \\ &= f(x)f(y)+I' \\ &= (f(x)+I')(f(y)+I') \\ &= f^*(x+I)f^*(y+I) \end{aligned}$$

para toda $x, y \in \Lambda$, el homomorfismo de anillos $f^*: \Lambda/I \rightarrow \Lambda'/I'$ se llama **homomorfismo inducido por f** .

Análogamente a II.3.2, se tiene

2.8 Proposición. Sea $f: \Lambda \rightarrow \Lambda'$ un homomorfismo de anillos con ideales $I \subset \Lambda$ e $I' \subset \Lambda'$ tales que $f(I) \subset I'$. Considérense las proyecciones canónicas a los cocientes correspondientes $p: \Lambda \rightarrow \Lambda/I$ y $p': \Lambda' \rightarrow \Lambda'/I'$. Entonces $f^*: \Lambda/I \rightarrow \Lambda'/I'$ es el homomorfismo inducido por f , el siguiente cuadrado es conmutativo

$$\begin{array}{ccc} \Lambda & \xrightarrow{f} & \Lambda' \\ \downarrow p & & \downarrow p' \\ \Lambda/I & \xrightarrow{f^*} & \Lambda'/I' \end{array}$$

e $\text{im } f^* = p'(\text{im } f)$ y $\ker f^* = p(f^{-1}(I'))$. ♦

Análogamente a II.3.3, se tiene

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

$$\begin{array}{ccc} \Lambda & \xrightarrow{f} & \Lambda' \\ \downarrow p & & \cong \downarrow I_{\Lambda'} \\ \Lambda/\ker f & \xrightarrow{f^*} & \Lambda' \end{array}$$

♦

Análogamente a II.3.4, se tiene

2.10 Teorema. Sea $f : \Lambda \rightarrow \Lambda'$ un homomorfismo de anillos con ideales $I \subset \Lambda$ e $I' \subset \Lambda'$ tales que $f(I) \subset I'$ y como caso particular del teorema anterior, $e = I' \subset \Lambda'$ con $I \subset \ker f$. Entonces existe un homomorfismo único $f^* : \Lambda/I \rightarrow \Lambda'$ dado por $x + I \mapsto f^*(x + I) = f(x) + I' = f(x)$. Además, $\ker f^* = \ker f/I$ e $\text{im } f = \text{im } f^*$. El homomorfismo f^* es un isomorfismo si, y sólo si, f es un epimorfismo e $I = \ker f$. ♦

Análogamente a II.3.5, se tiene

2.11 Corolario. (Primer Teorema de Isomorfismo). Bajo las mismas hipótesis del teorema anterior $\Lambda/\ker f \cong \text{im } f$.

Demostración. Como f es epimorfismo, $\text{im } f = \Lambda'$, luego $\Lambda/\ker f \cong \text{im } f$. ♦

En otras palabras, si $f : \Lambda \rightarrow \Lambda'$ es un epimorfismo de anillos con núcleo $\ker f$, entonces existe un isomorfismo único $f^* : \Lambda/\ker f \cong \Lambda'$, tal que $f = f^* \circ p$, es decir, cualquier homomorfismo de Λ con núcleo $\ker f$ tiene imagen isomórfica a $\Lambda/\ker f$. Aún más, nos dice cuál isomorfismo: aquel tal que $\text{im } f = \text{im } f^*$. Este resultado, $\Lambda/\ker f \cong \text{im } f$ se conoce como el **Primer Teorema de Isomorfismo**. Uno puede "determinar" cuál es el anillo cociente de dos anillos sin necesidad de establecer las clases laterales como veremos en más adelante.

2.12 Ejemplo. Sea I un ideal de un anillo Λ . Consideremos el anillo cociente Λ/I . Sea $\iota: I \rightarrow \Lambda$ el monomorfismo de inclusión y $p: \Lambda \rightarrow \Lambda/I$ el epimorfismo de proyección. Entonces $\text{im } \iota = I = \ker p$ y, por lo tanto,

$$0 \longrightarrow I \xrightarrow{\iota} \Lambda \xrightarrow{p} \Lambda/I \longrightarrow 0$$

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

$$0 \xrightarrow{h} \Lambda' \xrightarrow{f'} \Lambda \xrightarrow{f} \Lambda'' \xrightarrow{k} 0.$$

Recordemos entonces que $\text{im } f' = \ker f$, y f' es monomorfismo, pues $0 = \text{im } h = \ker f$ y, además, f es epimorfismo porque $\text{im } f = \ker k = \Lambda''$. Sea $I = \text{im } f' = \ker f$ el cual es un ideal de Λ , entonces f' establece un isomorfismo $I \xrightarrow{\cong} \Lambda'$ y f establece otro isomorfismo $\Lambda/I \xrightarrow{\cong} \Lambda''$ por el primer teorema de isomorfismo. Por lo tanto, una sucesión exacta corta es una sucesión con un ideal y el anillo cociente de un anillo.

2.13 Ejemplo. $f: \Lambda \rightarrow \Lambda''$ donde $\Lambda = \mathbb{Z}$ y $\Lambda'' = \mathbb{Z}_n$ es un epimorfismo con núcleo el subgrupo $n\mathbb{Z}$, es decir,

$$0 \longrightarrow n\mathbb{Z} \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z}_n \longrightarrow 0$$

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

Análogamente a II.3.11, se tiene

2.14 Teorema. (Segundo Teorema de Isomorfismo). Sean I, J ideales de Λ . Entonces $(I + J)/J \cong I/(I \cap J)$. ♦

Análogamente a II.3.13, se tiene

2.15 Teorema. (Tercer Teorema de Isomorfismo). Sean I, J ideales de Λ con $J \subset I$. Entonces, $\Lambda/I \cong (\Lambda/J)/(I/J)$. ♦

2.16 Teorema.

(i) Si Δ es un dominio entero de característica 0, entonces el subgrupo aditivo de Δ generado por el 1 es isomorfo a \mathbb{Z} .

(ii) Si Δ es un dominio entero de característica $p \neq 2$, p primo, entonces el subgrupo aditivo de Δ generado por el 1 es un subcampo isomorfo a \mathbb{Z}_p .

Demostración. (i) Sea $f : \mathbb{Z} \longrightarrow \Delta$ dada por $n \longrightarrow f(n) = n1$. Como $f(n + n') = (n + n')1 = n1 + n'1 = f(n) + f(n')$ y $f(nn') = (nn')1 = (n1)(n'1) = f(n)f(n')$. Luego f es un homomorfismo. Como Δ es de característica 0, el 1 es de orden infinito. Así que el núcleo de f consiste solamente del 0 y por lo tanto, f es monomorfismo. Claramente, la imagen de \mathbb{Z} bajo f es el subgrupo de Δ .

(ii) Si Δ no es de característica 0 entonces la característica de Δ es un número primo p y el 1 es de orden p . Por lo tanto, el núcleo de f es el ideal $p\mathbb{Z}$. Luego f induce un monomorfismo $f^* : \mathbb{Z}/p\mathbb{Z} \longrightarrow \Delta$. ♦

Problemas

2.1 Compruebe que todo dominio entero finito es un anillo con división.

2.2 Compruebe que el dominio entero \mathbb{Z} no es un campo.

2.3 Compruebe que \mathbb{Z}_n es campo sí, y sólo si, n es un número primo.

2.4 Compruebe que los dominios enteros \mathbb{Q} , \mathbb{R} y \mathbb{C} son campos.

2.5 (i) Pruebe que la intersección de subanillos de un anillo es un subanillo.

(ii) Pruebe lo correspondiente a la parte (i) para subdominios y subcampos.

2.6 Demuestre que los inversos izquierdo y derecho de una unidad en un anillo con uno Λ coinciden y que el conjunto de unidades es un grupo bajo la multiplicación, denotado Λ^* .

2.7 Compruebe que $\Lambda/\{0\} \cong \Lambda$ y que $\Lambda/\Lambda \cong \{0\}$.

2.8 Escriba detalladamente la demostración de 2.8.

2.9 Escriba detalladamente la demostración de 2.9.

2.10 Escriba detalladamente la demostración de 2.10.

2.11 Escriba detalladamente la demostración de 2.14.

2.12 Escriba detalladamente la demostración de 2.15.

IV.3 Polinomios y Campo de Cocientes

En los cursos de Álgebra Superior se estudia el anillo de polinomios. Ahí se definen, se le da una estructura de anillo al conjunto de polinomios, se estudia lo referente a divisibilidad y factorización, etc. En este curso damos por estudiado tales temas y únicamente haremos mención de los resultados que requerimos para nuestro estudio posterior.

A continuación definiremos el anillo de polinomios $\Lambda[t]$ de un anillo Λ .

3.1 Definición. Sea Λ un anillo con uno. Un **anillo de polinomios de Λ** es una terna,

$$(\Pi, f, t)$$

donde Π es un anillo, $f : \Lambda \rightarrow \Pi$ es un monomorfismo con $f(1)$ como identidad de Π , $t \in \Pi$ un elemento que conmuta con $f(x)$ para toda $x \in \Lambda$, tal que (cumple la siguiente *propiedad* llamada *universal*) para todo monomorfismo $g : \Lambda \rightarrow \Lambda'$ con $g(1)$ como identidad de Λ' y todo elemento $y \in \Lambda'$ que conmuta con $g(x)$ para toda $x \in \Lambda$, existe un homomorfismo único $h : \Pi \rightarrow \Lambda'$ tal que $h(t) = y$ y $h \circ f = g$, es decir, el siguiente diagrama conmuta:

$$\begin{array}{ccc} \Lambda & \xrightarrow{f} & \Pi \\ & g \searrow & \downarrow h \\ & & \Lambda' \end{array}$$

3.2 Teorema. Sea (Π, f, t) un anillo de polinomios de Λ . Entonces el conjunto $f(\Lambda) \cup \{t\}$ genera Π . Además, si (Π', f', t') es otro anillo de polinomios de Λ , entonces existe un isomorfismo único $k : \Pi \rightarrow \Pi'$ tal que $k(t) = t'$ y $k \circ f = f'$.

Demostración. La demostración es análoga a las de III.3 y la dejamos como ejercicio para el lector (Problema 3.1).♦

Considérese $\mathbb{Z}^+ \cup \{0\}$ el conjunto de enteros no negativos, Λ un anillo con uno, y sea $\Pi = \{\varphi : \mathbb{Z}^+ \cup \{0\} \rightarrow \Lambda \mid \varphi(n) = 0 \text{ para casi toda } n \in \mathbb{Z}^+ \cup \{0\}\}$. Démosle a Π una estructura de anillo (Problema 3.2 (i)) definiendo dos operaciones binarias

$$\begin{aligned} + & : \Pi \times \Pi \longrightarrow \Pi \\ (\varphi, \xi) & \mapsto (\varphi + \xi)(n) = \varphi(n) + \xi(n) \\ \cdot & : \Pi \times \Pi \longrightarrow \Pi \\ (\varphi, \xi) & \mapsto (\varphi\xi)(n) = \sum_{j=0}^n \varphi(j)\xi(n-j). \end{aligned}$$

Ahora, para cada $x \in \Lambda$, definamos una función que depende de x denotada f_x mediante

$$f_x(n) = x \text{ si } n = 0 \text{ ó } 0 \text{ si } n > 0.$$

Así, $f_x \in \Pi$ y la asignación dada por $x \mapsto f_x$ define una función $f : \Lambda \rightarrow \Pi$. Es fácil comprobar que f es un monomorfismo y que $f(1)$ es la identidad de Π (Problema 3.2 (ii)).

Definamos $t \in \Pi$ dado por $t(n) = 1$ si $n = 1$ o 0 si $n \neq 1$. Claramente t conmuta con f_x para toda $x \in \Lambda$. Veamos que (Π, f, t) es un anillo de polinomios de Λ : sea $g : \Lambda \rightarrow \Lambda'$ un monomorfismo con $g(1)$ como identidad tal que cualquier elemento $y \in \Lambda'$ conmute con $g(x)$ para toda $x \in \Lambda$. Definamos $h : \Pi \rightarrow \Lambda'$ mediante

$$\varphi \mapsto h(\varphi) = g(\varphi(0)) + \sum_{n=1}^{\infty} g(\varphi(n))y^n.$$

Como $\varphi(n) = 0$ para casi toda n , la sumatoria es finita. Es fácil ver que h es homomorfismo, $h(t) = y$, $h \circ f = g$ y que es única (Problema 3.2 (iii)). De aquí que cualquier elemento de Π puede escribirse de manera única como $\varphi = \lambda_n t^n + \dots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0$, donde $\lambda_i \in \Lambda$ y $\lambda_i = \varphi(i)$ para $i = 0, \dots, n$. Así tenemos el siguiente

3.3 Teorema. Para cualquier anillo con uno Λ , existe un anillo de polinomios de Λ . ♦

Identificaremos Λ con su imagen $f(\Lambda)$ dentro de Π . Así, Λ se puede ver como un subanillo de Π bajo la inclusión f . Llamaremos a Π , **anillo de polinomios de Λ** y a t **indeterminada**. Usualmente denotamos a Π como

$\Lambda[t]$ y sus elementos los llamaremos **polinomios en la indeterminada t con coeficientes en el anillo Λ** . Los elementos de Λ los llamaremos **constantes**. Los elementos de Λ se llaman **coeficientes del polinomio φ** , λ_n **coeficiente inicial** y λ_0 **término constante**. El **grado**, $gr(\varphi)$, de un elemento distinto de cero $\varphi \in \Lambda[t]$ es el mayor entero n tal que $\varphi(n) \neq 0$.

Sea Λ un anillo conmutativo. Si $\Lambda[t]$ es un anillo de polinomios del anillo Λ , podemos considerar el anillo de polinomios en la indeterminada t' del anillo de $\Lambda[t]$, es decir, $(\Lambda[t])[t']$, el cual se puede probar que es isomorfo a $(\Lambda[t'])[t]$. Usando esta identificación lo denotaremos simplemente con $\Lambda[t, t']$ y diremos que es el anillo de polinomios en las indeterminadas t y t' con coeficientes en Λ . Generalizando esto podemos definir el anillo de polinomios $\Lambda[t_1, \dots, t_s]$ en las indeterminadas t_1, \dots, t_s con coeficientes en Λ .

Consideremos $\Lambda'[t]$ un anillo de polinomios de un subanillo Λ' de un anillo conmutativo Λ y $a \in \Lambda$. Por la propiedad universal de los anillos de polinomios aplicada como en el siguiente diagrama

$$\begin{array}{ccc} \Lambda' & \xrightarrow{i} & \Lambda'[t] \\ & \searrow \iota & \downarrow E_a \\ & & \Lambda \end{array}$$

existe un homomorfismo

$$E_a : \Lambda'[t] \longrightarrow \Lambda$$

dado por

$$\begin{aligned} \lambda_n t^n + \dots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0 &\longmapsto E_a(\lambda_n t^n + \dots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0) \\ &= \lambda_n a^n + \dots + \lambda_2 a^2 + \lambda_1 a^1 + \lambda_0 \end{aligned}$$

tal que para $b \in \Lambda'$, $E_a(b) = b$ y $E_a(t) = a$ llamado **homomorfismo de evaluación o sustitución**. Resulta que a cada polinomio $f = \lambda_n t^n + \dots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0$ le asociamos el elemento de un anillo $E_a(f) = E_a(\lambda_n t^n + \dots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0) = \lambda_n a^n + \dots + \lambda_2 a^2 + \lambda_1 a^1 + \lambda_0$. Ésto es válido para anillos conmutativos y no necesariamente para no conmutativos. $E_a(f)$ significa evaluar el polinomio f en $t = a$. La asignación $a \mapsto E_a(f)$ determina una función $f^{\textcircled{a}} : \Lambda \longrightarrow \Lambda$ tal que $f^{\textcircled{a}} a = E_a(f)$, es decir: si

$$f = \lambda_n t^n + \dots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0$$

entonces

$$f^{\textcircled{a}} = E_a(f) = \lambda_n a^n + \cdots + \lambda_2 a^2 + \lambda_1 a^1 + \lambda_0.$$

Cualquier función de Λ en Λ que pueda escribirse como una función del tipo $f^{\textcircled{a}}$ se llama **función polinomial**.

Como observamos, cada polinomio $f \in \Lambda'[t]$ determina una función de Λ en Λ . Formalmente, podríamos resumir que la asignación $f \mapsto f^{\textcircled{a}}$ determina un homomorfismo de anillos $\Phi : \Lambda'[t] \rightarrow \Lambda^{\Lambda}$ (Problema 3.16), (el cual no siempre es inyectivo, a menos que Λ' sea dominio entero infinito).

Los elementos de $\Lambda[t]$ los denotaremos con letras como f . El uso tradicional de escribirlos como $f(t)$ sólo indicará que la indeterminada es t . Esta notación tradicional hace aparentar a f como si fuera una función con variable t .

Si Δ es un dominio entero, se estudió en un curso de Álgebra Superior que existe el algoritmo de la división para polinomios sobre Δ . Recordemos que un elemento $a \in \Delta$ es un **cero** o **raíz** del polinomio f si $f^{\textcircled{a}}(a) = 0$.

Recuerde (2.4) que si S es un subconjunto de un anillo Λ , la intersección de todos los subanillos de Λ que contienen a S se llama **subanillo de Λ generado por S** . De manera similar, si S un subconjunto de un anillo Λ , la intersección de todos los ideales de Λ que contienen a S es un ideal de Λ (Problema 3.13) y se llama **ideal de Λ generado por S** denotado $\langle S \rangle$. Los elementos de S se llaman **generadores** del ideal $\langle S \rangle$. Si S consiste de elementos t_1, \dots, t_n denotaremos el ideal $\langle S \rangle$ con $\langle t_1, \dots, t_n \rangle$ y diremos que es **finitamente generado**. Si $\langle S \rangle$ está generado por un solo elemento t diremos que $\langle t \rangle$ es un **ideal principal**. Un dominio entero en el cual todo ideal es principal lo llamaremos **dominio de ideales principales**.

Observe que el ideal $\langle t_1, \dots, t_n \rangle$, al contener los elementos t_1, \dots, t_n implica que debe contener a todos los elementos ("combinaciones lineales") de la forma $\lambda_1 t_1 + \cdots + \lambda_n t_n$ donde $\lambda_i \in \Lambda$. Los elementos t_1, \dots, t_n constituyen una "base" del ideal. Se tiene el siguiente resultado: si K es un campo, el anillo de polinomios $K[t]$ es un dominio de ideales principales. También, \mathbb{Z} es un dominio de ideales principales (Problema 3.10). Observe también que este concepto de generadores difiere del definido en Álgebra Lineal para espacios vectoriales.

Sea Λ un anillo. Diremos que un ideal m es **máximo** si los únicos ideales que lo contienen son m y Λ . Es decir, m es un ideal máximo de Λ , si para cualquier ideal n de Λ tal que $m \subset n \subset \Lambda$ se tiene que $n = m$ o $n = \Lambda$. Diremos que un ideal p es **primo** si para cualesquiera elementos $x, y \in \Lambda$, tales que si $xy \in p$ entonces $x \in p$ ó $y \in p$. Es fácil comprobar que si Λ es un anillo conmutativo con uno entonces Λ/m es un campo si, y sólo si, m es un ideal máximo. Además, p es un ideal primo si, y sólo si Λ/p es dominio entero (Problema 3.12).

Como un ejemplo de lo anterior, considere el caso en que $\Lambda' = \mathbb{Q}$, luego $\Lambda'[t] = \mathbb{Q}[t]$ es el anillo de polinomios de un subanillo $\Lambda' = \mathbb{Q}$ de un anillo $\Lambda = \mathbb{C}$ e $i \in \Lambda = \mathbb{C}$. Por la propiedad universal de los anillos de polinomios aplicada como en el siguiente diagrama

$$\begin{array}{ccc} \Lambda' = \mathbb{Q} & \xrightarrow{f} & \Lambda'[t] = \mathbb{Q}[t] \\ & \searrow i & \downarrow E_i \\ & & \Lambda = \mathbb{C} \end{array}$$

existe un homomorfismo

$$E_i : \Lambda'[t] = \mathbb{Q}[t] \longrightarrow \Lambda = \mathbb{C}$$

dado por

$$\begin{aligned} \lambda_n t^n + \dots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0 &\longmapsto E_i(\lambda_n t^n + \dots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0) \\ &= \lambda_n i^n + \dots + \lambda_2 i^2 + \lambda_1 i^1 + \lambda_0 \end{aligned}$$

tal que para $a \in \Lambda' = \mathbb{Q}$, $E_i(t) = i$ y $E_i(a) = a$. Denotamos $E_i(\mathbb{Q}[t])$ con $\mathbb{Q}[i]$ el cual consta de números complejos de la forma $a + bi$ con $a, b \in \mathbb{Q}$. Sabemos que el núcleo de E_i es el ideal de $\mathbb{Q}[t]$ generado por $t^2 + 1$ y por 2.11 considerando el siguiente diagrama

$$\begin{array}{ccccc} \ker E_i & \hookrightarrow & \mathbb{Q}[t] & \twoheadrightarrow & \mathbb{Q}[t]/\ker E_i \\ & & & \searrow & \downarrow \cong \\ & & & & E_i(\mathbb{Q}[t]) = \mathbb{Q}[i] \end{array}$$

también sabemos que $\mathbb{Q}[t]/\ker E_i \cong E_i(\mathbb{Q}[t]) = \mathbb{Q}[i]$. Como $\ker E_i$ es un ideal máximo, $\mathbb{Q}[i]$ es un subcampo de \mathbb{C} el cual denotaremos $\mathbb{Q}(i)$.

A continuación, veamos que todo dominio entero puede verse contenido en un campo que llamaremos campo de cocientes. Para que la ecuación $mx = n$, con $m, n \in \mathbb{Z}$, tenga solución nos vemos forzados a considerar el campo \mathbb{Q} de números racionales.

3.4 Definición. Sea Δ un dominio entero conmutativo no trivial. Un **campo de cocientes de Δ** es una pareja (K, f) donde K es un campo y $f : \Delta \rightarrow K$ es un monomorfismo de anillos tal que para cualquier monomorfismo $g : \Delta \rightarrow \Delta'$ con Δ' un anillo con división, existe un homomorfismo de anillos único $h : K \rightarrow \Delta'$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} \Delta & \xrightarrow{f} & K \\ & \searrow g & \downarrow h \\ & & \Delta' \end{array}$$

3.5 Teorema. Sea (K, f) un campo de cocientes de Δ . Entonces, $f(\Delta)$ genera a K . Además, si (K', f') es otro campo de cocientes de Δ , entonces existe un isomorfismo único $k : K \rightarrow K'$ tal que $k \circ f = f'$.

Demostración. La demostración es análoga a las de III.3 y la dejamos como ejercicio para el lector (Problema 3.3).♦

Para probar la existencia de un campo de cocientes, imitemos la construcción de los números racionales a partir de los números enteros pero para un dominio entero.

Consideremos el conjunto Δ^* de los elementos distintos de cero de Δ y denotemos con $\Xi = \Delta \times \Delta^*$. Definamos en Ξ una relación mediante $(a_1, b_1) \sim (a_2, b_2)$ sí y sólo si $a_1 b_2 = a_2 b_1$ en Δ . Es fácil verificar que \sim es una relación de equivalencia (Problema 3.4).

Sea $K = \Xi / \sim$ y denotemos con a/b la clase de equivalencia de (a, b) . Definamos la suma y multiplicación de clases como en los números racionales, es decir, $(a_1/b_1) + (a_2/b_2) = (a_1 b_2 + a_2 b_1) / b_1 b_2$ y $(a_1/b_1) \cdot (a_2/b_2) = (a_1 a_2) / (b_1 b_2)$. Es fácil comprobar que estas operaciones están bien definidas y que hacen de K un anillo conmutativo con uno, cuyo elemento cero es la clase de equivalencia de la forma $0/b$ y su uno la clase de la forma a/b con $a = b$. (Problema 3.5).

Como el inverso de un elemento diferente de cero a/b es b/a pues $a \neq 0$, $(a/b) \cdot (b/a) = 1$ luego, K es un campo. Veamos que $(K, f : \Delta \longrightarrow K)$ es un campo de cocientes de Δ . Definamos $f : \Delta \longrightarrow K$ mediante $f(a) = a/1$. Es inmediato comprobar que f es un monomorfismo. Consideremos cualquier monomorfismo $g : \Delta \longrightarrow \Delta'$ con Δ' un anillo con división. Como $g(b) \neq 0$ si $b \neq 0$ en Δ , podemos definir $h' : \Xi \longrightarrow \Delta'$ mediante $h'(a, b) = g(a)/g(b)$. Es fácil comprobar que h' está bien definida (Problema 3.6).

Así, $h'(a, b)$ depende solamente de la clase de equivalencia a/b , por lo tanto podemos definir una función $h : K \longrightarrow \Delta'$. Es fácil comprobar que h es un homomorfismo tal que $h \circ f = g$ (Problema 3.6). Veamos que h es única: sea $k : K \longrightarrow \Delta'$ cualquier otro homomorfismo tal que $k \circ f = g$. Sea $a/b \in K$. Luego $a/b = f(a)f(b)^{-1}$ y por lo tanto $k(a/b) = g(a)g(b)^{-1} = h(a/b)$. Así, $k = h$. Hemos probado el siguiente

3.6 Teorema. Para cualquier dominio entero conmutativo no trivial Δ existe un campo de cocientes. \blacklozenge

3.7 Ejemplos. Si Δ es el dominio entero conmutativo no trivial \mathbb{Z} , entonces su campo de cocientes es \mathbb{Q} . Si consideramos el campo K , el anillo de polinomios $K[t]$ de K es un dominio entero y no un campo. Sin embargo por el teorema 3.6 podemos construir su campo de cocientes $K(t)$, donde cada elemento puede escribirse de la forma f/g donde f y g son polinomios en $K[t]$ con $g \neq 0$. Análogamente, para $K[t_1, \dots, t_s]$ podemos construir $K(t_1, \dots, t_s)$ el cual se llama **campo de cocientes o de funciones racionales con s indeterminadas sobre K** .

3.8 Teorema. Sea K un campo de característica 0. El subcampo de K generado por el uno de K es isomorfo a \mathbb{Q} .

Demostración. Sea $x = m/n \in \mathbb{Q}$ con m un entero y n un entero positivo. Si $x \neq 0$ podemos considerar m y n con solamente ± 1 como divisor común. Si $x = 0$, podemos tomar $m = 0$ y $n = 1$. Así, la expresión para x es única. Definamos $f : \mathbb{Q} \longrightarrow K$ mediante $f(x) = m1/n1$, para toda $x = m/n$. Es fácil ver que f es un homomorfismo (Problema 3.11). Consideremos el ideal $\ker f$ de \mathbb{Q} . Como $f(1) = 1$, $\ker f \neq \mathbb{Q}$. Pero como un anillo con división no puede tener ideales propios no triviales (1.9), $\ker f = 0$. Luego, f es monomorfismo. Como $im f$ es un subcampo de K generado por el 1 hemos terminado. \blacklozenge

Por la proposición anterior y 2.16 (ii) todo campo contiene un subcampo isomorfo a \mathbb{Z}_p para algún primo p o un subcampo isomorfo a \mathbb{Q} . Llamaremos a \mathbb{Z}_p y a \mathbb{Q} **campos primos**. Ellos serán fundamentales para nuestro estudio posterior de campos.

Existe una manera, que no demostraremos, de probar cuando un polinomio

$$f(t) = \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0 \in \mathbb{Q}[t]$$

es irreducible llamado **Criterio de Einsenstein**. Dice que si p es un número primo y $f \in \mathbb{Z}[t]$, entonces f es irreducible sobre \mathbb{Q} si λ_n no es congruente con 0 módulo p , $\lambda_i \not\equiv 0 \pmod{p}$ para $i < n$, y λ_0 no es congruente con 0 módulo p^2 .

Problemas

3.1 Pruebe que si (Π, f, t) es un anillo de polinomios de Λ , entonces el conjunto $f(\Lambda) \cup \{t\}$ genera Π . También, pruebe que si (Π', f', t') es otro anillo de polinomios de Λ , entonces existe un isomorfismo único $k : \Pi \rightarrow \Pi'$ tal que $k(t) = t'$ y $k \circ f = f'$.

3.2 (i) Sea $\mathbb{Z}^+ \cup \{0\}$ el conjunto de enteros no negativos y Λ un anillo con uno. Compruebe que el conjunto $\Pi = \{\varphi : \mathbb{Z}^+ \cup \{0\} \rightarrow \Lambda \mid \varphi(n) = 0 \text{ para casi toda } n \in \mathbb{Z}^+ \cup \{0\}\}$ posee una estructura de anillo definiendo dos operaciones binarias mediante

$$\begin{aligned} n &\mapsto (\varphi + \xi)(n) = \varphi(n) + \xi(n) \\ n &\mapsto (\varphi\xi)(n) = \sum_{j=0}^n \varphi(j)\xi(n-j). \end{aligned}$$

(ii) Sea $f_x \in \Pi$ y considere la asignación dada por $x \mapsto f_x$ la cual define una función $f : \Lambda \rightarrow \Pi$. Compruebe que f es un monomorfismo y que $f(1)$ es la identidad de Π .

(iii) En el Teorema 3.2 compruebe que: h es homomorfismo, $h(t) = y$, $h \circ f = g$ y que h es única. Establezca que cualquier elemento de Π puede escribirse de manera única como $\varphi = \lambda_0 + \lambda_1 t^1 + \lambda_2 t^2 + \cdots + \lambda_n t^n$, donde $\lambda_i \in \Lambda$ y $\lambda_i = \varphi(n)$ para $i = 0, \dots, n$.

3.3 Pruebe que si (K, f) es un campo de cocientes de Δ , entonces, $f(\Delta)$ genera K . También, pruebe que si (K', f') es otro campo de cocientes de Δ , entonces existe un isomorfismo único $k : K \rightarrow K'$ tal que $k \circ f = f'$.

3.4 Considere el conjunto Δ^* de los elementos distintos de cero de Δ y denote con $\Xi = \Delta \times \Delta^*$. Defina en Ξ una relación mediante $(a_1, b_1) \sim (a_2, b_2)$ sí y sólo si $a_1 b_2 = a_2 b_1$ en Δ . Compruebe que \sim es una relación de equivalencia.

3.5 Sea $K = \Xi / \sim$ y denote con a/b la clase de equivalencia de (a, b) . Defina la suma y multiplicación de clases como en los números racionales, es decir, $(a_1/b_1) + (a_2/b_2) = (a_1 b_2 + a_2 b_1) / b_1 b_2$ y $(a_1/b_1) \cdot (a_2/b_2) = (a_1 a_2) / (b_1 b_2)$. Compruebe que estas operaciones están bien definidas y que hacen de K un anillo conmutativo con uno cuyo elemento cero es la clase de equivalencia de la forma $0/b$ y con uno la clase de la forma a/b con $a = b$.

3.6 (i) Defina $h' : \Xi \rightarrow \Delta'$ mediante $h'(a, b) = g(a)/g(b)$. Compruebe que h' está bien definida. **(ii)** Por la parte (i) $h'(a, b)$ depende solamente de la clase de equivalencia a/b , por lo tanto defina una función $h : K \rightarrow \Delta'$. Pruebe que h es un homomorfismo tal que $h \circ f = g$.

3.7 Pruebe que si Δ' es un anillo con división que contiene a un subdominio Δ entonces la función inclusión $\iota : \Delta \rightarrow \Delta'$ se extiende a un monomorfismo único $h : K \rightarrow \Delta'$ donde K es el campo de cocientes.

3.8 Pruebe que el campo de cocientes de un campo cualquiera K es K mismo.

3.9 Pruebe que en un anillo Λ el ideal $\langle 0 \rangle = 0$ donde $\langle 0 \rangle$ denota el ideal generado por el elemento de identidad aditivo 0 . También, pruebe que si Λ tiene uno, entonces $\langle 1 \rangle = \Lambda$.

3.10 Pruebe que (i) \mathbb{Z} es un dominio de ideales principales. (ii) Demuestre que si K es un campo, el anillo de polinomios $K[t]$ es un dominio de ideales principales. (iii) Pruebe que si Δ es un dominio entero finito, entonces $\Delta[t]$ es un dominio entero.

3.11 Pruebe que, en el Teorema 3.8, f es un homomorfismo.

3.12 Sea Λ es un anillo conmutativo con uno. Pruebe que Λ/m es un campo si, y sólo si, m es un ideal máximo y que p es un ideal primo si, y sólo si Λ/p es un dominio entero.

3.13 Pruebe que si S un subconjunto de un anillo Λ , la intersección de todos los ideales de Λ que contienen a S es un ideal de Λ .

3.14 Sea K un campo. Pruebe que un polinomio en $K[t]$ es irreducible si, y sólo si, el ideal generado por él es máximo.

3.15 Considere $\Lambda'[t]$ un anillo de polinomios de un campo Λ' , Λ' un subanillo de un anillo Λ y $a \in \Lambda$. Pruebe que la función

$$E_a : \Lambda'[t] \longrightarrow \Lambda$$

dada por

$$\begin{aligned} \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0 &\longmapsto E_a(\lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0) \\ &= \lambda_n a^n + \cdots + \lambda_2 a^2 + \lambda_1 a^1 + a_0 \end{aligned}$$

es un homomorfismo tal que para $b \in \Lambda'$, $E_a(b) = b$ y $E_a(t) = a$.

3.16 Pruebe que la asignación $f \mapsto f^\circledast$ determina un homomorfismo de anillos $\Phi : \Lambda'[t] \rightarrow \Lambda^\Lambda$.

3.17 Pruebe el algoritmo de la división para polinomios, es decir, pruebe que si $f(t) = \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0$ y $g(t) = \mu_m t^m + \cdots + \mu_2 t^2 + \mu_1 t^1 + \mu_0$ son polinomios en $K[t]$ con $\lambda_n, \mu_m \neq 0$ en K y $m > 0$ entonces existen polinomios únicos $q(t)$ y $r(t)$ en $K[t]$ tal que $f(t) = g(t)q(t) + r(t)$, con $r(t) = 0$ o bien el grado de $r(t)$ menor que el grado de $g(t)$.

3.18 Pruebe que (i) $(t - a)$ es un factor de un polinomio $f(t) \in K[t]$ si, y sólo si, a es una raíz de $f(t)$, $a \in K$.

(ii) Pruebe que cualquier polinomio no trivial de grado m en $K[t]$ tiene a lo más m raíces en K .

3.19 Recuerde que un polinomio es irreducible si no puede expresarse como producto de dos polinomios de menor grado. Pruebe que todo polinomio no trivial en $K[t]$ puede factorizarse en forma única como producto de polinomios irreducibles salvo el orden y constantes de los mismos.

3.20 Para un primo p considere el polinomio

$$\Phi_p(t) = \frac{t^p - 1}{t - 1} = t^{p-1} + t^{p-2} + \cdots + t + 1.$$

Pruebe que es irreducible en $\mathbb{Q}[t]$ y por tanto en $\mathbb{Z}[t]$. Sugerencia: pruebe que $\Phi_p(t)(t-1) \equiv (t-1)^p \pmod{p}$ y que $\Phi_p(t) \equiv (t-1)^{p-1}$ y utilice el Criterio de Eisenstein.

3.21 Los **polinomios ciclotómicos** $\Phi_n(t) \in \mathbb{Z}[t]$, $n \geq 1$ están definidos mediante

$$t^n - 1 = \prod_{d|n} \Phi_d(t).$$

Escriba los polinomios ciclotómicos para $n \leq 20$ y establezca la fórmula recursiva

$$\Phi_n(t) = \frac{t^n - 1}{\prod_{d|n, d < n} \Phi_d(t)}$$

para calcular $\Phi_n(t)$ a partir de $\Phi_i(t)$ para $i < n$. Las raíces del polinomio $t^n - 1$ se llaman **raíces n-ésimas de la unidad**. Los polinomios ciclotómicos aparecen en la Teoría Matemática de la Música, véase [Am] y artículos en [LL-M-N].

Capítulo V

Teoría de Campos y Teoría de Galois

V.1 Extensiones de Campos

Los objetos de estudio de la Teoría de Campos son precisamente éstos, sin embargo dicha teoría se concentra principalmente en el estudio de las extensiones de ellos.

Los campos que usaremos son: el de los números racionales denotado con \mathbb{Q} , el de los números reales denotado con \mathbb{R} , el de los números complejos denotado con \mathbb{C} , el de los enteros módulo un primo p denotado \mathbb{Z}_p . Recuerde también el campo de cocientes de un dominio entero del ejemplo I.3.7 $K(t)$ y $K(t_1, \dots, t_s)$.

Recuerde que todo homomorfismo de campos es inyectivo.

1.1 Definición. Consideremos dos campos K' y K . Diremos que K es una **extensión** de K' si la siguiente sucesión de homomorfismos es exacta:

$$0 \longrightarrow K' \xrightarrow{\iota} K$$

es decir, ι es un monomorfismo e identificamos K' con $\iota(K')$ dentro de K cuando esto sea posible. Decimos que K' es el **campo base** de la extensión. Vemos entonces a $K' \cong \iota(K')$ como un subcampo de K . Denotamos la **extensión K de K'** o **extensión de K' en K** con $K' \mapsto K$ o bien $K' \leq K$, o bien $K : K'$, o bien $K' < K$ cuando $K' \neq K$, o también K/K' , o

$$\begin{array}{c} K \\ | \\ K' \end{array}$$

También escribiremos simplemente **extensión** por abuso cuando esté implícito el contexto correspondiente.

1.2 Ejemplos.

$$\begin{array}{l} 0 \longrightarrow \mathbb{Q} \longrightarrow \mathbb{R} \\ 0 \longrightarrow \mathbb{R} \longrightarrow \mathbb{C} \\ 0 \longrightarrow \mathbb{Q} \longrightarrow \mathbb{C} \end{array}$$

son extensiones. Con las demás notaciones se verían así:

$$\begin{array}{l} \mathbb{Q} \mapsto \mathbb{R} \\ \mathbb{R} \mapsto \mathbb{C} \\ \mathbb{Q} \mapsto \mathbb{C} \end{array}$$

$$\begin{array}{l} \mathbb{R} : \mathbb{Q} \\ \mathbb{C} : \mathbb{R} \\ \mathbb{C} : \mathbb{Q} \end{array}$$

$$\begin{array}{l} \mathbb{R}/\mathbb{Q} \\ \mathbb{C}/\mathbb{R} \\ \mathbb{C}/\mathbb{Q} \end{array}$$

$$\begin{array}{c} \mathbb{R} \\ | \\ \mathbb{Q} \end{array}$$



Este tipo de "torres de campos" son uno de los principales temas de estudio de la Teoría de Campos. Preferiremos la notación $K' \rightsquigarrow K$ para denotar una extensión imitando una torre rotada 90 grados a la derecha, es decir, una torre o "condominio horizontal" de campos ya que esto facilita visualizar específicamente los campos y su respectiva inclusión en otros.

1.3 Definiciones. (i) Si $K' \rightsquigarrow K$ y $K \rightsquigarrow K''$ son extensiones, diremos que $K' \rightsquigarrow K$ es una **subextensión de** $K' \rightsquigarrow K''$ y se acostumbra escribir $(K' \rightsquigarrow K) \leq (K' \rightsquigarrow K'')$.

(ii) Diremos que dos extensiones

$$K' \rightsquigarrow K$$

y

$$L' \rightsquigarrow L$$

son **isomorfos** si existen homomorfismos de campos $\alpha : K' \longrightarrow L'$ y $\beta : K \longrightarrow L$ tal que el siguiente diagrama conmuta

$$\begin{array}{ccc} K' & \rightsquigarrow & K \\ \downarrow \alpha & & \downarrow \beta \\ L' & \rightsquigarrow & L \end{array}$$

Podemos identificar $K' \cong \iota(K')$, $L' \cong \iota'(L')$ y $\beta|_{K'} = \alpha$.

Ahora introduciremos el Álgebra Lineal en el estudio de las extensiones de campos. Considere una extensión $K' \rightsquigarrow K$. Como K' puede verse dentro de K , podemos considerar el espacio vectorial K sobre K' , denotar $\dim_{K'} K$ como $[K' \rightsquigarrow K]$ y llamarla **grado de K sobre K'** , el cual puede ser infinito.

Si el grado de K sobre K' es finito (infinito), entonces diremos que la extensión $K' \rightarrow K$ es **finita (infinita)**. El grado de una extensión es el invariante más importante de una extensión.

1.4 Teorema. Si $K' \rightarrow K$ y $K \rightarrow K''$ son extensiones finitas entonces $K' \rightarrow K''$ es una extensión finita y

$$[K' \rightarrow K][K \rightarrow K''] = [K' \rightarrow K''].$$

Demostración. Consideremos $\{u_i\}_{i=1}^n$ y $\{v_j\}_{j=1}^m$ bases para las extensiones $K' \rightarrow K$ y $K \rightarrow K''$, es decir para K como espacio vectorial sobre K' y para K'' como espacio vectorial sobre K . Veamos que los nm elementos $\{u_i v_j\}$ forman una base para $0 \rightarrow K' \rightarrow K''$, es decir, una base para K'' sobre K' .

Sea w cualquier elemento de K'' . Entonces $w = \sum_{j=1}^m \mu_j v_j$ con $\mu_j \in K$. Pero como $\mu_j \in K$ y K es un espacio sobre K' , $\mu_j = \sum_{i=1}^n \lambda_{ij} u_i$ con $\lambda_{ij} \in K'$. Sustituyendo, $w = \sum_{j=1}^m (\sum_{i=1}^n \lambda_{ij} u_i) v_j = \sum_{i,j} \lambda_{ij} (u_i v_j)$. Luego, los elementos $u_i v_j$ generan el espacio K'' sobre K' .

Consideremos una combinación lineal $\sum_{i,j} \eta_{ij} (u_i v_j) = 0$ con $\eta_{ij} \in K'$. Entonces, $\sum_{j=1}^m (\sum_{i=1}^n \eta_{ij} u_i) v_j = 0$ con $\sum_{i=1}^n \eta_{ij} u_i \in K$. Como $\{v_j\}_{j=1}^m$ es base del espacio K'' sobre K , $\sum_{i=1}^n \eta_{ij} u_i = 0$ para toda j . Como a la vez, $\{u_i\}_{i=1}^n$ es una base para K sobre K' , $\sum_{i=1}^n \eta_{ij} u_i = 0$ implica que $\eta_{ij} = 0$ para toda i, j . Luego, los elementos $\{u_i v_j\}$ son linealmente independientes. Así, $\{u_i v_j\}$ es una base para K'' sobre K' . ♦

En esta situación, decimos que K es un **campo intermedio de K' y K''** . Nótese que si $K' \rightarrow K''$ es una extensión infinita, también lo serán $K' \rightarrow K$ y $K \rightarrow K''$. También observe que si $K' \rightarrow K''$ es una extensión finita, como corolario se tiene que la dimensión de K sobre K' o la de K'' sobre K divide a la dimensión de K'' sobre K' , es decir $[K' \rightarrow K] \mid [K' \rightarrow K'']$ o $[K \rightarrow K''] \mid [K \rightarrow K']$. Dicho de otra manera, el grado de K sobre K' divide al grado de K'' sobre K' o bien que el grado de K'' sobre K divide al grado de K'' sobre K' .

1.5 Corolario. Consideremos una familia de campos $\{K_i\}$ para $i = 1, \dots, s$ tal que cada K_{i+1} es una extensión finita de K_i . Entonces K_s es una extensión finita de K_1 y

$$[K_1 \rightarrow K_2][K_2 \rightarrow K_3] \cdots [K_{s-1} \rightarrow K_s] = [K_1 \rightarrow K_s].$$

Demostración. Problema 1.1.♦

1.6 Ejemplos. Considere la extensión $\mathbb{R} \rightarrow \mathbb{C}$ donde $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$. Entonces 1 e i generan a \mathbb{C} como espacio vectorial sobre \mathbb{R} . Como $i \notin \mathbb{R}$, $\{1, i\}$ es linealmente independiente sobre \mathbb{C} . Luego, $\{1, i\}$ es una base para \mathbb{C} sobre \mathbb{R} y por lo tanto $\dim_{\mathbb{R}} \mathbb{C} = [\mathbb{R} \rightarrow \mathbb{C}] = 2$. Sea $\mathbb{R}(i)$ el subcampo que contiene a los elementos de la forma $x + iy$, con $x, y \in \mathbb{R}$. Luego, $\mathbb{C} = \mathbb{R}(i)$, (Problema 1.2).

1.7 Ejemplo. Sea $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Al definir así $\mathbb{Q}(\sqrt{2})$, cualquier elemento es de la forma $a + b\sqrt{2}$ y por lo tanto $\{1, \sqrt{2}\}$ genera el espacio vectorial $\mathbb{Q}(\sqrt{2})$ sobre \mathbb{Q} . Veamos que es linealmente independiente: supongamos que es linealmente dependiente, es decir, que existe una combinación lineal de ellos $c + d\sqrt{2} = 0$ con $c, d \in \mathbb{Q}$ no ambos cero. Si $d = 0$, entonces $c = 0$ lo cual implica que ambos c, d serían cero contra lo supuesto. También, si $c = 0$, entonces $d\sqrt{2} = 0$ lo cual implica que ambos c, d sean cero contra lo supuesto. La única posibilidad es que ambos c y d sean distintos de cero y por lo tanto se tendría que $d\sqrt{2} = -c$ y así $\sqrt{2} = -\frac{c}{d} \in \mathbb{Q}$ lo cual es imposible. Por lo tanto $\{1, \sqrt{2}\}$ es linealmente independiente y constituye una base para el espacio vectorial $\mathbb{Q}(\sqrt{2})$ sobre \mathbb{Q} . Luego $[\mathbb{Q} \rightarrow \mathbb{Q}(\sqrt{2})] = 2$.

Recordemos de (I.3) el homomorfismo de evaluación o sustitución adaptado a campos: consideremos $K'[t]$ el anillo de polinomios de un subcampo K' de un campo K'' y $a \in K''$. El homomorfismo

$$E_a : K'[t] \longrightarrow K''$$

dado por

$$\begin{aligned} \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0 &\longmapsto E_a(\lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0) \\ &= \lambda_n a^n + \cdots + \lambda_2 a^2 + \lambda_1 a^1 + \lambda_0 \end{aligned}$$

tal que para $b \in K'$, $E_a(b) = b$ y $E_a(t) = a$ se llama **homomorfismo de evaluación o sustitución**. Es decir, a cada polinomio $f = \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0$ le asociamos el elemento del campo $E_a(f) = E_a(\lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0) = \lambda_n a^n + \cdots + \lambda_2 a^2 + \lambda_1 a^1 + \lambda_0$. $E_a(f)$ significa evaluar el polinomio f en $t = a$. La asignación $a \mapsto E_a(f)$ determina una función $f^\circledast : K'' \longrightarrow K''$ tal que $f^\circledast a = E_a(f)$, es decir: si

$$f = \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0$$

entonces

$$f^{\circledast}a = E_a(f) = \lambda_n a^n + \cdots + \lambda_2 a^2 + \lambda_1 a^1 + \lambda_0.$$

Cualquier función de K'' en K'' que pueda escribirse como una función del tipo f^{\circledast} se llama **función polinomial**.

Como observamos, cada polinomio $f \in K'[t]$ determina una función de K'' en K'' . Formalmente, decimos que la asignación $f \mapsto f^{\circledast}$ determina un homomorfismo de anillos $\Phi : K'[t] \rightarrow K''^{K''}$, (el cual no siempre es inyectivo, a menos que K' sea dominio entero infinito). Los elementos de $K'[t]$ los denotaremos con letras como f, g, h . El uso tradicional de escribirlos como $f(t)$ sólo indicará que la indeterminada es t . Esta notación tradicional hace aparentar a f como si fuera una función con variable t y no debe causar confusión alguna. Como $K'[t]$ es un dominio entero, existe un algoritmo de la división para polinomios sobre K' (Problema I.3.17).

Nos interesa considerar campos que estén entre K' y K'' . Considere el subcampo de K'' generado por un subconjunto X de K'' (IV.2.4 y P.IV.2.5 ii).

1.8 Definición. Sea X un subconjunto de K'' y $K' \hookrightarrow K''$ una extensión. El subcampo de K'' generado por $K' \cup X$ denotado con $K'(X)$, se llama **subcampo obtenido por la adjunción de X a K'** .

Obsérvese que el subcampo $K'(X)$ puede ser mucho más grande que $K' \cup X$. $K'(\{x, y, z\})$ se denota $K'(x, y, z)$. Consideremos la extensión $K' \hookrightarrow K''$ con $X = \{a_1, \dots, a_j \mid a_i \in K'' \text{ para } i = 1, \dots, j\}$. Denotamos con $K'(a_1, \dots, a_j)$ el mínimo subcampo de K'' que contiene a K' y a los elementos a_1, \dots, a_j .

La extensión $K' \hookrightarrow K'(a_1, \dots, a_j)$ se dice que está **generada** por a_1, \dots, a_j y también decimos que es una extensión **finitamente generada** de K' . La extensión $K' \hookrightarrow K'(a)$ se llama **extensión simple** de K' por a . El reordenar las $a_i \in K''$ para $i = 1, \dots, j$, no cambia $K'(a_1, \dots, a_j)$ y se tiene que $K'(a_1, \dots, a_n) = K'(a_1, \dots, a_{n-1})(a_n)$.

1.9 Ejemplo. Por 1.7 sabemos que $[\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{2})] = 2$. Adjuntemos $\sqrt{3}$ a $\mathbb{Q}(\sqrt{2})$, es decir, consideremos $(\mathbb{Q}(\sqrt{2}))(\sqrt{3})$. Entonces sus elementos son de la forma $a = c + d\sqrt{3}$ con $c, d \in \mathbb{Q}(\sqrt{2})$. Luego, $1, \sqrt{3}$ generan $(\mathbb{Q}(\sqrt{2}))(\sqrt{3})$. Es fácil ver que son linealmente independientes sobre $\mathbb{Q}(\sqrt{2})$. Por lo tanto son

una base de $(\mathbb{Q}(\sqrt{2}))(\sqrt{3})$ sobre $\mathbb{Q}(\sqrt{2})$. Así, $[\mathbb{Q}(\sqrt{2}) \rightarrow (\mathbb{Q}(\sqrt{2}))(\sqrt{3})] = 2$. Por 1.4, se tiene que $[\mathbb{Q} \rightarrow \mathbb{Q}(\sqrt{2})(\sqrt{3})] = 4$. Por la demostración de 1.4, $\{\sqrt{6}, \sqrt{3}, \sqrt{2}, 1\}$ es base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre \mathbb{Q} .

1.10 Ejemplo. Como vimos en 1.7 $[\mathbb{Q} \rightarrow \mathbb{Q}(\sqrt{2})] = 2$. Sabemos que $\mathbb{Q}(\sqrt{2})$ es subcampo de \mathbb{R} y que $i \notin \mathbb{Q}(\sqrt{2})$ pues $i \notin \mathbb{R}$. Como $i^2 + 1 = 0$, $\mathbb{Q}(\sqrt{2})(i) = \mathbb{Q}(\sqrt{2}, i)$ y $[\mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2}, i)] = 2$. Luego

$$[\mathbb{Q} \rightarrow \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2}, i)] = [\mathbb{Q} \rightarrow \mathbb{Q}(\sqrt{2}, i)] = 4$$

Observe que $K'[t]$ puede verse como un espacio vectorial sobre K' donde los elementos a^n con $n \geq 0$ generan $K'[t]$ sobre K' y que $K'[t]$ no es de dimensión finita pues los polinomios pueden tener un grado muy grande y no ser combinaciones lineales de un conjunto finito de polinomios.

Podemos hacer equivalente el problema de "encontrar las soluciones" de una ecuación polinomial

$$f = \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0$$

al problema de encontrar las raíces o ceros de

$$f^{\textcircled{a}} = E_a(f) = \lambda_n a^n + \cdots + \lambda_2 a^2 + \lambda_1 a^1 + \lambda_0.$$

Es decir, resolveremos el problema original traducido a un problema equivalente usando homomorfismos, ideales, cocientes, etc. Nos preguntamos si existe una extensión $K' \rightarrow K$ tal que $f(t) \in K'[t]$ posea una raíz en K . Veremos que todo polinomio de grado mayor o igual a 1 con coeficientes en cualquier campo K' posee una raíz en algún subcampo K de K'' que lo contenga. ¿Existirá una extensión K de K' tal que un polinomio $f(t) \in K'[t]$ tenga una raíz en K ?

Consideremos la extensión $K' \rightarrow K''$, $a \in K''$ y t la indeterminada. Entonces el homomorfismo de evaluación $E_a : K'[t] \rightarrow K''$ envía K' isomórficamente en sí mismo tal que para $b \in K'$, $E_a(b) = b$ y $E_a(t) = a$. Como todo polinomio f se factoriza en $K'[t]$ en polinomios irreducibles sobre K' , si q denota uno de tales polinomios irreducibles, el ideal I generado por q es máximo en $K'[t]$. Luego el cociente $K'[t]/I$ es campo. Considérese

$$\varphi : K' \rightarrow K'[t]/I$$

dada por

$$x \longmapsto x + I$$

Es fácil ver que φ envía a K' isomórficamente en sí mismo dentro de $K'[t]/I$ (Problema 1.4). Así, podemos considerar $K = K'[t]/I$ como una extensión de K' . Sea $a = t + I$, $a \in K$. Consideremos $E_a : K'[t] \longrightarrow K$. Si

$$q(t) = \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0, \lambda_i \in K'$$

entonces

$$q^{\textcircled{a}} a = E_a(q(t)) = (\lambda_n (t + I)^n + \cdots + \lambda_2 (t + I)^2 + \lambda_1 (t + I)^1 + \lambda_0) + I \in K.$$

Como t es un representante de la clase lateral $a = t + I$, $q(a) = (\lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0) + I = q(t) + I = I$ en K . Luego, a es tal que $q(a) = 0$ y, por lo tanto, $f(a) = 0$. Hemos probado el siguiente

1.11 Teorema. (Kronecker) Si $f(t)$ es un polinomio no trivial en $K'[t]$ donde K' es un campo, entonces existe una extensión K de K' y un elemento $a \in K$ tal que $f(a) = 0$. ♦

1.12 Ejemplo. El polinomio $f(t) = t^2 + t + 1 \in \mathbb{Z}_2[t]$ es irreducible sobre \mathbb{Z}_2 , (Problema 1.5). Por el Teorema 1.11 existe un campo $K = \mathbb{Z}_2(a)$ que contiene una raíz a de f . Luego, $\mathbb{Z}_2(a)$ posee los elementos de la forma

$$\begin{array}{cccc} 0 + 0a & 1 + 0a & 0 + 1a & 1 + 1a \\ \parallel & \parallel & \parallel & \parallel \\ 0 & 1 & a & 1 + a \end{array}$$

lo cual nos proporciona un campo con cuatro elementos.

1.13 Ejemplo. Considere $K' = \mathbb{R}$ y $f(t) = t^2 + 1$ un polinomio irreducible en $\mathbb{R}[t]$. Luego, el ideal $I = \langle t^2 + 1 \rangle$ generado por este polinomio irreducible es máximo y por lo tanto el cociente $\mathbb{R}[t]/I$ es campo. Podemos ver a \mathbb{R} como un subcampo de $\mathbb{R}[t]/I$. Sea $a = t + I$. Entonces $a^2 + 1 = (t + I)^2 + (1 + I) = (t^2 + 1) + I = 0_{\mathbb{R}[t]/I}$. Así, a es una raíz de $t^2 + 1$.

Nos interesarán las extensiones $K' \twoheadrightarrow K$ para las cuales cualquier elemento $a \in K$ sea raíz de una ecuación polinomial sobre K' .

1.14 Definición. Sea $K' \twoheadrightarrow K$ una extensión. Diremos que un elemento $a \in K$ es **algebraico sobre K'** si existe un polinomio no nulo $f \in K'[t]$

tal que a es raíz de f . Si a no es raíz de algún polinomio no nulo $f \in K'[t]$ diremos que es **trascendente sobre K'** . Diremos que K es una **extensión algebraica de K'** si todo elemento de K es algebraico sobre K' . Diremos que K es una **extensión trascendente de K'** si al menos un elemento de K es trascendente sobre K' .

Se acostumbra llamar **número algebraico** a un elemento de \mathbb{C} el cual es algebraico sobre \mathbb{Q} y **número trascendente** si es trascendente sobre \mathbb{Q} .

1.15 Ejemplos. Considere la extensión $\mathbb{Q} \rightarrow \mathbb{R}$. $\sqrt{2}$ es un elemento algebraico sobre \mathbb{Q} pues es raíz del polinomio $t^2 - 2 \in \mathbb{Q}[t]$. También, si consideramos la extensión $\mathbb{Q} \rightarrow \mathbb{C}$, $\sqrt{2}$ e $i = \sqrt{-1}$ son elementos algebraicos sobre \mathbb{Q} pues son raíces de los polinomios $t^2 - 2 \in \mathbb{Q}[t]$ y $t^2 + 1 \in \mathbb{Q}[t]$ respectivamente. Cualquier elemento $a \in K'$ es raíz del polinomio $t - a \in K'[t]$ y por lo tanto es algebraico sobre K' . Se puede probar que $\pi, e \in \mathbb{R}$ son trascendentes sobre \mathbb{Q} . Pero π es algebraico sobre \mathbb{R} al ser raíz de $t - \pi \in \mathbb{R}[t]$. Observe que $\sqrt{2}$ también es raíz de muchos polinomios más, propóngala usted algunos.

Considere la extensión $K' \rightarrow K''$, y $a \in K''$ algebraico sobre K' . El **polinomio mínimo para a sobre K'** , denotado $m_{a,K'}$, es el polinomio mónico irreducible único de grado mínimo $m(t) \in K'[t]$ tal que $m(a) = 0$ el cual divide a cualquier otro polinomio que tenga a a como raíz (Problema 1.7). El grado del polinomio $m_{a,K'}$ lo llamaremos **grado de a sobre K'** y lo denotaremos $gr(a, K')$. A continuación veamos que si $a \in K''$ es algebraico sobre K' entonces $[K' \rightarrow K'(a)] = gr(a, K')$: considérese la extensión simple $K'(a)$ de K' tal que el núcleo $\ker E_a$ del homomorfismo de evaluación

$$E_a : K'[t] \longrightarrow K'(a)$$

sea no trivial. Si suponemos que a es algebraico sobre K' , el núcleo de E_a es un ideal, el cual es principal (P I.3.10) generado por $m_{a,K'}$ el cual es máximo (P I.3.14) i.e. $\ker E_a = \langle m_{a,K'} \rangle$ es un ideal máximo. Luego, $K'[t]/\langle m_{a,K'} \rangle$ es un campo el cual es isomorfo a $E_a(K'[t])$ el cual es un subcampo de $K'(a)$ que contiene a a , i.e. $K'(a)$. Todo elemento de $K'[t]/\langle m_{a,K'} \rangle$ es de la forma $f(t) + I$ donde $I = \langle m_{a,K'} \rangle$ con el grado de $f(t) < gr(m_{a,K'})$. Luego, cualquier elemento de $K'[t]/\langle m_{a,K'} \rangle$ puede escribirse como combinación lineal de n clases laterales $1 + I, t + I, t^2 + I, \dots, t^{n-1} + I$ donde $n = gr(m_{a,K'})$. Como

$t^i + I \rightarrow a^i$, vemos que los elementos $1, a, \dots, a^{n-1}$ son base para $K'(a)$ sobre K' . Así, $[K' \rightarrow K'(a)] = gr(m_{a, K'})$. (Véase el Problema 1.8)

Si consideramos la misma extensión simple $K'(a)$ de K' tal que el núcleo $\ker E_a$ del homomorfismo de evaluación $E_a : K'[t] \rightarrow K'(a)$ sea trivial. Entonces E_a es un monomorfismo. Luego $E_a(K'[t])$ no es un campo pero es un dominio entero y podemos considerar el campo de cocientes $K'(t)$ y se tiene un monomorfismo $K'(t) \rightarrow K'(a)$ el cual también es suprayectivo pues a está en la imagen. (a es trascendente sobre K').

1.16 Ejemplos. Considere la extensión $\mathbb{Q} \rightarrow \mathbb{C}$, el polinomio $f(t) = t^2 - 2$ y el homomorfismo de evaluación $E_{\sqrt{2}} : \mathbb{Q}[t] \rightarrow \mathbb{C}$. Entonces $E_{\sqrt{2}}(f(t)) = f(\sqrt{2}) = (\sqrt{2})^2 - 2 = 0$. Luego, $f(t) = t^2 - 2 \in \ker E_{\sqrt{2}}$. Así $[\mathbb{Q} \rightarrow \mathbb{Q}(\sqrt{2})] = 2 = gr(\sqrt{2}, \mathbb{Q})$, luego $m_{\sqrt{2}, \mathbb{Q}}(t) = t^2 - 2$.

Considere la extensión $\mathbb{Q} \rightarrow \mathbb{C}$, el polinomio $f(t) = t^2 + 1$ y el homomorfismo de evaluación $E_i(f(t)) = f(i) = i^2 + 1 = 0$. Luego, $f(t) = t^2 + 1 \in \ker E_i$. Así $[\mathbb{Q} \rightarrow \mathbb{Q}(i)] = 2 = gr(i, \mathbb{Q})$, luego $m_{i, \mathbb{Q}}(t) = t^2 + 1$. No es trivial el obtener el polinomio mínimo en general.

1.17 Proposición. Si una extensión $K' \rightarrow K$ es finita, entonces es algebraica sobre K' .

Demostración. Sea $a \in K$. Veamos que a es algebraico sobre K' . El conjunto $\{a^n, a^{n-1}, \dots, a^2, a^1, 1\}$ no es linealmente independiente, es decir, existe una combinación lineal

$$\lambda_n a^n + \dots + \lambda_2 a^2 + \lambda_1 a^1 + \lambda_0 = 0$$

con no toda $\lambda_i = 0$. Luego $f(t) = \lambda_n t^n + \dots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0$ es un polinomio no trivial en $K'[t]$ con $f(a) = 0$. Luego, a es algebraico sobre K' . ♦

El inverso de 1.17 es falso pues hay extensiones algebraicas de grado infinito.

1.18 Teorema. Considere la extensión algebraica $K' \rightarrow K$. Entonces, $K = K'(a_1, \dots, a_n)$ para $a_1, \dots, a_n \in K$ sí, y sólo si K es una extensión finita sobre K' .

Demostración. Si $K = K'(a_1, \dots, a_n)$, a_i es algebraico sobre K' y por lo tanto es algebraico sobre cualquier extensión de K' . Luego, el campo $K'(a_1)$ es algebraico sobre K' y generalizando $K'(a_1, \dots, a_k)$ es algebraico sobre

$K'(a_1, \dots, a_{k-1})$ para $k = 2, \dots, n$. Luego $K = K'(a_1, \dots, a_n)$ es una extensión finita de K' . La parte, sólo si, se deja como ejercicio, ver Problema 1.10.♦

1.19 Definición. Considere la extensión algebraica $K' \rightarrow K$. La **cerradura algebraica de K' en K** es el conjunto $\{a \in K \mid a \text{ es algebraico sobre } K'\}$ y lo denotaremos con $\overline{K'_K}$ o simplemente, por abuso, $\overline{K'}$.

1.20 Proposición. Si $K' \rightarrow K$ es una extensión y $\overline{K'_K}$ la cerradura algebraica de K' en K entonces $\overline{K'_K}$ es un campo y es la extensión más grande de K' en K .

Demostración. Si $a, b \in K$ son algebraicos sobre K' entonces $a \pm b$, ab y a/b con $b \neq 0$ son algebraicos sobre K' . Si $a, b \in \overline{K'_K}$ entonces $K'(a, b)$ es una extensión finita y sus elementos son algebraicos sobre K' . Es decir, $K'(a, b) \subset \overline{K'_K}$. Luego, $\overline{K'_K}$ contiene a todo elemento de K que es algebraico sobre K' , y así, $\overline{K'_K}$ es la extensión más grande de K' contenida en K .♦

Problemas

1.1 Considere una familia de campos $\{K_i\}$ para $i = 1, \dots, s$ tal que cada K_{i+1} es una extensión finita de K_i . Pruebe que K_s es una extensión finita de K_1 y que

$$[K_1 \rightarrow K_s] = [K_1 \rightarrow K_2][K_2 \rightarrow K_3] \cdots [K_{s-1} \rightarrow K_s].$$

1.2 Sea $\mathbb{R}(i)$ el subcampo que contiene a los elementos de la forma $x + iy$, con $x, y \in \mathbb{R}$. Pruebe que $\mathbb{C} = \mathbb{R}(i)$.

1.3 Pruebe que $\mathbb{Q} \rightarrow \mathbb{R}$ y $\mathbb{Q} \rightarrow \mathbb{C}$ son extensiones infinitas y que $[\mathbb{Q} \rightarrow \mathbb{Q}(i)] = 2$.

1.4 Considérese

$$\varphi : K' \longrightarrow K'[t]/I$$

dada por

$$t \longmapsto t + I$$

Verifique que φ envía a K' isomórficamente en sí mismo dentro de $K'[t]/I$.

1.5 Pruebe que si f es un polinomio en $K'[t]$ de grado 2 ó 3, entonces f tiene una raíz en K' si, y sólo si, f es reducible sobre K' .

1.6 Escriba las tablas de sumar y multiplicar del campo con cuatro elementos del Ejemplo 1.12.

1.7 Pruebe que el polinomio mínimo para a sobre K' , denotado $m_{a,K'}$, divide a cualquier otro polinomio que tenga a a como raíz.

1.8 Pruebe que si $a \in K$ entonces son equivalentes las siguientes: (i) a es algebraico sobre K' , (ii) el homomorfismo de evaluación posee un núcleo no trivial y (iii) la extensión $K' \mapsto K'(a)$ es finita.

1.9 Compruebe que $m_{\sqrt{2},\mathbb{Q}}(t) = t^2 - 2$, que $m_{\sqrt{2},\mathbb{R}}(t) = t^2 - \sqrt{2}$, y por lo tanto, $\sqrt{2}$ es algebraico de grado 2 sobre \mathbb{Q} y es algebraico de grado 1 sobre \mathbb{R} . También compruebe que $m_{i,\mathbb{C}}(t) = t - i$.

1.10 Pruebe la parte "sólo si" de 1.18.

1.11 Compruebe que $K'[t]$ puede verse como un espacio vectorial sobre K' donde los elementos a^n con $n \geq 0$ generan $K'[t]$ sobre K' .

1.12 Considere la extensión $\mathbb{Q} \mapsto \mathbb{C}$. Encuentre el polinomio mínimo para $\sqrt{2} + \sqrt{3}$ sobre \mathbb{Q} .

1.13 Compruebe que $\mathbb{Q}(\sqrt[6]{2}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$. Sugerencia: Verifique que

$$[\mathbb{Q}(\sqrt[6]{2}) \mapsto \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})] = 1.$$

V.2 Automorfismos y más sobre extensiones

2.1 Definición. Sea Λ un anillo. Un **automorfismo** de Λ es un isomorfismo de anillos $\sigma : \Lambda \rightarrow \Lambda$. Denotaremos con $Aut(\Lambda)$ el conjunto de automorfismos de Λ .

2.2 Definición. Sea Γ un subanillo de Λ . Un **automorfismo de Λ sobre Γ** es un isomorfismo de anillos $\sigma : \Lambda \rightarrow \Lambda$ tal que $\sigma(a) = a$ para toda $a \in \Gamma$. Denotaremos con $Aut_\Gamma(\Lambda)$ el conjunto de automorfismos de Λ sobre Γ .

2.3 Proposición. $Aut(\Lambda)$ y $Aut_\Gamma(\Lambda)$ son grupos bajo la composición de funciones.

Demostración. Como la composición de automorfismos es automorfismo, como vale la asociatividad de funciones bajo la composición, como el inverso de un automorfismo también es un automorfismo y la identidad también lo es, el conjunto $Aut(\Lambda)$ es un grupo bajo la composición. Análogamente para $Aut_\Gamma(\Lambda)$.♦

2.4 Ejemplo. Considere $\Lambda = \mathbb{Z}$. Entonces todo $m \in \mathbb{Z}$ es de la forma $m1$ para $m \in \mathbb{Z}$. Claramente $\sigma(m1) = m1$. Por lo tanto $\sigma = I_{\mathbb{Z}}$. Luego, $Aut(\mathbb{Z}) = \{I_{\mathbb{Z}}\}$.

2.5 Proposición. Sea Δ un dominio entero, (K, f) su campo de cocientes y $\sigma : \Delta \rightarrow \Delta$ un automorfismo. Entonces el homomorfismo inducido $\sigma_* : K \rightarrow K$ es un automorfismo.

Demostración. Por I.3.4, existe $\sigma_* : K \rightarrow K$. Veamos que posee inverso. Como $\sigma : \Delta \rightarrow \Delta$ induce $\sigma_*^{-1} : K \rightarrow K$ y $\sigma^{-1}\sigma = \sigma\sigma^{-1} = I$. Por el Problema 2.3 (i), $\sigma_*^{-1}\sigma_* = \sigma_*\sigma_*^{-1} = I_K$. Luego, σ_* posee a σ_*^{-1} como inverso.♦

2.6 Definición. Sea $K' \succ K$ una extensión y $f \in K'[t]$. Diremos que f se **descompone en** $K' \succ K$ o **sobre** K si se factoriza en factores lineales en $K[t]$.

Observe que si se tiene un campo K'' tal que $f \in K'[t]$ se descompone sobre K'' , entonces las distintas raíces a_1, \dots, a_j de $f(t)$ en K'' generan el subcampo $K'(a_1, \dots, a_j)$ de K'' que es el campo mínimo de K'' en el cual f se factoriza en factores lineales en $K''[t]$.

2.7 Definición. La extensión mínima de K' que cumple lo anterior se llama **campo de descomposición** de f sobre K' y lo denotaremos K'_f .

Nos preguntamos si existe una extensión $K' \succ K''$ tal que un polinomio f se factorice en factores lineales. Para contestar esta pregunta, supongamos que a_1 es una raíz en $K' \succ K^1$ y omitimos el factor $(t - a_1)$ considerando el polinomio $f_1(t) = f(t)/(t - a_1) \in K^1[t]$. Luego hacemos lo mismo encontrando una extensión $K' \succ K^2$ que contenga una raíz de $f_1(t)$, etc. Así tenemos el siguiente

2.8 Teorema. Sea $f \in K'[t]$ un polinomio. Entonces existe una extensión finita $K' \succ K''$ que es un campo de descomposición de f sobre K' . ♦

2.9 Ejemplo. Considere el polinomio $f(t) = t^4 - 4$ en $\mathbb{Q}[t]$. Como $f(t) = (t^2 - 2)(t^2 + 2)$ podemos adjuntar las raíces $-\sqrt{2}$ y $\sqrt{2}$ de $t^2 - 2$ obteniendo $\mathbb{Q}(-\sqrt{2}, \sqrt{2}) = \mathbb{Q}(\sqrt{2})$ el cual es una extensión $\mathbb{Q} \succ \mathbb{Q}(\sqrt{2})$ de grado 2. Nos fijamos en $(t^2 + 2) \in \mathbb{Q}(\sqrt{2})[t]$. Las raíces $-\sqrt{2}i$ y $\sqrt{2}i$ son complejas, no en \mathbb{R} , luego $(t^2 + 2)$ es irreducible en $\mathbb{Q}(\sqrt{2})[t]$. Ahora consideramos $\mathbb{Q}(\sqrt{2}, \sqrt{2}i) = \mathbb{Q}(\sqrt{2}, i)$ y la extensión $\mathbb{Q}(\sqrt{2}) \succ \mathbb{Q}(\sqrt{2}, i)$ la cual es de grado 2. Considere la torre acostada de campos $\mathbb{Q} \xrightarrow{2} \mathbb{Q}(\sqrt{2}) \xrightarrow{2} \mathbb{Q}(\sqrt{2}, i) \xrightarrow{\dots} \mathbb{C}$. Luego el campo de descomposición de f sobre \mathbb{Q} en \mathbb{C} es $\mathbb{Q}(\sqrt{2}, i)$ y por lo tanto $[\mathbb{Q} \succ \mathbb{Q}(\sqrt{2}, i)] = 4$.

Suponga que $a_1, \dots, a_j \in K$ son las distintas raíces de $f \in K'[t]$. $K'(a_1, \dots, a_j)$ es el mínimo subcampo que contiene a K' y a las a_i . Pero $K'(a_1, \dots, a_j)$ está contenido en cualquiera o todo subcampo de descomposición. Por lo tanto tenemos la siguiente

2.10 Proposición. Sea $K' \succ K''$ una extensión y $f \in K''[t]$. Si K^1 y K^2 son subcampos de descomposición para f sobre K' entonces $K^1 = K^2$. ♦

Notación. (i) Para las extensiones $K' \succ K$ y $K' \succ K''$ denotaremos con $\text{hom}_{K'}(K, K'')$ el conjunto de homomorfismos (inyectivos) de K en K'' que dejan fijo a K' . Considere la extensión finita $K' \succ K''$, entonces $\text{hom}_{K'}(K'', K'') = \text{Aut}_{K'}(K'', K'')$ es un grupo. (ii) Sea $K' \succ K''$ una extensión y $f \in K'[t]$. Denotaremos con $R(f, K'')$ el conjunto de las raíces de f en K'' .

2.11 Proposición. Sea $K' \succ K''$ una extensión y $f \in K'[t]$ un polinomio irreducible. Sea $a_i \in K''$ una raíz de f . Entonces los conjuntos

$$\text{hom}_{K'}(K'(a_i), K'') \text{ y } R(f, K'')$$

poseen la misma cardinalidad.

Demostración. Considere el diagrama

$$\begin{array}{ccccc}
 K' & \longrightarrow & K'[t] & \xrightarrow{\varphi} & K'[t]/\langle f \rangle \\
 & \searrow & \downarrow E_a & \swarrow \varphi_a & \downarrow \cong \varphi_{a_i} \\
 & & K'' & \longleftarrow & K'(a_i)
 \end{array}$$

donde $E_a : K'[t] \rightarrow K''$ es el homomorfismo de evaluación, el cual se factoriza mediante $\varphi_a : K'[t]/\langle f \rangle \rightarrow K''$. Para cada raíz a_i existe un φ_{a_i} . Entonces, cada raíz a_i da lugar a un homomorfismo $\psi_a = \varphi_a \circ (\varphi_{a_i})^{-1}$ para el cual $\psi_a(a_i) = a_i$. ♦

2.12 Ejemplo. Como $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[t]/\langle t^2 - 2 \rangle$ donde $t^2 - 2$ es irreducible sobre \mathbb{Q} , hay dos homomorfismos que dejan fijo a \mathbb{Q} que envían $\sqrt{2}$ en $\pm\sqrt{2}$, que son raíces complejas de $t^2 - 2$. Estas dos raíces nos dan los homomorfismos

$$\begin{aligned}
 1, \delta : \mathbb{Q}(\sqrt{2}) &\longrightarrow \mathbb{C} \\
 a + b\sqrt{2} &\longmapsto 1(a + b\sqrt{2}) = a + b\sqrt{2} \\
 a + b\sqrt{2} &\longmapsto \delta(a + b\sqrt{2}) = a - b\sqrt{2}
 \end{aligned}$$

Si ponemos $\mathbb{Q}(\sqrt{2})$ en lugar de \mathbb{C} obtenemos

$$\text{hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}), \mathbb{C}) = \text{hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{2})) = \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})).$$

Luego $|\text{hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}), \mathbb{C})| = 2$.

La siguiente proposición es clave para comprender el grupo de automorfismos para el caso de extensiones algebraicas.

2.13 Proposición. Considere las extensiones $K' \succ K$ y $K' \succ K''$. Entonces

(i) para $f \in K[t]$, cada $\delta \in \text{hom}_{K'}(K, K'')$ se restringe a una función inyectiva $\delta_f : R(f, K) \longrightarrow R(f, K'')$.

(ii) si $\delta \in \text{hom}_{K'}(K, K)$ entonces $\delta_f : R(f, K) \longrightarrow R(f, K)$ es biyectiva.

Demostración. (i) Para $a \in R(f, K)$ se tiene que $f(\delta(a)) = \delta(f(a)) = \delta(0) = 0$, por lo tanto δ envía $R(f, K)$ en $R(f, K'')$. Como δ es inyectiva, su restricción a $R(f, K) \subseteq K$ es una inyección también.

(ii) De (i), $\delta_f : R(f, K) \longrightarrow R(f, K)$ es inyectiva y como es de un conjunto finito en sí mismo es suprayectiva. ♦

Observe que (ii) dice que cualquier automorfismo de K permuta el conjunto de raíces de K de un polinomio $f \in K[t]$.

2.14 Definición. Considere la extensión $K' \succ K''$. Diremos que los elementos $a, b \in K''$ son **conjugados sobre K'** si son raíces del mismo polinomio mínimo sobre K' , es decir, $m_{a,K'} = m_{b,K'}$.

2.15 Ejemplos. Considere la extensión $\mathbb{Q} \succ \mathbb{C}$, i y $-i$ son conjugados sobre \mathbb{Q} pues son raíces del mismo polinomio mínimo sobre \mathbb{Q} , $m_{i,\mathbb{Q}}(t) = t^2 + 1 = m_{-i,\mathbb{Q}}(t)$. Si se considera la extensión $\mathbb{Q} \succ \mathbb{C}$, $\sqrt{2}$ y $-\sqrt{2}$ son conjugados sobre \mathbb{Q} pues son raíces del mismo polinomio mínimo sobre \mathbb{Q} , $m_{\sqrt{2},\mathbb{Q}}(t) = t^2 - 2 = m_{-\sqrt{2},\mathbb{Q}}(t)$. También, para $\mathbb{Q} \succ \mathbb{C}$, $\sqrt[3]{2}$, $\sqrt[3]{2}e^{2\pi i/3}$, $\sqrt[3]{2}e^{4\pi i/3}$ son conjugados sobre \mathbb{Q} pues son raíces del mismo polinomio mínimo sobre \mathbb{Q} , $m_{\sqrt[3]{2},\mathbb{Q}}(t) = t^3 - 2$.

2.16 Teorema. Sea K' un campo, a, b elementos algebraicos sobre K' , $n = \text{gr}(m_{a,K'})$. Entonces a y b son conjugados sobre K' si, y sólo si, la función

$$\varphi_{a,b} : K'(a) \longrightarrow K'(b)$$

dada por

$$\lambda_{n-1}a^{n-1} + \cdots + \lambda_1a^1 + \lambda_0 \longmapsto \lambda_{n-1}b^{n-1} + \cdots + \lambda_1b^1 + \lambda_0$$

es un isomorfismo de campos.

Demostración. Supongamos que a y b son conjugados, es decir, $m_{a,K'} = m_{b,K'}$. Consideremos el siguiente diagrama

$$\begin{array}{ccccc}
 \langle m_{a,K'} \rangle & \longrightarrow & K'[t] & \longrightarrow & K'[t]/\langle m_{a,K'} \rangle \equiv K'[t]/\langle m_{b,K'} \rangle \\
 & & \searrow E_a & & \downarrow \cong \varphi_b \\
 & & & & K'(a) \xrightarrow{\varphi_{a,b}} K'(b) \\
 & & & & \downarrow \cong \varphi_a \\
 & & & & K'(a)
 \end{array}$$

Definimos $\varphi_{a,b} = \varphi_b \circ \varphi_a^{-1}$ el cual es un isomorfismo tal que

$$\begin{aligned}
 \varphi_{a,b}(\lambda_{n-1}a^{n-1} + \dots + \lambda_1a^1 + \lambda_0) &= \varphi_b \circ \varphi_a^{-1}(\lambda_{n-1}a^{n-1} + \dots + \lambda_1a^1 + \lambda_0) \\
 &= \varphi_b[(\lambda_{n-1}a^{n-1} + \dots + \lambda_1a^1 + \lambda_0) + \langle m_{a,K'} \rangle] \\
 &= \lambda_{n-1}b^{n-1} + \dots + \lambda_1b^1 + \lambda_0.
 \end{aligned}$$

Ahora veamos que si $\varphi_{a,b}$ es isomorfismo entonces a y b serán conjugados. Considere $m_{a,K'}(t) = \lambda_n t^n + \dots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0$. Entonces $\lambda_n a^n + \dots + \lambda_2 a^2 + \lambda_1 a^1 + \lambda_0 = 0$. Por lo tanto $\varphi_{a,b}(\lambda_n a^n + \dots + \lambda_2 a^2 + \lambda_1 a^1 + \lambda_0) = \lambda_n b^n + \dots + \lambda_2 b^2 + \lambda_1 b^1 + \lambda_0 = 0$. Luego $m_{b,K'} | m_{a,K'}$. Análogamente $m_{a,K'} | m_{b,K'}$ y así, a y b son conjugados. ♦

2.17 Ejemplo. Considere la extensión $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{2})$ y el polinomio $m_{\sqrt{2},\mathbb{Q}}(t) = t^2 - 2$. Sus raíces son $-\sqrt{2}$ y $\sqrt{2}$ y por definición, son conjugadas sobre \mathbb{Q} . Por el teorema anterior, $\varphi_{\sqrt{2},-\sqrt{2}} : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$ dada por $a + b\sqrt{2} \mapsto \varphi_{\sqrt{2},-\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2}$ es un automorfismo de $\mathbb{Q}(\sqrt{2})$.

2.18 Definiciones. Sea $f \in K'[t]$ un polinomio irreducible. Diremos que el polinomio f es **separable sobre** K'' si toda raíz de f es simple en la extensión $K' \hookrightarrow K''$. Un elemento algebraico $a \in K''$ en una extensión $K' \hookrightarrow K''$ es **separable** si su polinomio mínimo $m_{a,K'} \in K'[t]$ es separable. Si $K' \hookrightarrow K''$ es una extensión finita, el **grado de separabilidad**, denotado $\{K' \hookrightarrow K''\}$, de la extensión $K' \hookrightarrow K''$, es el orden de $\text{hom}_{K'}(K'', \overline{K'})$. Si $K' \hookrightarrow K''$ es una extensión finita, se dice que es **separable** si $\{K' \hookrightarrow K''\} = [K' \hookrightarrow K'']$.

Observe que si $K' \hookrightarrow K'(a)$ es una extensión finita simple, por 2.11 aplicado a $K'' = \overline{K'}$ se tiene que $\{K' \hookrightarrow K'(a)\} = |R(m_{a,K'}, \overline{K'})|$.

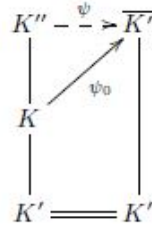
2.19 Proposición. Si $K' \rightsquigarrow K$ y $K \rightsquigarrow K''$ son extensiones finitas, entonces $\{K' \rightsquigarrow K\}\{K \rightsquigarrow K''\} = \{K' \rightsquigarrow K''\}$.

Demostración. Problema 2.6.♦

2.20 Definición. Considere $K' \rightsquigarrow K''$ una extensión finita. Diremos que es una **extensión normal** si K'' es el campo de descomposición sobre K' de algún polinomio $f \in K'[t]$.

Recuérdese que $hom_{K'}(K, K'')$ denota el conjunto de homomorfismos de K en K'' que dejan fijo a K' . Así, $hom_{K'}(K'', K'') = Aut_{K'}(K'')$ pues todo homomorfismo inyectivo es suprayectivo y por lo tanto invertible. Por el Problema 2.8, una extensión $K' \rightsquigarrow K''$ es normal si para toda $\psi \in hom_{K'}(K'', \overline{K'})$ se tiene que $\psi(K'') = K''$. Obsérvese que si $K' \rightsquigarrow K''$ es una extensión normal, entonces, siempre que se tenga un polinomio irreducible $f \in K'[t]$ el cual posea una raíz en K'' , se separa en K'' puesto que cada par de raíces de f son conjugadas sobre K' y una va a dar a la otra mediante un homomorfismo $\overline{K'} \rightarrow \overline{K'}$ que envía a K'' en sí mismo.

2.21 Teorema. Sea $K' \rightsquigarrow K''$ una extensión algebraica y $K' \rightsquigarrow K \rightsquigarrow K''$ una torre de campos. Si $\psi_0 : K \rightarrow \overline{K'}$ es un homomorfismo que fija los elementos de K' , entonces existe un homomorfismo $\psi : K'' \rightarrow \overline{K'}$ que "extiende" a ψ_0 .



Demostración. Sea A el conjunto de las parejas (C, φ) donde $(K \rightsquigarrow C) \leq (K \rightsquigarrow K'')$ y $\varphi : C \rightarrow \overline{K'}$ extiende a ψ_0 . Ordenemos A mediante la relación \lll para la cual $(C_1, \varphi_1) \lll (C_2, \varphi_2)$ siempre que $C_1 \leq C_2$ y φ_2 extiende a φ_1 . Luego (A, \lll) es un conjunto parcialmente ordenado. Supóngase que $B \subseteq A$ es un subconjunto totalmente ordenado. Sea $\mathcal{C} = \cup_{(C, \varphi) \in B} C$. Entonces $(K \rightsquigarrow \mathcal{C}) \leq (K \rightsquigarrow K'')$. También existe una función $\overline{\varphi} : \mathcal{C} \rightarrow \overline{K'}$ dada por $\overline{\varphi}(a) = \varphi(a)$ cuando $a \in C$ para $(C, \varphi) \in B$. Es claro que si $a \in C'$ para $(C', \varphi') \in B$ entonces $\overline{\varphi}(a) = \varphi'(a)$ y por lo tanto $\overline{\varphi}$ está bien definida. Entonces para toda pareja $(C, \varphi) \in B$ tenemos que $(C, \varphi) \lll (\mathcal{C}, \overline{\varphi})$ y así $(\mathcal{C}, \overline{\varphi})$ es una cota superior de B . Por el Lema de Zorn, debe de haber un elemento máximo de A , a saber, (K'', φ_0) .

Supongamos que $K_0'' \neq K''$, entonces existe un elemento $a \in K''$ para el cual $a \notin K_0''$. Como K'' es algebraico sobre K' , también es algebraico sobre K_0'' pues a es algebraico sobre K_0'' . Si $m_{a, K_0''}(t) = t^n + \dots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0$, entonces el polinomio $f(t) = t^n + \dots + \varphi_0(\lambda_2)t^2 + \varphi_0(\lambda_1)t^1 + \varphi_0(\lambda_0) \in (\varphi_0(K_0''))[t]$ es también irreducible y por lo tanto tiene una raíz b en $\overline{K'}$ el cual es también la cerradura algebraica de $\varphi_0(K_0'')$. Por la propiedad universal del anillo de polinomios $K_0''[t]$, φ_0 da lugar a φ_0'' como en el siguiente diagrama

$$\begin{array}{ccccc}
 K_0'' & \longrightarrow & K_0''[t] & \longrightarrow & K_0''[t]/\langle m_{a, K_0''}(t) \rangle \cong K_0''(a) \\
 & \searrow \varphi_0 & \downarrow \varphi_0' & & \swarrow \varphi_0'' \\
 & & K' & &
 \end{array}$$

Pero $(K_0'', \varphi_0) \lll (K_0''(a), \varphi_0'')$ y $(K_0'', \varphi_0) \neq (K_0''(a), \varphi_0'')$ contradiciendo la maximalidad de (K_0'', φ_0) . Por lo tanto, $K_0'' = K''$ y podemos tomar $\psi = \varphi_0$. ♦

2.22 Definición. Considere $K' \rightarrow K''$ una extensión finita simple. Diremos que $a \in K''$ es un **elemento primitivo** de la extensión si $K'' = K'(a)$.

El siguiente teorema se conoce como el teorema del elemento primitivo.

2.23 Teorema (del elemento primitivo) . Sea $K' \rightarrow K''$ una extensión separable. Entonces K'' posee un elemento primitivo.

Demostración. Supongamos que K'' es un campo infinito. Como K'' se construye a partir de una sucesión de extensiones simples, basta considerar el caso $K'' = K'(a, b)$. Sean $f, g \in K'[t]$ los polinomios mínimos de a y b sobre K' respectivamente. Considere $a = a_1, \dots, a_r$ y $b = b_1, \dots, b_s$ las distintas raíces de f y g respectivamente en K' . Como $K' \rightarrow K''$ es separable, $r = gr(f)$ y $s = gr(g)$. Para $j \neq 1$ se tiene que $b = b_1 \neq b_j$ y por lo tanto la ecuación $a + xb = a_i + xb_j$ tiene solamente una solución, a saber, $a - a_i = xb_j - xb = x(b_j - b)$ y $x = \frac{a - a_i}{b_j - b}$. Si escogemos una $x \in K'$ diferente de estas soluciones (pues K' es infinito), entonces $a + xb \neq a_i + xb_j$, excepto cuando $i = j = 1$.

Sea $c = a + xb$. Entonces los polinomios $g(t)$ y $f(c - xt)$ tienen coeficientes en $K'(c)[t]$ y poseen a b como raíz, es decir, $g(b) = 0$ y $f(c - xb) = f(a) = 0$. De hecho, b es su única raíz común pues escogimos x tal que $c \neq a_i + xb_j$, es decir, $a_i \neq c - xb_j$ a menos que $1 = i = j$.

Por lo tanto, el $m.c.d.(g(t), f(c - xt)) = t - b$. Se sabe que el máximo común divisor de dos polinomios tiene coeficientes en el mismo campo que los coeficientes de los polinomios. Luego $b \in K'(c)$ y esto implica que $a = c - xb$ también está en $K'(c)$. Por lo tanto, $K'(a, b) = K'(c)$. Para el caso en que K'' sea un campo finito, ver el Problema 3.5 en la siguiente sección. ♦

Problemas

2.1 Pruebe que $Aut(\mathbb{Z}_n) = \{I_{\mathbb{Z}_n}\}$.

2.2 Suponga que un anillo Λ contiene a $\Gamma = \mathbb{Z}$ ó \mathbb{Z}_n y $\sigma \in Aut(\Lambda)$. Pruebe que σ se restringe a la identidad en Λ y por lo tanto $Aut(\Lambda) = Aut_{\Gamma}(\Lambda)$.

2.3 Sean Δ' y Δ dominios enteros, K' y K sus campos de cocientes respectivamente y $\sigma : \Delta' \rightarrow \Delta$ un monomorfismo. (i) Pruebe que existe un único homomorfismo inducido $\sigma_* : K' \rightarrow K$ tal que $\sigma_*(a) = \sigma(a)$ para $a \in \Delta' \subset K'$. (ii) Pruebe que $I_{\Delta'} : \Delta' \rightarrow \Delta'$ induce $I_* = I : K' \rightarrow K'$ y que si $\Delta' \xrightarrow{\sigma} \Delta \xrightarrow{\mu} \Delta''$ son monomorfismos de dominios enteros, entonces $\mu_*\sigma_* = (\mu\sigma)_* : K' \rightarrow K'$.

2.4 (i) Pruebe que $(\)_* : Aut(\Delta') \rightarrow Aut(K')$ es un monomorfismo. (ii) Pruebe que $(\)_* : Aut(\mathbb{Z}) \rightarrow Aut(\mathbb{Q})$ es un isomorfismo y por lo tanto $Aut(\mathbb{Q}) = \{I_{\mathbb{Q}}\}$.

2.5 Pruebe que las raíces de polinomios con coeficientes en \mathbb{R} son conjugadas. Sugerencia: considere $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}(-i)$.

2.6 Pruebe la Proposición 2.19: si $K' \rightarrow K$ y $K \rightarrow K''$ son extensiones finitas, entonces $\{K' \rightarrow K\}\{K \rightarrow K''\} = \{K' \rightarrow K''\}$.

2.7 Pruebe que si $K' \rightarrow K$ y $K \rightarrow K''$ son extensiones finitas, entonces $K' \rightarrow K$ y $K \rightarrow K''$ son separables si, y sólo si $K' \rightarrow K''$ es separable.

2.8 Pruebe que K'' es el campo de descomposición sobre K' de algún polinomio $f \in K'[t]$ (es decir $K' \rightarrow K''$ es una extensión normal) si, y sólo si, $\psi(K'') = K''$ para todo $\psi \in hom_{K'}(K'', \overline{K'})$.

2.9 Considere las extensiones finitas $K' \rightarrow K$ y $K \rightarrow K''$. Pruebe que si la extensión $K' \rightarrow K''$ es normal, entonces la extensión $K \rightarrow K''$ es normal.

2.10 Sea f un polinomio en $K'[t]$. Un elemento $a \in \overline{K'}$ tal que $f(a) = 0$ es una **raíz de multiplicidad** n si n es el mayor entero tal que $(t - a)^n$ es un factor de f en $\overline{K'}[t]$. Pruebe que si f es irreducible en $K'[t]$ entonces todas las raíces de f en $\overline{K'}$ tienen la misma multiplicidad. Sugerencia: Use los Teoremas 2.16 y 2.21.

V.3 Teoría de Galois

Recordemos que hemos estado estudiando la estructura de una extensión algebraica $K' \rightarrow K''$ analizando los automorfismos de K'' que dejan fijo a K' , es decir, analizando $\text{Aut}_{K'}(K'')$.

3.1 Definición. Una extensión finita $K' \rightarrow K''$ se llama **extensión de Galois** si es normal y separable.

Por el teorema 2.21, todo automorfismo $K' \rightarrow K'$ se extiende a un homomorfismo de $K'' \rightarrow \overline{K'}$ manteniendo fijos a los elementos de K' . Luego tenemos la biyección $\text{hom}_{K'}(K'', \overline{K'}) \longleftrightarrow \text{Aut}_{K'}(K'')$ y por lo tanto

$$|\text{Aut}_{K'}(K'')| = \{K' \rightarrow K''\} = [K' \rightarrow K''].$$

3.2 Definición. El **grupo de Galois de la extensión** $K' \rightarrow K''$ es el grupo $\text{Aut}_{K'}(K'')$ denotado $\text{Gal}(K' \rightarrow K'')$. Sus elementos se llaman **automorfismos de Galois** de $K' \rightarrow K''$.

$$\text{Así, } |\text{Gal}(K' \rightarrow K'')| = \{K' \rightarrow K''\} = [K' \rightarrow K''].$$

3.3 Ejemplo. Por 1.9 sabemos que $[\mathbb{Q} \rightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3})] = 4$. Consideremos $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{3})$. El isomorfismo $\varphi_{\sqrt{3}, -\sqrt{3}} : \mathbb{Q}(\sqrt{2}, \sqrt{3}) \rightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3})$ dado por $c + d\sqrt{3} \mapsto c - d\sqrt{3}$, con $c, d \in \mathbb{Q}(\sqrt{2})$ es un automorfismo que tiene a $\mathbb{Q}(\sqrt{2})$ como campo fijo. Análogamente, $\varphi_{\sqrt{2}, -\sqrt{2}} : \mathbb{Q}(\sqrt{2}, \sqrt{3}) \rightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3})$ tiene a $\mathbb{Q}(\sqrt{3})$ como campo fijo. Como la composición de automorfismos es un automorfismo, vemos que $\varphi_{\sqrt{3}, -\sqrt{3}} \circ \varphi_{\sqrt{2}, -\sqrt{2}}$ no deja fijo ni a $\sqrt{2}$, ni a $\sqrt{3}$. Consideremos el grupo $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3}))$. Sabemos que $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ es una base para $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre \mathbb{Q} . Consideremos $\iota = 1_{\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3}))}$, $\alpha_1 = \varphi_{\sqrt{2}, -\sqrt{2}}$, $\alpha_2 = \varphi_{\sqrt{3}, -\sqrt{3}}$ y $\alpha_3 = \varphi_{\sqrt{3}, -\sqrt{3}} \circ \varphi_{\sqrt{2}, -\sqrt{2}}$. Como $\alpha_1(\sqrt{2}) = -\sqrt{2}$, $\alpha_1(\sqrt{6}) = -\sqrt{6}$ y $\alpha_2(\sqrt{3}) = -\sqrt{3}$, \mathbb{Q} es el campo fijo de $\{\iota, \alpha_1, \alpha_2, \alpha_3\}$.

Sea $K' \rightarrow K''$ una extensión de Galois y H un subgrupo de $Gal(K' \rightarrow K'')$. Denotemos con

$$(K'')^H = \{a \in K'' \mid \alpha(a) = a, \text{ para toda } \alpha \in H\}.$$

Entonces $(K'')^H$ es un subcampo de K'' que contiene a K' pues si $a, b \in (K'')^H$ y $\alpha \in H$, $\alpha(a + b) = \alpha(a) + \alpha(b) = a + b$, $\alpha(ab) = \alpha(a)\alpha(b) = ab$, $\alpha(a^{-1}) = \alpha(a)^{-1}$ si $a \neq 0$ y si $c \in K'$, entonces $\alpha(c) = c$, es decir $K' \leq (K'')^H$. Llamaremos a $(K'')^H$ **subcampo fijo de H** . Si H denota una familia $\{\varphi_i\}$ de automorfismos de K'' que dejan fijo a K' , denotamos con $(K'')^{\{\varphi_i\}}$ al subcampo fijo de la familia $\{\varphi_i\}$.

3.4 Ejemplo. Considere la extensión $\mathbb{Q} \rightarrow \mathbb{Q}(\sqrt{2})$ y el polinomio $m_{\sqrt{2}, \mathbb{Q}}(t) = t^2 - 2$. Sus raíces son $-\sqrt{2}$ y $\sqrt{2}$ y son conjugadas sobre \mathbb{Q} . Como vimos en el Ejemplo 2.17, $\varphi_{\sqrt{2}, -\sqrt{2}} : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$ dada por $a + b\sqrt{2} \mapsto \varphi_{\sqrt{2}, -\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2}$ es un automorfismo de $\mathbb{Q}(\sqrt{2})$. Pero $a + b\sqrt{2} = a - b\sqrt{2}$ cuando $b = 0$. Luego, el subcampo fijo de $\{\varphi_{\sqrt{2}, -\sqrt{2}}\}$ es $\mathbb{Q}(\sqrt{2})^{\{\varphi_{\sqrt{2}, -\sqrt{2}}\}} = \mathbb{Q}$.

Por el Problema 2.7, si $K' \rightarrow K''$ es una extensión de Galois entonces las extensiones $K' \rightarrow (K'')^H$ y $(K'')^H \rightarrow K''$ son separables y también $(K'')^H \rightarrow K''$ es normal y por lo tanto es una extensión de Galois. Recuerde que $|Gal((K'')^H \rightarrow K'')| = \{(K'')^H \rightarrow K''\} = [(K'')^H \rightarrow K'']$. Todo automorfismo de $Gal((K'')^H \rightarrow K'')$ es un automorfismo de $Gal(K' \rightarrow K'')$, luego $Gal((K'')^H \rightarrow K'')$ es un subgrupo de $Gal(K' \rightarrow K'')$. Observe que, por definición, $H \leq Gal((K'')^H \rightarrow K'')$ y por el Teorema de Lagrange, $o(H) \mid o(Gal((K'')^H \rightarrow K''))$.

3.5 Proposición. Si H es un subgrupo de $Gal(K' \rightarrow K'')$ entonces $Gal((K'')^H \rightarrow K'') = H$.

Demostración. Como la extensión $(K'')^H \rightarrow K''$ es separable, por el teorema 2.23, es una extensión simple, es decir, $K'' = (K'')^H(a)$. Considere los distintos elementos de $H = \{1_H = \beta_1, \beta_2, \dots, \beta_n\}$. Considere el polinomio de grado n

$$f(t) = (t - a)(t - \beta_2(a)) \cdots (t - \beta_n(a)) \in K''[t].$$

Observe que $f(t)$ no cambia al aplicar β_j a sus coeficientes puesto que las raíces $\beta_k(a)$ son permutadas por β_j . Por lo tanto, $f(t) \in (K'')^H[t]$. Así,

$[(K'')^H \twoheadrightarrow K''] = [(K'')^H \twoheadrightarrow ((K'')^H)(a)] \leq n = o(H)$. Por otro lado, como $H \leq (Gal((K'')^H \twoheadrightarrow K''))$, tenemos que $n = o(H) \leq o(Gal((K'')^H \twoheadrightarrow K'')) = [(K'')^H \twoheadrightarrow K'']$. Por las dos desigualdades anteriores se tiene que $o(H) = n = o(Gal((K'')^H \twoheadrightarrow K'')) = [(K'')^H \twoheadrightarrow K'']$ y por lo tanto $Gal((K'')^H \twoheadrightarrow K'') = H \blacklozenge$

Sea $K' \twoheadrightarrow K''$ una extensión de Galois y $(K' \twoheadrightarrow K) \leq (K' \twoheadrightarrow K'')$. Entonces la extensión $K \twoheadrightarrow K''$ también es de Galois cuyo grupo de Galois lo denotamos $Gal(K \twoheadrightarrow K'')$.

3.6 Definición. El grupo de Galois $Gal(K \twoheadrightarrow K'')$ anterior se llamará **grupo de Galois relativo de las extensiones** $(K' \twoheadrightarrow K)$ y $(K' \twoheadrightarrow K'')$.

3.7 Proposición. Considere $(K' \twoheadrightarrow K) \leq (K' \twoheadrightarrow K'')$. Entonces $(K'')^{Gal(K \twoheadrightarrow K'')} = K$.

Demostración. Es claro que $K \leq (K'')^{Gal(K \twoheadrightarrow K'')}$. Por otro lado, sea $a \in K'' - K$. Por el Problema 3.3, existe un automorfismo $\sigma \in Gal(K \twoheadrightarrow K'')$ tal que $\sigma(a) \neq a$ y por lo tanto $a \notin (K'')^{Gal(K \twoheadrightarrow K'')}$. Así, $(K'')^{Gal(K \twoheadrightarrow K'')} \leq K$. Por lo tanto, $(K'')^{Gal(K \twoheadrightarrow K'')} = K \blacklozenge$

Consideremos una extensión de Galois finita $K' \twoheadrightarrow K''$. Denotemos con $Subgr(K' \twoheadrightarrow K'')$ el conjunto de todos los subgrupos de $Gal(K' \twoheadrightarrow K'')$ y $Subext(K' \twoheadrightarrow K'')$ el conjunto de todas las subextensiones $K' \twoheadrightarrow K$ de $K' \twoheadrightarrow K''$, es decir, donde K es un campo intermedio $K' \leq K \leq K''$. Ordenemos estos conjuntos por inclusiones. Claramente $Subgr(K' \twoheadrightarrow K'')$ es un conjunto finito.

Los siguientes resultados constituyen los principales de la Teoría de Galois.

3.8 Teorema . Sea $K' \twoheadrightarrow K''$ una extensión de Galois finita. Definamos las siguientes funciones

$$\begin{aligned} g : Subgr(K' \twoheadrightarrow K'') &\longrightarrow Subext(K' \twoheadrightarrow K'') \text{ dada por} \\ H &\longmapsto g(H) = ((K'')^H \twoheadrightarrow K'') \end{aligned}$$

y

$$\begin{aligned} f : Subext(K' \twoheadrightarrow K'') &\longrightarrow Subgr(K' \twoheadrightarrow K'') \text{ dada por} \\ (K' \twoheadrightarrow K'') &\longmapsto f(K' \twoheadrightarrow K'') = Gal(K' \twoheadrightarrow K'') \end{aligned}$$

Entonces las funciones f y g son biyecciones mutuamente inversas que preservan el orden de contención inverso.

Demostración. Utilizando los resultados anteriores, considere las composiciones siguientes

$$\begin{array}{ccc} \text{Subgr}(K' \twoheadrightarrow K'') & \xrightarrow{g} \text{Subext}(K' \twoheadrightarrow K'') \xrightarrow{f} & \text{Subgr}(K' \twoheadrightarrow K'') \\ & & f(g(H)) = \\ H \longmapsto & g(H) = ((K'')^H \twoheadrightarrow K'') \longmapsto & = f((K'')^H \twoheadrightarrow K'') \\ & & = \text{Gal}((K'')^H \twoheadrightarrow K'') \\ & & = H \end{array}$$

$$\begin{array}{ccc} \text{Subext}(K' \twoheadrightarrow K'') & \xrightarrow{f} \text{Subgr}(K' \twoheadrightarrow K'') \xrightarrow{g} & \text{Subext}(K' \twoheadrightarrow K'') \\ & & f(K' \twoheadrightarrow K) \\ (K' \twoheadrightarrow K) \longmapsto & \parallel \longmapsto & (K'')^{\text{Gal}(K' \twoheadrightarrow K)} \twoheadrightarrow K'' = \\ & \text{Gal}(K' \twoheadrightarrow K) & = (K' \twoheadrightarrow K) \end{array}$$

i.e., $f \circ g = 1_{\text{Subgr}(K' \twoheadrightarrow K'')}$ y $g \circ f = 1_{\text{Subext}(K' \twoheadrightarrow K'')}$. Luego, f y g son inversos uno del otro. Si H_1 y H_2 son elementos del conjunto $\text{Subgr}(K' \twoheadrightarrow K'')$ tal que $H_1 \leq H_2$ entonces $(K' \twoheadrightarrow (K'')^{H_2}) \leq (K' \twoheadrightarrow (K'')^{H_1})$ pues si $b \in (K'')^{H_2}$ entonces permanece fijo por todo elemento de H_1 pues H_1 es un subconjunto de H_2 . Por lo tanto, g también invierte el orden. También, si $(K' \twoheadrightarrow K_1) \leq (K' \twoheadrightarrow K_2)$ son elementos de $\text{Subext}(K' \twoheadrightarrow K'')$, entonces como $K_1 \leq K_2$, $\text{Gal}(K_2 \twoheadrightarrow K'') \leq \text{Gal}(K_1 \twoheadrightarrow K'')$ y si $\sigma \in \text{Gal}(K_2 \twoheadrightarrow K'')$ entonces σ fija todo elemento de K_1 . Por lo tanto $f(K' \twoheadrightarrow K_2) \leq f(K' \twoheadrightarrow K_1)$ y f invierte el orden de contención. ♦

Es de mencionarse que este fenómeno no se estudia solamente en la Teoría de Galois, sino en general en la Teoría de Conjuntos Parcialmente Ordenados. Tal par de biyecciones son, de hecho, funtores y se les conoce como una conexión de Galois. Esto tiene mucha importancia en la Teoría de la Computación y en la Teoría Matemática de la Música.

3.9 Proposición. Sea $K' \twoheadrightarrow K''$ una extensión de Galois y $(K' \twoheadrightarrow K) \leq (K' \twoheadrightarrow K'')$. Entonces el grupo de Galois relativo $\text{Gal}(K \twoheadrightarrow K'')$ de las extensiones $(K' \twoheadrightarrow K)$ y $(K' \twoheadrightarrow K'')$ es un subgrupo normal de $\text{Gal}(K' \twoheadrightarrow K'')$ si, y sólo si $(K' \twoheadrightarrow K)$ es una extensión normal.

Demostración. Supongamos que $\text{Gal}(K \twoheadrightarrow K'') \triangleleft \text{Gal}(K' \twoheadrightarrow K'')$, es decir, para toda $\alpha \in \text{Gal}(K \twoheadrightarrow K'')$ y $\beta \in \text{Gal}(K' \twoheadrightarrow K'')$ tenemos que

$\beta\alpha\beta^{-1} \in Gal(K \rightarrow K'')$. Si $k \in K$, entonces para cualquier $\kappa \in Gal(K' \rightarrow K'')$ y $\alpha \in Gal(K \rightarrow K'')$, $\kappa(k) \in K''$ satisface $\alpha\kappa(k) = \kappa(\kappa^{-1}\alpha\kappa(k)) = \kappa(k)$ puesto que $\kappa^{-1}\alpha\kappa \in Gal(K \rightarrow K'')$; luego $\kappa(k) \in (K'')^{Gal(K \rightarrow K'')} = K$. Por el Teorema 2.21, todo homomorfismo $K \rightarrow \overline{K'}$ que deja fijo a K' se extiende a un homomorfismo $K'' \rightarrow \overline{K'}$ el cual debe tener imagen K'' . Por lo tanto, $K' \rightarrow K''$ es una extensión normal.

Ahora supongamos que $K' \rightarrow K''$ es una extensión normal. Entonces, para cada $\alpha \in Gal(K \rightarrow K'')$ y $k \in K$, $\alpha(k) \in K$. También, para cada $\beta \in Gal(K' \rightarrow K'')$, $\beta(\alpha(k)) = \alpha(k)$ y por lo tanto $\alpha^{-1}\beta\alpha(k) = k$. Así que $\alpha^{-1}\beta\alpha \in Gal(K \rightarrow K'')$. Luego, para toda $\alpha \in Gal(K' \rightarrow K'')$, $\alpha Gal(K \rightarrow K'')\alpha^{-1} = Gal(K \rightarrow K'')$ y por lo tanto $Gal(K \rightarrow K'') \triangleleft Gal(K' \rightarrow K'')$. ♦

3.10 Proposición. Sea $K' \rightarrow K$ una extensión de Galois. Entonces existe un isomorfismo de grupos

$$Gal(K' \rightarrow K'')/Gal(K \rightarrow K'') \cong Gal(K' \rightarrow K)$$

dado por $\alpha Gal(K \rightarrow K'') \mapsto \alpha|_K$.

Demostración. Como $K' \rightarrow K$ es una extensión normal, si $\alpha \in Gal(K' \rightarrow K'')$ entonces $\alpha K = K$. Así es que podemos restringir α a un automorfismo de K , $\alpha|_K : K \rightarrow K$. Entonces $\alpha|_K$ es la identidad en K sí, y sólo si, $\alpha \in Gal(K \rightarrow K'')$. Es inmediato comprobar que la función

$$\begin{aligned} Gal(K' \rightarrow K'') &\longrightarrow Gal(K' \rightarrow K) \\ \alpha &\longmapsto \alpha|_K \end{aligned}$$

es un homomorfismo de grupos con núcleo $Gal(K \rightarrow K'')$. Así que obtenemos un monomorfismo

$$Gal(K' \rightarrow K'')/Gal(K \rightarrow K'') \rightarrow Gal(K' \rightarrow K)$$

tal que

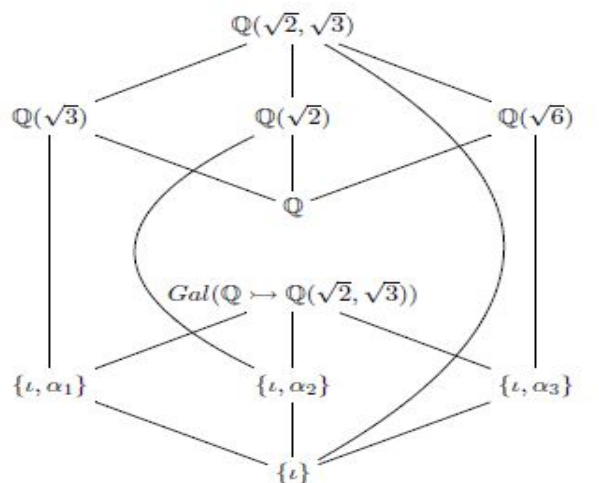
$$\begin{aligned} o(Gal(K' \rightarrow K'')/Gal(K \rightarrow K'')) &= [K' \rightarrow K'']/[K \rightarrow K''] \\ &= [K' \rightarrow K] = o(Gal(K' \rightarrow K)) \end{aligned}$$

y por lo tanto es un isomorfismo. ♦

3.11 Ejemplo. El problema 3.1 y el ejemplo 3.3 nos dicen que

$$Gal(\mathbb{Q} \rightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3})) \cong V$$

y que los cuatro automorfismos $\iota, \alpha_1, \alpha_2, \alpha_3$ dejan fijo a \mathbb{Q} . Los diagramas siguientes ilustran la correspondencia de Galois para la extensión $\mathbb{Q} \rightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3})$:



Consideremos una extensión finita $K' \rightarrow K''$ de grado l . Veamos a K'' como espacio vectorial sobre K' . Supongamos que K' tiene q elementos. Luego, cualquier elemento u de K'' puede escribirse en forma única como $u = \lambda_1 v_1 + \dots + \lambda_l v_l$ para $\{\lambda_i\}_{i=1}^l \in K'$ y $\{v_i\}_{i=1}^l$ una base de K'' . Hay q^l expresiones para u pues cada λ_i puede ser cualquiera de los q elementos de K' . Luego K'' tiene q^l elementos.

Observe que si K'' es un campo finito de característica p , entonces se tiene una extensión $K' \rightarrow K''$ donde $K' \cong \mathbb{Z}_p$. Luego K'' tiene p^l elementos, para l un entero positivo, es decir, $|K''| = p^{[\mathbb{Z}_p \rightarrow K'']}$.

Ahora, si consideramos el grupo multiplicativo $(K'')^*$ de los elementos distintos de cero de K'' , recordemos que tiene orden $p^l - 1$. Si tomamos un elemento $a \in K''$, el orden de a , $o(a) | o((K'')^*) = p^l - 1$. Luego $a^{p^l - 1} = 1$ y $a^{p^l} = a$. Por lo tanto, cualquier elemento de K'' es raíz del polinomio $t^{p^l} - t$, el cual tiene a lo más p^l raíces. Así, si K'' está contenido en $\overline{\mathbb{Z}_p}$, los elementos de K'' son las raíces en $\overline{\mathbb{Z}_p}$ del polinomio $t^{p^l} - t \in \mathbb{Z}_p[t]$.

Considere el polinomio $f(t) = t^{p^l} - t \in \mathbb{Z}_p[t]$. Su derivada es $f'(t) = p^l t^{p^l - 1} - 1 = -1$. Por el problema 3.4 todas las raíces de $f(t)$ en $\overline{\mathbb{Z}_p}$ son simples. Luego, f posee p^l raíces distintas en $\overline{\mathbb{Z}_p}$. Si $\{0, a_1, \dots, a_{p^l - 1}\}$ son las

distintas raíces, entonces en $\overline{\mathbb{Z}_p}[t]$, $t^{p^l} - t = t(t - a_1) \cdots (t - a_{p^l-1})$ y cada raíz es simple sobre \mathbb{Z}_p .

Denotemos con $\mathbb{F}_{p^l} = \{a \in \overline{\mathbb{Z}_p} \mid f(a) = 0\} \subseteq \overline{\mathbb{Z}_p}$.

3.12 Teorema. \mathbb{F}_{p^l} es un subcampo de $\overline{\mathbb{Z}_p}$ con p^l elementos, $l \geq 1$.

Demostración. Si $a, b \in \mathbb{F}_{p^l}$ entonces $(a + b)^{p^l} - (a + b) = (a^{p^l} + b^{p^l}) - (a + b) = (a^{p^l} - a) + (b^{p^l} - b) = 0$ y $(ab)^{p^l} - (ab) = (a^{p^l} b^{p^l}) - (ab) = ab - ab = 0$. Claramente 0,1 son raíces de $t^{p^l} - t$. Si $a \neq 0$, $a^{p^l} = a$ y $(1/a)^{p^l} = 1/a$. Por lo tanto, \mathbb{F}_{p^l} es un subcampo de $\overline{\mathbb{Z}_p}$. ♦

Observe que $\mathbb{Z}_p \leq \mathbb{F}_{p^l}$ y que $\mathbb{Z}_p \hookrightarrow \mathbb{F}_{p^l}$ es una extensión finita. El subcampo \mathbb{F}_{p^l} se llama **campo de Galois** de orden p^l . Se acostumbra denotar a \mathbb{Z}_p con \mathbb{F}_p . También se usa la notación $GF(p^l)$ para \mathbb{F}_{p^l} en la literatura sobre este tema. Es claro que $[\mathbb{F}_p \hookrightarrow \mathbb{F}_{p^l}] = l$.

Problemas

3.1 Compruebe que $Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3})) = Gal(\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3})) \cong V$ (el grupo 4 de Klein).

3.2 Pruebe que el grupo de Galois $Gal(K \hookrightarrow K'')$ relativo de las extensiones $(K' \hookrightarrow K)$ y $(K' \hookrightarrow K'')$ es un subgrupo de $Gal(K' \hookrightarrow K'')$, es decir, $Gal(K \hookrightarrow K'') \leq Gal(K' \hookrightarrow K'')$ cuyo orden $o(Gal(K \hookrightarrow K'')) = [K' \hookrightarrow K'']$.

3.3 Recuerde que [A-D-Ll-M p.107] una acción de un grupo G en un conjunto X es **transitiva** si para cualesquiera $x, y \in X$ existe $g \in G$ tal que $gx = y$. También decimos que la acción es **libre** si solamente para $g = e \in G$ se tiene que $gx = x$, de otra manera, si para cuando $g \neq e \in G$, $gx \neq x$. Pruebe que si $K' \hookrightarrow K''$ es una extensión de Galois finita donde K'' es el campo de descomposición de un polinomio irreducible $f \in K'[t]$ de grado n entonces el grupo $Gal(K' \hookrightarrow K'')$ actúa transitiva y libremente en $R(f, K'')$.

3.4 Considere el anillo de polinomios $K[t]$ para un campo K . Se define la **derivada** $\partial : K[t] \rightarrow K[t]$ dada por $\partial(f(t)) = \partial(\lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0) = n\lambda_n t^{n-1} + \cdots + 2\lambda_2 t^1 + \lambda_1 = f'(t)$; $\lambda_i \in K$. Pruebe que si $f \in K[t]$ posee una raíz $a \in K''$ para una extensión $K \hookrightarrow K''$, entonces a es una raíz

múltiple de f si, y sólo si, f y f' poseen un factor lineal común en $K[t]$ que se anula en a .

3.5 Pruebe el teorema del elemento primitivo para el caso en que K'' sea finito.

3.6 Pruebe que $\mathbb{F}_{p^l} \leq \overline{\mathbb{F}_p}$ es el subcampo de descomposición para los polinomios $t^{p^l} - t$ y $t^{p^l-1} - 1$ sobre \mathbb{F}_p .

3.7 Pruebe que \mathbb{F}_{p^l} es el único subcampo (salvo isomorfismo) con p^l elementos.

3.8 Considere \mathbb{F}_{p^k} y \mathbb{F}_{p^l} dos campos de Galois de característica p . Pruebe que \mathbb{F}_{p^k} es subcampo de \mathbb{F}_{p^l} si, y sólo si, k divide a l .

3.9 Dibuje un diagrama de los subcampos de $\mathbb{F}_{p^{60}}$ ordenados via la divisibilidad por $l = 60$.

Bibliografía y Referencias

[A] Armstrong, M.A. Groups and Symmetry. UTM. Springer. 1988.

[Am] Amiot, E. Rhythmic Canons and Galois Theory. H. Friepertinger, L. Reich (Eds.). Colloquium on Mathematical Music Theory. Grazer Math. Ber. Bericht Nr. 347. (2005).

[A-D-LI-M] Agustín-Aquino, O., du Plessis, J., Lluís-Puebla, E., Montiel, M. Una introducción a la Teoría de Grupos con aplicaciones en la Teoría Matemática de la Música. Pub. Electr. Sociedad Matemática Mexicana. Serie textos. Vol. 10 (2009).

[A-LI1] Aceff, F., Lluís-Puebla, E. Matemática en la Matemática, Música, Medicina y Aeronáutica. Pub. Electr. Sociedad Matemática Mexicana. Serie Divulgación. Vol. 1 (2006).

[A-LI2] Aceff, F., Lluís-Puebla, E. Matemática en la Matemática II, Música II, Naturaleza y Nuestro Cuerpo. Pub. Electr. Sociedad Matemática Mexicana. Serie Divulgación. Vol. 2 (2007).

Artin E. Galois Theory. (1944 Segunda Ed.) Dover. (1998).

Baker, A. An Introduction to Galois Theory. www.maths.gla.ac.uk/~ajb/dvi-ps/Galois.pdf (2007).

Bewersdorff, J. Galois Theory for Beginners. Student Math. Library. Vol. 35. American Mathematical Society. (2006).

[B-M] Birkhoff, G. MacLane, S. Algebra. Macmillan. 1968.

Birkhoff, G. MacLane, S. Algebra. Macmillan. (1968).

- Bourbaki, N. Algebra I. Addison Wesley. (1973).
- [F] Fraleigh, J.B. Abstract Algebra. Seventh Edition. Addison Wesley. (2003).
- Hu, S-T. Elements of Modern Algebra. Holden-Day. (1965).
- Hungerford, T.W. Algebra. Springer. (1980).
- Lang, S. Algebra. Addison Wesley. (1965).
- [L] Larrea-Schiavon, M. Los subgrupos de los p -subgrupos de Sylow de S_{p^2} . Tesis de licenciatura bajo la dirección de E. Lluís-Puebla. Facultad de Ciencias, UNAM. (2011).
- [L1] Lluís-Puebla, E. Álgebra Homológica. Addison Wesley Ib. (1990).
- [L12] Lluís-Puebla, E. Álgebra Lineal. Sitesa. (1997).
- [Ll-M-N] Lluís-Puebla, E., Mazzola, G. and Noll, T. (Eds.). Perspectives in Mathematical and Computational Music Theory. EpOs, 149–164, Universität Osnabrück. (2004).
- [M] Mazzola, G. Notas sobre la demostración de los Teoremas de Sylow. (Comunicación personal).
- Milne, J.S. Fields and Galois Theory. www.jmilne.org/math/CourseNotes/ft.html. (2003).
- Morandi, P. Field and Galois Theory. Graduate Texts in Mathematics Vol. 167. Springer. (1996).
- Robinson, J.S. A Course in the Theory of Groups. Springer. 1980.
- Rotman, J.J. Galois Theory. Second Edition. Universitext, Springer. (2001).
- Rotman, J.J. The Theory of groups. Allyn and Bacon. 1976.
- Rotman, J.J. An Introduction to the Theory of Groups, Spriger, Cuarta Edición (1994).
- Snaith, V.P. Groups, Rings and Galois Theory. World Scientific. (2003).
- Stewart, I. Galois Theory. Chapman & Hall. (2004).

Lista de Símbolos

\mathbb{Z} ,	15	\cong ,	31
\mathbb{Z}_3 ,	17	$\ker f$	31
$f : A \rightarrow B$	15	$\text{im } f$,	32
Δ_3 ,	19	\hookrightarrow ,	32
xfy ,	20	\twoheadrightarrow ,	32
$j : G^n = G \times \dots \times G \rightarrow G$,	20	$H < G$,	32
S_n ,	21	$\text{Hom}(X, Y)$,	34
$(V, +, \mu)$,	22	ψ_*	34
$(G, +)$,	28	φ^*	34
$+: G \times G \rightarrow G$,	22	V ,	35
$+(u, v)$,	22	D_n ,	35
$O \in G$,	22	1_G	35
$-v$	23	O_G	35
$(E, +)$	23	$\text{Hom}(G, G')$,	36
$(S, +)$	23	(x) ,	39
$(M, +)$	23	$\dots \longrightarrow G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i}$	
$o(G)$,	23	$G_{i+1} \xrightarrow{f_{i+1}} \dots$,	43
$ G $,	23	O	43
$(\Lambda, +, \cdot)$,	24	$e \longrightarrow G' \xrightarrow{f} G \xrightarrow{g} G'' \longrightarrow e$	44
$(A, +, \mu, \cdot)$,	26	$G' \xrightarrow{f} G \xrightarrow{g} G''$	
$T^k(V)$,	26	$\{C_n\}_{n \in \mathbb{Z}}$,	47,48
TV ,	27	G/H ,	49
$\bigwedge^k V$,	27	p	70
$\bigwedge V$,	27	$x \equiv_i y \pmod{H}$	50
e	29	$x \equiv_d y \pmod{H}$	50
$f : G \xrightarrow{\cong} G'$	31	xH	51
f^{-1}	31	Hx	51

$H \triangleleft G$,	51	(L, f) ,	85
$(G : H)$,	53	(T, f) ,	92
$H_n(C)$,	55	$(X R)$,	88
C_n	55	$X \otimes Y$,	93
∂_n	55	1	112
$Z_n(C)$	55	${}^\circ\Lambda$	112
$B_n(C)$	55	$\Gamma < \Lambda$	112
$[c]$	55	$\ker f$	115
$H_*(C)$	55	$f : \Lambda \xrightarrow{\cong} \Lambda'$	31
$H^n(C)$,	56	$\Lambda \cong \Lambda'$	115
g^*	57	$\text{im } f$	115
HN ,	60	$f : \Lambda \twoheadrightarrow \Lambda'$	32
$\text{Aut}(G)$,	62	$f : \Lambda \rightarrow \Lambda'$	32
$\text{In}(G)$,	62	ι	115
$\text{coim } g$,	63	$\text{End}(G, G)$	116
$\text{co ker } g$,	63	f^{-1}	117
$\prod_{i \in I} G_i$,	64	$\text{car } (\Lambda) = 0$	120
$\bigoplus_{i \in I} G_i$,	64	$\text{car } (\Lambda) = n$	120
$G_1 \times G_2$,	64	$x + I$	121
$\prod_{i \in I}^d G_i$,	66	Λ/I	122
$\sum_{i \in I} G_i$,	66	(Π, f, t)	127
ι_i	70	f_x	128
p_j	70	$\Lambda[t]$	129
$\beta_n(C)$	74	$\text{gr } (\varphi)$	129
$\chi(C)$,	74	E_a	129
(i_1, i_2, \dots, i_r) ,	76	f^\circledast	129
$h x h^{-1}$,	78	$\langle S \rangle$	130
G_x ,	78	$\langle t_1, \dots, t_n \rangle$	130
G_x ,	78	Ξ	132
$C_H(x)$,	79	(K, f)	132
$C_G(x)$,	79	$t^n - 1 = \prod_{d n} \Phi_d(t)$	137
$N_H(K)$,	79	$K' \twoheadrightarrow K$	140
$N_G(K)$,	79	$K' \leq K$	140
$h K h^{-1}$,	83	$K : K'$	140
$\text{sg}(\sigma)$,	83	$K' < K$	140
A_n ,	84	K	
			140
		K'	

$(K' \twoheadrightarrow K) \leq (K' \twoheadrightarrow K'')$	141	$Aut_{K'}(K'', K'')$	153
$[K' \twoheadrightarrow K]$	141	$R(f, K'')$	153
$K'(X)$	144	$\{K' \twoheadrightarrow K''\}$	155
$K'(a_1, \dots, a_j)$	144	$Gal(K' \twoheadrightarrow K'')$	160
$K' \twoheadrightarrow K'(a_1, \dots, a_j)$	144	$(K'')^H$	161
$gr(a, K')$	147	$(K'')^{\{\varphi_i\}}$	161
$\frac{K'_K}{K'}$	149	$Subgr(K' \twoheadrightarrow K'')$	162
$Aut(\Lambda)$	151	$Subext(K' \twoheadrightarrow K'')$	162
$Aut_\Gamma(\Lambda)$	151	\mathbb{F}_p	166
K'_f	152	$GF(p^l)$	166
$hom_{K'}(K, K'')$	153	∂	166

Índice Analítico

A			
acción	24	exteriores	62
libre	166	B	
transitiva	166	base	
alfabeto	85	de un ideal	130
álgebra	26	del grupo abeliano libre	89
asociativa	26	C	
con división	26	cadena	47
con uno	26	cadena	
conmutativa	26	de grado n	55
de Grassmann	27	campo	25,112
exterior	27	base de la extensión	140
graduada	26	de cocientes	
tensorial	27	con s indeterminadas	133
anillo	24,111	de un dominio entero	132
con división	25,112	de descomposición	152
con identidad,	25	de funciones racionales	
con uno	25,112	con s indeterminadas	133
conmutativo	25,111	de Galois	166
de polinomios	127	intermedio	142
local	180	campos	
opuesto	112	primos	134
automorfismo	32,57,115,151	característica 0	
de un anillo sobre un subanillo	151	anillo de	120
interior	57	característica	
automorfismos		de un anillo	120
de Galois	160	Euler-Poincaré, de	74
		Cayley	82

centralizador	79	D	
cero		derivada	166
de un polinomio	130	diferenciales	55
divisores de	25	divisores de cero	25,112
cerradura algebraica	149	dominio	
ciclo de longitud r	76	de ideales principales	130
ciclos de grado n	55	de una función	16
clase		entero	25,112
conjugada	79	E	
de homología	55	ecuación	
clases laterales	51	de clases conjugadas	82
cocadena	48	elemento	
codominio		algebraico	146
de una función	16	conjugado	78
coeficiente inicial	129	de orden infinito	39
coeficientes		idempotente	36
de torsión	72	identidad	22
de torsión de grado n	74	identidad de un grupo	29
del polinomio	129	identidad derecho	29
coimagen	63	identidad izquierdo	29
combinaciones lineales	130	inverso	23
complejo		invertible	119
de cadenas	47	invertible por la derecha	119
de cocadenas	48	invertible por la izquierda	119
composición		nilpotente	182
de x y y	20	orden de un	39
ley de	16	primitivo	157
conúcleo	63	separable	155
congruente		trascendente	147
por la derecha	50	elementos	
por la izquierda	50	conjugados	154
conjugación	78	homólogos	55
conjunto		endomorfismo	32,115
cerrado	20	epimorfismo	32,115
estable	20	espacio	
conmutador	56	tensorial de grado k	27
constantes	129	vectorial	22
criterio de Einstein	134	estabilizador	78

estructura algebraica	20	de separabilidad de una	
extensión		extensión	155
algebraica	147	de un elemento	129
de Galois	160	grupo	22,28
de K' en K	140	abeliano	28
de un campo	139	abeliano libre	89
finita	142	abeliano libre generado por X	89
separable	155	alternante de grado n	84
finitamente generada	144	cíclico	
generada	144	de orden n	39
infinita	142	generado por	39
normal	156	cociente	49,121
simple	144	con operadores	24
trascendente	147	conmutativo	23,28
extensiones		de cohomología de grado n	56
isomorfas	141	de Galois	
F		relativo a las extensiones	162
fronteras		de Galois de una extensión	160
de grado n	55	de homología de grado n	55
función	15	de Klein	35
biaditiva	37	diedro	35
biaditiva universal	94	elemento identidad de un	29
codominio de una	16	libre	
dominio de una	16	en el conjunto X	85
imagen de una	16	generado por los elementos de	
polinomial	130	X	87
se extiende	89	simple	53
G		grupoide	23
G actúa por la izquierda	77	H	
G -conjunto	77	homología	
generador		de la cadena	55
de subgrupo cíclico	39	homomorfismo	
generadores		de anillos	25,114
de G	88	de evaluación	129
de un ideal	130	de grupos	24,30
grado		de identidad	116
de a sobre K	147	de Λ -módulos	25
de K sobre K	141	de sustitución	129

identidad	35	finitamente generado	26
inducido por g en los grupos		izquierdo	25
cociente	57	libre	26
inducido por ψ	34	proyectivo	26
inducido por φ	34	ley de composición	16
trivial	32,35,115	ley distributiva	111
I		M	
ideal	113	magma	23
derecho	113	monoide	23
finitamente generado	130	monomorfismo	32,115
generado por	130	morfismo	
izquierdo	113	cero	43
máximo	131	de cadenas	47
primo	131	de cocadenas	48
principal	130	trivial	43
ideales		multiplicidad	
propios no triviales	113	de una raíz	159
triviales	113	N	
identidad		núcleo de f	31
derecha	29	número	
izquierda	29	algebraico	147
imagen		de Betti	74
de una función	16,32	trascendente	147
inclusión	115	normalizador	79
indeterminada	128	O	
índice		operación	
de H en G	53	binaria	16,22
inverso		inducida	20
de un elemento	23,29	nula	20
de una función	31	operaciones	20
derecho	119	operador	24
izquierdo	119	operadores	
inyección canónica	69	frontera	55
isomorfismo		órbita	78
de anillos	115	órbitas de σ	76
de grupos	31	orden	
L		de un elemento	39
Λ -módulo		de un grupo	23

<i>Índice Analítico</i>		179
grupo cíclico de	39	de la unidad 137
P		raíz
p-grupo	102	de multiplicidad n 159
p-subgrupo de Sylow	102	de un polinomio 130
palabra reducida	85	rango
palabras	85	de un grupo abeliano libre 90
permutación		regla de conmutación 105
impar	84	relaciones que definen a G 88
par	84	S
signo, de una	83	Segundo Teorema de Isomorfismo 61
permutaciones		semigrupo 23
de n elementos	21	signo de una permutación 83
polinomio		sistema algebraico 20
en la indeterminada t	129	subanillo 112
mínimo	147	generado 130
separable	155	generado por S 120
polinomios		subcampo 112
ciclotómicos	137	fijo 161
presentación	88	generado por 120
presentaciones		obtenido por adjunción 144
isomorfas	88	subdominio 112
Primer Teorema de Isomorfismo	59	generado por 120
producto		subextensión de campos 141
de grupos	64	subgrupo 32
de subgrupos	60	cíclico 39
directo externo	64	generador de 39
directo externo débil	66	infinito 39
exterior	27	conjugado 83
tensorial	92	de isotropía 78
propiedad universal		normal 51
producto directo, del	66	trivial 33
proyección		subgrupos
canónica	50,51,70,122	impropios 33
natural	51	propios 33
proyecciones	65	sucesión
R		exacta 44
r-ciclo	76	exacta corta 44
raíces		semiexacta 43

suma directa		de Isomorfismo, Tercer	61,125
completa	64	de la órbita-estabilizador	80
externa	66	de Lagrange	53
T		del elemento primitivo	157
término constante	129	Kronecker	146
Teorema		Teoremas de Sylow	106
Cauchy para Grupos Abelianos		Tercer Teorema de Isomorfismo	61
Finitos	54	translación	78
Cauchy, de	102	transposición	76
de Isomorfismo, Primer	59	U	
de isomorfismo, Primer	124	unidad	119
de Isomorfismo, Segundo	61,125		