Introducción al Álgebra

ISBN: 978-956-306-062-1
Registro de Propiedad Intelectual: 200.534
Colección: Herramientas para la formación de profesores de matemáticas.
Diseño: Jessica Jure de la Cerda.
Diseño de Ilustraciones: Cristina Felmer Plominsky, Catalina Frávega Thomas.
Diagramación: Pedro Montealegre Barba, Francisco Santibáñez Palma.
Financiamiento: Proyecto Fondef D05I-10211.

Datos de contacto para la adquisición de los libros:
Para Chile:
1. En librerías para clientes directos.
2. Instituciones privadas directamente con:
   Juan Carlos Sáez C.
   Director Gerente
   Comunicaciones Noreste Ltda.
   J.C. Sáez Editor
   jcsaezc@vtr.net
   www.jcsaezeditor.blogspot.com
   Oficina: (56 2) 3260104 - (56 2) 3253148
3. Instituciones públicas o fiscales: www.chilecompra.cl

Desde el extranjero:
1. Liberalia Ediciones: www.liberalia.cl
2. Librería Antártica: www.antartica.cl
3. Argentina: Ediciones Manantial: www.emanantial.com.ar
4. Colombia: Editorial Siglo del Hombre
   Fono: (571) 3377700
5. España: Tarahumara, tarahumara@tarahumaralibros.com
   Fono: (34 91) 3656221
6. México: Alejandría Distribución Bibliográfica, alejandria@alejandrialibros.com.mx
   Fono: (52 5) 556161319 - (52 5) 6167509
7. Perú: Librería La Familia, Avenida República de Chile # 661
8. Uruguay: Dolmen Ediciones del Uruguay
   Fono: 00-598-2-7124857

Introducción al Álgebra — Renato Lewin
Facultad de Matemáticas, Pontificia Universidad Católica de Chile
rlewin@mat.puc.cl

ESTA PRIMERA EDICIÓN DE 2.000 EJEMPLARES
Se terminó de imprimir en febrero de 2011 en WORLDCOLOR CHILE S.A.

INTRODUCCIÓN AL ÁLGEBRA

Renato Lewin

Pontificia Universidad Católica de Chile

Dirección del Proyecto Fondef D05I-10211
Herramientas para la Formación de Profesores de Matemática

Patricio Felmer, Director del Proyecto
Universidad de Chile.

Leonor Varas, Directora Adjunta del Proyecto
Universidad de Chile.

Salomé Martínez, Subdirectora de Monografías
Universidad de Chile.

Cristián Reyes, Subdirector de Estudio de Casos
Universidad de Chile.

Presentación de la Colección

La colección de monografías que presentamos es el resultado del generoso esfuerzo de los autores, quienes han dedicado su tiempo y conocimiento a la tarea de escribir un texto de matemática. Pero este esfuerzo y generosidad no se encuentra plenamente representado en esta labor, sino que también en la enorme capacidad de aprendizaje que debieron mostrar, para entender y comprender las motivaciones y necesidades de los lectores: Futuros profesores de matemática.

Los autores, encantados una y otra vez por la matemática, sus abstracciones y aplicaciones, enfrentaron la tarea de buscar la mejor manera de traspasar ese encanto a un futuro profesor de matemática. Éste también se encanta y vibra con la matemática, pero además se apasiona con la posibilidad de explicarla, enseñarla y entregarla a los jóvenes estudiantes secundarios. Si la tarea parecía fácil en un comienzo, esta segunda dimensión puso al autor, matemático de profesión, un tremendo desafío. Tuvo que salir de su oficina a escuchar a los estudiantes de pedagogía, a los profesores, a los formadores de profesores y a sus pares. Tuvo que recibir críticas, someterse a la opinión de otros y reescribir una y otra vez su texto. Capítulos enteros resultaban inadecuados, el orden de los contenidos y de los ejemplos era inapropiado, se hacía necesario escribir una nueva versión y otra más. Conversaron con otros autores, escucharon sus opiniones, sostuvieron reuniones con los editores. Escuchar a los estudiantes de pedagogía significó, en muchos casos, realizar eventos de acercamiento, desarrollar cursos en base a la monografía, o formar parte de cursos ya establecidos. Es así que estas monografías recogen la experiencia de los autores y del equipo del proyecto, y también de formadores de profesores y estudiantes de pedagogía. Ellas son el fruto de un esfuerzo consciente y deliberado de acercamiento, de apertura de caminos, de despliegue de puentes entre mundos, muchas veces, separados por falta de comunicación y cuya unión es vital para el progreso de nuestra educación.

La colección de monografías que presentamos comprende una porción importante de los temas que usualmente encontramos en los currículos de formación de profesores de matemática de enseñanza media, pero en ningún caso pretende ser exhaustiva. Del mismo modo, se incorporan temas que sugieren nuevas formas de abordar los contenidos, con énfasis en una matemática más pertinente para el futuro profesor, la que difiere en su enfoque de la matemática para un ingeniero o para un licenciado en matemática, por ejemplo. El formato de monografía, que aborda temas específicos

con extensión moderada, les da flexibilidad para que sean usadas de muy diversas maneras, ya sea como texto de un curso, material complementario, documento básico de un seminario, tema de memoria y también como lectura personal. Su utilidad ciertamente va más allá de las aulas universitarias, pues esta colección puede convertirse en la base de una biblioteca personal del futuro profesor o profesora, puede ser usada como material de consulta por profesores en ejercicio y como texto en cursos de especialización y post-títulos. Esta colección de monografías puede ser usada en concepciones curriculares muy distintas. Es, en suma, una herramienta nueva y valiosa, que a partir de ahora estará a disposición de estudiantes de pedagogía en matemática, formadores de profesores y profesores en ejercicio.

El momento en que esta colección de monografías fue concebida, hace cuatro años, no es casual. Nuestro interés por la creación de herramientas que contribuyan a la formación de profesores de matemática coincide con un acercamiento entre matemáticos y formadores de profesores que ha estado ocurriendo en Chile y en otros lugares del mundo. Nuestra motivación nace a partir de una creciente preocupación en todos los niveles de la sociedad, que ha ido abriendo paso a una demanda social y a un interés nacional por la calidad de la educación, expresada de muy diversas formas. Esta preocupación y nuestro interés encontró eco inmediato en un grupo de matemáticos, inicialmente de la Universidad de Chile, pero que muy rápidamente fue involucrando a matemáticos de la Pontificia Universidad Católica de Chile, de la Universidad de Concepción, de la Universidad Andrés Bello, de la Universidad Federico Santa María, de la Universidad Adolfo Ibáñez, de la Universidad de La Serena y también de la Universidad de la República de Uruguay y de la Universidad de Colorado de Estados Unidos.

La matemática ha adquirido un rol central en la sociedad actual, siendo un pilar fundamental que sustenta el desarrollo en sus diversas expresiones. Constituye el cimiento creciente de todas las disciplinas científicas, de sus aplicaciones en la tecnología y es clave en las habilidades básicas para la vida. Es así que la matemática actualmente se encuentra en el corazón del currículo escolar en el mundo y en particular en Chile. No es posible que un país que pretenda lograr un desarrollo que involucre a toda la sociedad, descuide el cultivo de la matemática o la formación de quienes tienen la misión de traspasar de generación en generación los conocimientos que la sociedad ha acumulado a lo largo de su historia.

Nuestro país vive cambios importantes en educación. Se ha llegado a la convicción que la formación de profesores es la base que nos permitirá generar los cambios cualitativos en calidad que nuestra sociedad ha impuesto. Conscientes de que la tarea formativa de los profesores de matemática y de las futuras generaciones de jóvenes es extremadamente compleja, debido a que confluyen un sinnúmero de factores y disciplinas, a través de esta colección de monografías, sus editores, autores y todos los que han participado del proyecto en cada una de sus etapas, contribuyen a esta tarea, poniendo a disposición una herramienta adicional que ahora debe tomar vida propia en los formadores, estudiantes, futuros profesores y jóvenes de nuestro país.

Patricio Felmer y Salomé Martínez
Editores

Agradecimientos

Agradecemos a todos quienes han hecho posible la realización de este proyecto Fondef: "Herramientas para la formación de Profesores de Matemáticas". A Cristián Cox, quien apoyó con decisión la idea original y contribuyó de manera crucial para obtener la participación del Ministerio de Educación como institución asociada. Agradecemos a Carlos Eugenio Beca por su apoyo durante toda la realización del proyecto. A Rafael Correa, Edgar Kausel y Juan Carlos Sáez, miembros del Comité Directivo. Agradecemos a Rafael Benguria, Servet Martínez y Fidel Oteiza, miembros del Comité Editorial de la colección, quienes realizaron valiosos aportes a los textos. A Guillermo Marshall, Decano de la Facultad de Matemáticas de la Pontificia Universidad Católica de Chile y José Sánchez, entonces Decano de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Concepción, quienes contribuyeron de manera decisiva a lograr la integridad de la colección de 15 monografías. A Jaime San Martín, director del Centro de Modelamiento Matemático por su apoyo durante toda la realización del proyecto. Agradecemos a Víctor Campos, Ejecutivo de Proyectos de Fondef, por su colaboración y ayuda en las distintas etapas del proyecto.

Agradecemos también a Bárbara Ossandón de la Universidad de Santiago, a Jorge Ávila de la Universidad Católica Silva Henríquez, a Víctor Díaz de la Universidad de Magallanes, a Patricio Canelo de la Universidad de Playa Ancha en San Felipe y a Osvaldo Venegas y Silvia Vidal de la Universidad Católica de Temuco, quienes hicieron posible las visitas que realizamos a las carreras de pedagogía en matemática. Agradecemos a todos los evaluadores, alumnos, académicos y profesores -cuyos nombres no incluimos por ser más de una centena- quienes entregaron sugerencias, críticas y comentarios a los autores, que ayudaron a enriquecer cada uno de los textos.

Agradecemos a Marcela Lizana por su impecable aporte en todas las labores administrativas del proyecto, a Aldo Muzio por su colaboración en la etapa de evaluación, y también a Anyel Alfaro por sus contribuciones en la etapa final del proyecto y en la difusión de los logros alcanzados.

Dirección del Proyecto

Índice General

Prefacio

Al revisar la historia de la matemática nos damos cuenta que la introducción de letras, a partir del siglo XV, para representar números y magnitudes arbitrarios y de símbolos para las operaciones o manipulaciones de los mismos, fue el paso decisivo para el desarrollo de la matemática moderna. La geometría analítica y el cálculo son impensables sin estas herramientas que hoy llamamos álgebra.

Por otra parte, en nuestra vida diaria tampoco parece posible resolver sencillos problemas de dinero u otros cálculos prácticos sin contar con una manera expedita de plantear y resolver ciertas ecuaciones. Sin embargo, todos tenemos la experiencia de que el álgebra es considerada un tema abstruso y difícil. Uno de los factores que incide en esta apreciación es que el álgebra elemental es enseñada como un tema independiente y no como lo que es en su origen, una herramienta para resolver problemas que provienen de distintas áreas de la matemática, la aritmética, la geometría, el análisis, etc., e incluso problemas que tienen su origen en otras ciencias: la física, la química, la ingeniería, en donde se aplica la matemática. Si el álgebra se enseña como un problema en sí mismo, para la inmensa mayoría de las personas aparece como un malabarismo incomprensible de símbolos.

Naturalmente en una segunda fase de su aprendizaje el álgebra sí tiene un contenido propio que debe ser aprendido por quienes quieren profundizar en la matemática. En particular, los profesores de matemática, ya sea de enseñanza secundaria o primaria con especialización, deben conocer el entramado más sutil de las estructuras algebraicas que se repiten una y otra vez en diversos ámbitos de la disciplina. Hay aquí un segundo error en la enseñanza del álgebra, esta vez en la universidad. Lo habitual es que los futuros profesores tengan un curso de álgebra abstracta en el que estudian estructuras algebraicas, como grupos, anillos y cuerpos, sin establecer las conexiones entre estos conceptos y la matemática elemental que los futuros profesores deberán enseñar. Es frecuente que los estudiantes de pedagogía consideren que los cursos de introducción al álgebra y de álgebra abstracta tienen un mero alcance de nombres, porque, aparentemente, nada tienen en común.

Este libro trata sobre este segundo nivel en el aprendizaje del álgebra, a saber, el estudio (de algunas) de las estructuras algebraicas que se presentan en la práctica matemática. Ha sido escrito especialmente para alumnos de educación en sus distintos niveles e intenta establecer ese puente entre la matemática elemental

y las abstracciones y generalizaciones que están detrás de ella. Es por eso que tiene ciertas características que, si bien no son originales, lo hacen diferente de otros textos.

La primera característica es el orden de los temas. La mayoría de los libros de álgebra sigue la secuencia grupos, anillos, cuerpos. Hemos comenzado por los anillos por varios motivos. El principal es que estos son la generalización de temas con los que los alumnos están familiarizados: la aritmética de los números, el álgebra de los polinomios, algunos incluso conocen la operatoria de las matrices (aunque este libro pone escaso énfasis en ellas). Los anillos, a diferencia de lo que parecen indicar los textos más estándar, no son una extensión de los grupos abelianos agregando otra operación, esto es sólo una consecuencia de las propiedades de los anillos. Los grupos, en cambio, tienen su origen en el álgebra de las transformaciones o funciones y son por lo tanto objetos mucho más sofisticados conceptualmente, a los que los alumnos han tenido escaso acceso previo. Si este texto tratara el tema de los cuerpos, probablemente éste iría entre los anillos y los grupos, porque algebraicamente los cuerpos sí son una extensión de los anillos.

La segunda característica de este libro es que cada una de las dos estructuras estudiadas es introducida por uno o dos capítulos en los que se presenta en detalle algunos ejemplos paradigmáticos de ellas. Estos capítulos, además de motivar la generalización, tienen interés en sí mismos, porque son contenidos que todos los profesores deben manejar.

En el caso de los anillos, se comienza con un capítulo de introducción a la Teoría de Números. En él se revisan los principales conceptos de los números enteros y se introducen las clases residuales, importante ejemplo, ya que se presenta, probablemente por primera vez para el alumno, una estructura finita que comparte muchas propiedades con los números enteros. También se plantea el problema de las ecuaciones diofánticas lineales. El segundo capítulo trata sobre los polinomios, especialmente sobre los racionales, enfatizando el paralelo entre el álgebra de los polinomios y la aritmética, mostrando como ambos campos comparten conceptos y propiedades. Con estos ejemplos estamos en condiciones, en el tercer capítulo, de desarrollar los primeros pasos de la teoría de anillos. El concepto más complejo tratado en este tema es el de anillos cuociente por un ideal maximal, con el que podemos construir raíces de polinomios irreducibles.

El cuarto capítulo, sin introducir el concepto de grupo, desarrolla algunos ejemplos de los que el alumno tiene nociones informales en cursos previos de álgebra elemental o de geometría: permutaciones, isometrías y simetrías. La idea detrás de este capítulo es que estos conocimientos previos sirvan de motivación para introducir, en el siguiente, el concepto de grupo. Es importante también presentar el nexo entre el álgebra y la geometría, a menudo concebidos en la enseñanza escolar como temas sin conexión.

El último capítulo desarrolla los elementos de la teoría de grupos. El resultado más avanzado incluido en este texto es el teorema de Sylow, como un recíproco parcial del teorema de Lagrange, pero sin entrar en las aplicaciones más profundas de este teorema.

Una tercera característica de este libro es que contiene demostraciones detalladas del 90 % de las proposiciones, exceptuando sólo las pruebas que simplemente repiten una anterior muy similar. En esta etapa de sus estudios el alumno debe desarrollar habilidades que le permitan deducir por sí mismo los teoremas, para ello necesita de una guía y modelo. Creemos que este texto ayuda a lograrlo dando además explicaciones del argumento lógico empleado, al menos, la primera vez que éste se usa. Así, se indica cuando se ha hecho una demostración por contradicción, por casos, usando el contrapositivo, etc.

Versiones previas de este libro han sido usadas por varios profesores de la Facultad de Matemáticas de la Pontificia Universidad Católica de Chile, como notas de clase para un curso que fue dictado regularmente durante algunos años para alumnos de Licenciatura en Matemática con interés en una carrera en pedagogía. El autor agradece a todos ellos sus aportes. Así mismo durante el proceso de preparación de esta versión, he recibido valiosos comentarios de Roberto Aravire, Iván Correa y Avelino Suazo, así como también de varios lectores anónimos, profesores y alumnos de Licenciatura y de Pedagogía en Matemática, quienes hicieron numerosas correcciones y otras mejoras al manuscrito original; para ellos también va mi agradecimiento. Quiero también agradecer a Patricio Felmer y Salomé Martínez, primero por haberme invitado a participar en esta apasionante empresa, enseguida por su cuidadoso trabajo editorial, el que incluyó una minuciosa lectura del primer manuscrito. Por último, es necesario destacar la labor infatigable y de permanente apoyo de Salomé, verdadero motor del proyecto. Su contribución en todos los aspectos, desde los académicos a los administrativos, (¡incluyendo las necesarias presiones por la fecha de entrega!), fue sin duda decisiva para la publicación de este libro.

Capítulo 1: Introducción a la Teoría de Números

La Teoría de Números, al menos originalmente, es la rama de la matemática que estudia las propiedades de los números naturales $1, 2, 3, \ldots$. A poco andar uno descubre que este estudio no se confina a dicho conjunto de números, ni siquiera al conjunto de los números enteros $\ldots, -3, -2, -1, 0, 1, 2, \ldots$, sino que muchas veces se debe recurrir a otros conjuntos de números: algebraicos, reales, complejos, etc., para resolver asuntos relacionados con los números naturales (y viceversa).

Algunos problemas clásicos de la Teoría de Números como el llamado último teorema de Fermat o el de la distribución de los números primos, han dado origen a áreas completas de la matemática. Por ejemplo, al primero de éstos se debe gran parte del desarrollo de los cuerpos ciclotómicos, al segundo todo el progreso de la función zeta de Riemann. Es así que en la Teoría de Números moderna se emplean sofisticadas técnicas de análisis matemático y de teoría de probabilidades. Estudiaremos aquí tan sólo los rudimentos de esta disciplina y haremos algunos alcances acerca de su relación con la llamada álgebra abstracta.

1.1 Los Números Naturales y los Números Enteros

Comenzaremos nuestro estudio suponiendo que el lector está familiarizado con los conjuntos

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, \ldots\} \quad \text{y} \quad \mathbb{N} = \{1, 2, 3, \ldots\},$$

de los números enteros y de los números naturales (o enteros positivos), respectivamente. En particular supondremos conocimiento de las operaciones de suma y multiplicación, así como de la estructura de orden sobre estos conjuntos, por lo tanto, no daremos una definición axiomática de ellas.

La única propiedad de los números naturales que agregaremos es el siguiente axioma:

Principio de Buen Orden. *Todo conjunto no vacío de números naturales tiene un menor elemento.*

Decimos que $\mathbb{N}$ es un conjunto *Bien Ordenado*. Intuitivamente, este sencillo principio nos dice que si existe un número natural que tiene alguna propiedad, entonces podemos encontrar el número natural más pequeño que cumpla con esa propiedad.

Ejemplo 1.1. Demuestre que no existe ningún número natural entre n y $n+1$.

Demostración. Lo demostraremos por contradicción. Para ello supongamos que existe un número natural x tal que $n < x < n+1$. Esto equivale a decir que el conjunto $P = \{x \in \mathbb{N} : n < x < n+1\}$ no es vacío y, por el Principio de Buen Orden, tiene un menor elemento al que llamaremos m.

Ahora consideramos el número $m - n$. Primero observamos que $0 < m - n < 1$ y por lo tanto $0 < (m-n)^2 < m - n < 1$. Pero entonces sumando n, tenemos

$$n < n + (m-n)^2 < m < n + 1\,,$$

es decir, el número natural $n+(m-n)^2$ es un entero entre n y $n+1$ que es más chico que m. Pero m era el más pequeño tal número, hay una contradicción que proviene de suponer que el teorema es falso. □

> *Hemos usado una de las reglas lógicas más comunes, la demostración por contradicción. Si queremos demostrar una afirmación suponemos que ella es falsa (en nuestro caso, supusimos que existe un número natural entre n y $n+1$), luego argumentamos hasta llegar a una proposición que sabemos es falsa, por ejemplo que $0 = 1$, o bien que niega alguna de las hipótesis (encontramos un número más pequeño que el que por definición es el más pequeño). Esto es lo que llamamos contradicción. Como esto no es posible nuestra suposición de que la afirmación es falsa debe desecharse porque produce una situación imposible. Por lo tanto la afirmación es verdadera y el teorema queda demostrado.*

Cabe hacer notar que este menor elemento de un conjunto no vacío A, cuya existencia garantiza el Principio, es único ya que si hubiera dos, digamos a y b, entonces $a \leq b$, ya que a es el menor elemento de A y $b \in A$. Similarmente, $b \leq a$, por lo tanto $a = b$. Tampoco está de más recalcar que el menor elemento de A pertenece a A. (Esto contrasta con el concepto de ínfimo de un conjunto, que puede no pertenecer a él.)

Observe que $\mathbb{Z}$ no verifica el Principio de Buen Orden: $\mathbb{Z}$ mismo (o los enteros menores que 8, o los enteros negativos, etc.) es un subconjunto no vacío de $\mathbb{Z}$ que no tiene un menor elemento. La propiedad de ser un conjunto bien ordenado no es exclusiva de los conjuntos de números enteros positivos. Dado cualquier conjunto linealmente ordenado uno puede preguntarse si es bien ordenado o no. Ver ejercicios.

La segunda propiedad importante de los números naturales es:

Teorema 1.2. Principio de Inducción.
Sea P un conjunto de números naturales tal que:

1. $1 \in P$.
2. *Si $k \in P$, entonces $k + 1 \in P$.*

Entonces $P = \mathbb{N}$.

Demostración. Sea P un conjunto de números naturales que verifica las dos hipótesis del Principio de Inducción. Sea A el conjunto de los números naturales que no pertenecen a P. (Nos basta pues demostrar que A es vacío). Supongamos que A no es

vacío. En virtud del Principio de Buen Orden, A tiene un menor elemento a. Es claro que a no puede ser 1 ya que por hipótesis, $1 \in P$. Luego a tiene un predecesor, $a-1$, que es un entero positivo que pertenece a P porque a es el más pequeño que *no* pertenece a P. Pero entonces, por la segunda parte de la hipótesis de inducción, $a = (a-1)+1 \in P$, lo que es una contradicción porque $a \in A$. Esta contradicción proviene de suponer que A es no vacío. Luego todos los enteros positivos pertenecen a P. □

Intuitivamente, el Principio de Inducción corresponde al "Principio de Dominó": si cae el primero, éste bota al que le sigue y éste bota al siguiente y el siguiente al de más allá..., por lo tanto caen todos.

Supondremos que el lector está familiarizado con este principio y sus aplicaciones. Aunque no lo usaremos mayormente en este texto, es conveniente saber que ambos principios, el de Inducción y el de Buen Orden, son equivalentes, de modo que podemos agregar cualquiera de los dos como axioma y tendremos los mismos resultados.

Teorema 1.3. *El Principio de Inducción implica el Principio de Buen Orden.*

Demostración. Supongamos que existe un conjunto A de naturales que no tiene menor elemento. Demostraremos que A debe ser vacío. Para ello aplicamos inducción al conjunto $P = \{n : 1 \notin A, 2 \notin A, \ldots, n \notin A\}$.

Veamos que $1 \in P$. Supongamos que ocurre lo contrario, o sea, $1 \in A$. Entonces obviamente 1 sería el menor elemento de A, cosa que no existe. Por lo tanto $1 \notin A$ lo que equivale a $1 \in P$.

Supongamos ahora que $n \in P$, es decir, $1 \notin A, 2 \notin A, \ldots, n \notin A$. Si $n+1 \in A$, $n+1$ sería el menor elemento de A, nuevamente obtenemos una contradicción. Luego también se cumple $n+1 \notin A$ y entonces por definición, $n+1 \in P$.

Hemos probado entonces que se cumplen ambas hipótesis del Principio de Inducción, luego podemos concluir que $P = \mathbb{N}$, y por lo tanto $A = \emptyset$, que es lo que queríamos demostrar. □

1.1.1 Ejercicios

1. Sea $\mathbb{R}^+$ el conjunto de los números reales positivos ordenados en la forma habitual, ¿es este un buen orden?
2. Sea $A = \{n^2 : n \in \mathbb{Z}\}$, con el orden natural, ¿es este un buen orden?
3. Demuestre que no puede existir enteros $n_1 > n_2 > \cdots > n_k > \cdots > 0$, para cada k natural. Un conjunto como el anterior suele llamarse *cadena descendente infinita de enteros positivos.*

Una interesante aplicación de este teorema es la siguiente: Demostrar que $\sqrt{2}$ no es racional.

Demostración. Supongamos que sí lo es, es decir, $\sqrt{2} = \frac{p_1}{q_1}$ con p_1 y q_1 enteros positivos. Como $1 < \sqrt{2}$ tenemos además que $p_1 > q_1$.
Observamos ahora que

$$\frac{1}{\sqrt{2}-1} = \frac{\sqrt{2}+1}{1}\,.$$

Reemplazamos la primera $\sqrt{2}$ y despejamos la segunda. Queda

$$\frac{1}{\frac{p_1}{q_1}-1} - 1 = \sqrt{2}\,,$$

o sea,

$$\sqrt{2} = \frac{2q_1 - p_1}{p_1 - q_1}\,.$$

Vemos que $\sqrt{2} = \frac{p_2}{q_2}$ y que $p_1 > p_2$. Podemos repetir el argumento una y otra vez encontrando $\sqrt{2} = \frac{p_1}{q_1} = \frac{p_2}{q_2} = \frac{p_3}{q_3} = \frac{p_4}{q_4} = \cdots$, con $p_1 > p_2 > p_3 > p_4 > \cdots > 0$, lo que como hemos visto es imposible, por lo tanto $\sqrt{2}$ no es racional. □

4. Modifique la demostración del ejercicio anterior para demostrar que $\sqrt{3}$ no es racional.
5. A partir del problema anterior, defina el Principio de Descenso Infinito como sigue: "*Si suponemos que cada vez que un número verifica una cierta propiedad entonces existe otro número estrictamente menor que también la verifica, entonces ningún número natural puede verificar esa propiedad.*"

   Demuestre que este principio es equivalente con el principio del buen orden. El primer registro del uso de este principio se encuentra en la correspondencia matemática de Pierre de Fermat (1601–1665).

1.1.2 Divisibilidad

Definición 1.4. Sean a y b dos enteros con $a \neq 0$. Decimos que a *divide* a b si existe un entero n tal que $na = b$. También decimos que b es un *múltiplo* de a. Denotamos este hecho por $a \mid b$. Si a no divide a b escribiremos $a \nmid b$.

Teorema 1.5. *Si a, b y c son enteros, entonces:*

1. *Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.*
2. *Si $a \mid b$ y $a \mid c$, entonces $a \mid mb + nc$, para cualquier par de enteros m, n.*
3. *Si $a \mid b$ y $b \neq 0$, entonces $0 < |a| \leq |b|$.*
4. *Si $a \mid b$ y $b \mid a$, entonces $a = \pm b$.*

Demostración.

1. $b = ma$ y $c = nb$, luego $c = n(ma) = (nm)a$, es decir $a|c$.

2. $b = pa$ y $c = qa$, luego $mb + nc = m(pa) + m(qa) = (mp + nq)a$, es decir $a|mb + nc$.

3. $b = ma \neq 0$, luego $a \neq 0$ y $m \neq 0$. Por lo tanto, $|a| \geq 1$, $|m| \geq 1$ y $|b| = |ma| = |m||a| \geq 1\,|a| = |a| \geq 1 > 0$.

4. Como $a \mid b$, por 3, $0 < |a| \leq |b|$. Análogamente, $0 < |b| \leq |a|$. Luego $|a| = |b|$ y por lo tanto $a = \pm b$. □

El siguiente teorema es el más importante sobre divisibilidad. Préstese especial atención a su demostración porque es interesante en sí misma como método de demostración.

Teorema 1.6. El Algoritmo de la División.
Sean a y b dos enteros, $b > 0$. Entonces existen dos enteros q y r tales que $a = bq + r$ y $0 \leq r < b$. Los enteros q y r son únicos.

Demostración. Si a es un múltiplo de b, $a = bq + 0$ y el teorema se cumple. Observe que en este caso $r = 0$. Podemos entonces suponer que a no es un múltiplo de b. Consideremos el conjunto

$$A = \{a - bn : n \in \mathbb{Z} \text{ y } a - bn \geq 0\}.$$

Como $a \geq -|a| \geq -|a|b$, tenemos $a + |a|b \geq 0$, luego $a - (-|a|)b \geq 0$, o sea, A es un conjunto no vacío de enteros positivos. Observe que $0 \notin A$ ya que a no es un múltiplo de b.

Por el principio de Buen Orden, A debe tener un menor elemento. Llamémoslo r. Como $r \in A$ debe existir un entero q tal que $r = a - bq$, i.e., $a = bq + r$.

Supongamos que $r \geq b$. Entonces $r - b = a - bq - b = a - b(q + 1) \geq 0$, luego $r - b \in A$, pero $0 \leq r - b < r$, contradiciendo la minimalidad de r. Por lo tanto $0 \leq r < b$. (Como vimos arriba, $r = 0$ si y sólo si a es un múltiplo de b).

Finalmente, para probar la unicidad de q y r, supongamos que q' y r' son números tales que $a = bq' + r'$ y $0 \leq r' < b$. Entonces $bq + r = bq' + r'$, luego $b(q - q') = r' - r$, o sea, $b \mid (r' - r)$. Si $r \neq r'$, por Teorema 1.5,3, $|r' - r| \geq |b| = b > 0$. Pero esto es imposible ya que $-b < r' - r < b$. Luego $r = r'$. Pero entonces $b(q - q') = 0$ y como $b \neq 0$, tenemos $q = q'$.

□

> *La demostración anterior ilustra cómo se demuestra que un objeto que tiene alguna propiedad es único. Suponemos que hay otro con la mismas características (en este caso, hay dos restos y dos cuocientes) y demostramos usando nuestra teoría que deben ser iguales.*

Ejemplos 1.7.

1. Demuestre que si a y b son números impares entonces $a^2 + b^2$ es par pero no es divisible por 4.

Como a es impar, $a = 2k+1$ para cierto k, e igualmente $b = 2j+1$, por lo tanto $a^2+b^2 = (2k+1)^2+(2j+1)^2 = 4k^2+4k+1+4j^2+4j+1 = 4(k^2+j^2+k+j)+2$ es par, pero al dividirse por 4 deja resto 2, luego a^2+b^2 no es divisible por 4.

2. Dado cualquier entero n, n^3-n es divisible por 6.
Observemos que $N = n^3-n = (n-1)\,n\,(n+1)$, es decir, el producto de tres números consecutivos. Resolveremos este problema haciendo un uso típico del teorema de la división (hay otras soluciones más elegantes). Por el axioma de la división, n debe ser de la forma $n = 6k+r$ con $r \in \{0,1,2,3,4,5\}$. Es cosa de analizar los seis casos:
Si $n = 6k$, entonces $N = (6k-1)6k(6k+1)$ es obviamente múltiplo de 6.
Si $n = 6k+1$, entonces $N = 6k(6k+1)(6k+2)$ es también obviamente múltiplo de 6.
Si $n = 6k+2$, entonces $N = (6k+1)(6k+2)(6k+3) = 6(6k+1)(3k+1)(2k+1)$ es múltiplo de 6.
Si $n = 6k+3$, entonces $N = (6k+2)(6k+3)(6k+4) = 6(3k+1)(2k+1)(6k+4)$ es múltiplo de 6.
Si $n = 6k+4$, entonces $N = (6k+3)(6k+4)(6k+5) = 6(2k+1)(2k+2)(6k+5)$ es múltiplo de 6.
Si $n = 6k+5$, entonces $N = (6k+4)(6k+5)(6k+6) = 6(6k+4)(6k+5)(k+1)$ es múltiplo de 6.

> *La situación que se presenta aquí es habitual. Tenemos varios casos (aquí son seis, pero podrían presentarse más). Enseguida para cada uno de ellos probamos que se cumple una cierta afirmación (aquí es que N es divisible por 6). Entonces la afirmación debe ser cierta porque se cumple en todos los casos posibles.*

Definición 1.8.

1. Un entero positivo $p \neq 1$ se dice *primo* si sus únicos divisores son ± 1 y $\pm p$.
2. Sean a, b dos enteros no ambos nulos. El mayor entero que divide tanto a a como a b se llama el *máximo común divisor* de a y b. El máximo común divisor de a y b se denota (a,b) (o bien $\mathrm{MCD}\{a,b\}$).
   Similarmente definimos $(a_1,a_2,\ldots,a_n)$, el máximo común divisor de $a_1,a_2,\ldots,a_n$, como el mayor entero que divide a todos esos números.
3. Dos enteros se dicen *primos relativos* si su máximo común divisor es 1.

A priori no es obvio que el máximo común divisor de dos números deba existir, sin embargo, esto es consecuencia inmediata del próximo teorema.

Teorema 1.9. *Dados dos enteros a y b no ambos nulos, su máximo común divisor (a,b) es el menor entero positivo que se puede escribir como suma de múltiplos de a y de b.*

Demostración. Supongamos sin pérdida de generalidad que $a \neq 0$ y consideremos el conjunto:

$$A = \{ma + nb : m, n \in \mathbb{Z} \text{ y } ma + nb > 0\}$$

A no es vacío ya que $0 < |a| = \pm 1a + 0b \in A$. Por el Principio de Buen Orden, A tiene un menor elemento, al que llamaremos d. Observe que $d > 0$. Como $d \in A$, existen enteros m, n tales que $d = ma + nb$. Debemos verificar que éste es el máximo común divisor de a y b.

Por el algoritmo de la división, $a = qd + r$, con $0 \leq r < d$. Entonces,

$$r = a - qd = a - q(ma + nb) = (1 - mq)a - nqb.$$

Si $r > 0$, entonces $r \in A$, pero $r < d$, lo que contradice la minimalidad de d. Por lo tanto $r = 0$ y $d \mid a$.

Análogamente podemos demostrar que $d \mid b$, por lo tanto d es un divisor común de a y de b.

Para verificar que d es el mayor divisor común, sea $s \geq 1$ otro divisor común. Por el Teorema 1.5,2, $s \mid ma + nb$, para cualquier $m, n \in \mathbb{Z}$, en particular, $s \mid d$, luego por 1.5,3, $0 < s \leq d$. □

El siguiente corolario se prueba usando inducción.

Corolario 1.10. *El máximo común divisor de $a_1, a_2, \ldots, a_n$ es el menor entero positivo que puede escribirse como suma de múltiplos de los números $a_1, a_2, \ldots, a_n$.*

Observación 1.1.

1. a y b son primos relativos si y sólo si existen $m, n \in \mathbb{Z}$ tales que $1 = ma + nb$.
2. Si $s \mid a_1$, $s \mid a_2$, $\ldots$, $s \mid a_n$, entonces $s \mid (a_1, a_2, \ldots, a_n)$.

Corolario 1.11. *Si $a_1, a_2, \ldots, a_n$ son enteros, entonces*

$$(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n).$$

Demostración. Sea $d = (a_1, a_2, \ldots, a_n)$. Por definición $d \mid a_1$, $d \mid a_2, \ldots, d \mid a_n$, luego $d \mid (a_1, a_2, \ldots, a_{n-1})$ y también $d \mid a_n$, por lo tanto $d \mid ((a_1, a_2, \ldots, a_{n-1}), a_n)$. A la inversa, $((a_1, a_2, \ldots, a_{n-1}), a_n)$ es divisor común de $(a_1, a_2, \ldots, a_{n-1})$ y de a_n, luego $((a_1, a_2, \ldots, a_{n-1}), a_n) \mid d$. Como ambos son positivos, por 1.5,4, son iguales. □

Corolario 1.12. *Si $d = (a, b)$, entonces $(\frac{a}{d}, \frac{b}{d}) = 1$. (i.e. $\frac{a}{d}$ y $\frac{b}{d}$ son primos relativos. ¡Observe que $\frac{a}{d}$ y $\frac{b}{d}$ son enteros!).*

El siguiente es un importante teorema, a veces conocido como Lema de Euclides. Responde parcialmente la pregunta: Si un número divide a un producto, ¿debe dividir a alguno de sus factores? En general no, por ejemplo, $6 \mid 12 = 3 \cdot 4$, sin embargo, $6 \nmid 3$ y $6 \nmid 4$.

Teorema 1.13. *Si p es un número primo y $p \mid bc$, entonces $p \mid b$ ó $p \mid c$.*

Esto se puede generalizar fácilmente por inducción a:

Corolario 1.14. *Si p es un número primo y $p \mid a_1\, a_2 \cdots a_n$, entonces $p \mid a_k$, para algún $k \leq n$.*

El Teorema 1.13 es un caso particular del próximo teorema que responde la pregunta anterior en forma más general.

Teorema 1.15. *Si $(a, b) = 1$ y $a \mid bc$, entonces $a \mid c$.*

Demostración. Si $a \mid bc$, entonces $bc = ak$ para algún k, y como $1 = ma + nb$, multiplicando ambos miembros por c,

$$c = mac + nbc = mac + nak = a(mc + nk).$$

□

El siguiente ejemplo es un pequeño lema que usaremos en la próxima sección. Ilustra cómo se usa la descomposición del máximo común divisor de dos números como combinación de ellos.

Ejemplo 1.16. Si $a = bq + r$ y $b \neq 0$, entonces $(a, b) = (b, r)$.

Demostración. $(a, b) = ma + nb = m(bq + r) + nb = (mq + n)b + mr$, es decir, (a, b) es una suma de múltiplos de b y de r, luego por el teorema 1.9, $(a, b) \leq (b, r)$.

De una manera similar demostramos que $(b, r) \leq (a, b)$. □

1.1.3 El Algoritmo de Euclides

Existe un método para calcular el máximo común divisor de dos números, tal método se denomina el *Algoritmo de Euclides*. Aparece por primera vez en el Libro VII de los Elementos de Euclides, pero los historiadores creen que el algoritmo y algunas de sus consecuencias era conocido antes de eso.

Sean a y b dos números no ambos nulos, digamos, $b > 0$. Entonces, por el algoritmo de la división, existen q y r tales que $a = bq + r$, con $0 \leq r < b$.

Si $r = 0$, entonces $b \mid a$, $(a, b) = b$ y hemos terminado.

Si $r > 0$, entonces existen q_1 y r_1 tales que $b = rq_1 + r_1$, con $0 \leq r_1 < r$.

Si $r_1 = 0$, entonces $(b, r) = r$ y por el lema que demostramos en el ejemplo 1.16, $(a, b) = r$ y nuevamente hemos terminado.

Si $r_1 > 0$, entonces existen q_2 y r_2 tales que $r = r_1 q_2 + r_2$ y $0 \leq r_2 < r_1$.

Este proceso se puede continuar indefinidamente de tal manera que en cada paso, si obtenemos un resto cero, nos detenemos y si no, aplicamos el algoritmo de la división una vez más. Es importante notar que en cada aplicación del algoritmo de la división, el resto obtenido es estrictamente menor que el de la aplicación precedente. Vale decir, tenemos $r > r_1 > r_2 > \cdots > r_n > \cdots \geq 0$.

Pero tiene que existir un n tal que $r_n = 0$, ya que si no, habría una cadena descendente infinita de números naturales, lo que contradice el Principio de Buen Orden (ver Ejercicios). Pero si $r_n = 0$, $r_{n-1} \mid r_{n-2}$ en cuyo caso $(r_{n-2}, r_{n-1}) = r_{n-1}$ y aplicando el Ejemplo 1.16 varias veces,

$$(a, b) = (r, r_1) = (r_1, r_2) = \cdots = (r_{n-2}, r_{n-1}) = r_{n-1}.$$

Vale decir, el máximo común divisor de a y de b es el resto inmediatamente anterior al resto que se anula.

Destaquemos que el algoritmo de Euclides funciona por tres principios:

1. Si $b \mid a$, entonces $(a, b) = b$.
2. Si $a = bq + r$ y $b \neq 0$, entonces $(a, b) = (b, r)$. (Ejemplo 1.16).
3. No existen cadenas descendentes infinitas de números naturales.

Ejemplo 1.17. Calculemos el máximo común divisor de 454 y 136.

$$\begin{aligned} 454 &= 136 \cdot 3 + 46 \\ 136 &= 46 \cdot 2 + 44 \\ 46 &= 44 \cdot 1 + 2 \\ 44 &= 2 \cdot 22 + 0 \end{aligned}$$

Es decir, el máximo común divisor de 454 y 136 es 2.

Uno de los métodos más habituales para calcular el máximo común divisor de dos números es hacer una lista de todos los divisores de cada número y luego destacar los que se repiten y elegir entre ellos el más grande. Este es uno de los algoritmos que se aprende en el colegio y es correcto, pero tiene el defecto de que debemos encontrar todos los divisores de cada número, tarea que para números grandes es muy costosa. El Algoritmo de Euclides en cambio requiere de comparativamente pocos cálculos para llegar al resultado, incluso si los números son grandes. Otros algoritmos escolares los discutiremos en la próxima sección.

Para calcular el máximo común divisor de tres o más números, aplicamos el Corolario 1.11 y el algoritmo de Euclides.

Definición 1.18. El *mínimo común múltiplo* de dos enteros no nulos a y b es el menor entero positivo que es múltiplo de a y de b. Se le denotará por $[a, b]$ (o bien por m.c.m.$\{a, b\}$).

Como en el caso del máximo común divisor, el mínimo común múltiplo de dos números siempre existe. En este caso, en virtud del Principio de Buen Orden.

Teorema 1.19. *Si m es un múltiplo común de a y de b, entonces $[a, b] \mid m$.*

Demostración. Por el algoritmo de la división, $m = [a,b]q + r$, con $0 \leq r < [a,b]$. Pero $a \mid m$ y $a \mid [a,b]$, luego $a \mid r = m - [a,b]q$.

Similarmente, $b \mid r$, o sea, r es un múltiplo común de a y de b. Si $r > 0$, entonces $[a,b]$ no sería el mínimo común múltiplo de a y de b. Por lo tanto $r = 0$ y $[a,b] \mid m$. □

Teorema 1.20. *Si a y b son enteros no nulos,*

$$[a,b] = \frac{|ab|}{(a,b)}.$$

Demostración. Sean $d = (a,b)$ y $m = [a,b]$. Entonces

$$\frac{|ab|}{d} = \frac{|a|}{d}|b| = |a|\frac{|b|}{d},$$

o sea $\frac{|ab|}{d}$ es un múltiplo de a y de b, luego $m \mid \frac{|ab|}{(a,b)}$ y en particular, $m \leq \frac{|ab|}{d}$.

Por otra parte, $|ab|$ es un múltiplo común de a y b, luego $m \mid |ab|$ y, en particular, $\frac{|ab|}{m}$ es un entero.

Ahora bien, $m = ka$, luego

$$k\frac{|ab|}{m} = \frac{k|a|}{m}|b| = \pm b,$$

o sea, $\frac{|ab|}{m} \mid b$. Análogamente, $\frac{|ab|}{m} \mid a$. Es decir, $\frac{|ab|}{m}$ es divisor común de a y de b, luego $\frac{|ab|}{m} \mid d$ y por el Teorema 1.5.3., $\frac{|ab|}{m} \leq d$ y esto es lo mismo que $\frac{|ab|}{d} \leq m$. Por lo tanto $\frac{|ab|}{d} = m$. □

El siguiente teorema, conocido también como teorema de factorización única, es la piedra angular de toda la teoría de números y, como veremos en el próximo capítulo, se puede extender a otros campos. Aparece en los Elementos de Euclides.

Teorema 1.21. El Teorema Fundamental de la Aritmética.
Todo número entero mayor que 1 *es un número primo o bien se puede factorizar como producto de números primos. Más aún, tal factorización es única salvo por el orden de los factores.*

Demostración. Supongamos que el teorema no es cierto, es decir, existe un entero positivo mayor que 1 que no es primo y que no se descompone como producto de primos. Sea n el más pequeño tal número. Este debe existir por el Principio de Buen Orden.

Como n no es primo, debe tener divisores no triviales. Sea $n = ab$, donde a y b son distintos de ± 1 y de $\pm n$. Sin pérdida de generalidad podemos suponer que a y b son positivos. Además sabemos que $a < n$ y $b < n$. Pero entonces, como n es minimal para la propiedad indicada, tanto a como b son o bien primos, o bien

producto de primos y por lo tanto, en cualquier caso, n es producto de números primos, contradiciendo la suposición original. Luego ésta es falsa.

Para demostrar la unicidad de la descomposición, supongamos que existen enteros que tienen más de una descomposición. Sea n ahora el menor entero positivo tal que la factorización no es única. Es decir,

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

donde $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ son números primos. Entonces $p_1 | (q_1 q_2 \cdots q_s)$ y por el Corolario 1.14, para algún j, $1 \leq j \leq s$, $p_1 | q_j$. Pero como ambos son primos, $p_1 = q_j$. Podemos suponer (reordenando) que $j = 1$, luego

$$n' = p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s,$$

pero $n' < n$, luego n' verifica la condición de unicidad de la factorización, por lo tanto $r = s$ y, reordenando, $p_i = q_i$, para $1 \leq i \leq r$, por lo tanto la descomposición de n es única. □

Observación 1.2. Obviamente no todos los primos que aparecen en la descomposición de un número tienen que ser distintos. En general todo entero $n > 1$ se puede escribir como

$$n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m},$$

donde los p_k son primos, los k_i son enteros positivos. El número k_i suele llamarse la *multiplicidad* de p_i en la descomposición de n.

Este teorema tiene muchas aplicaciones, la más elemental es probablemente el algoritmo para calcular máximo común divisor y mínimo común múltiplo de dos o más números:

El máximo común divisor de dos números es el producto de todos los primos (considerando su multiplicidad) que se repiten en la factorización de ambos números.

El mínimo común múltiplo de dos números es el producto de las máximas potencias de cada primo que aparece en la descomposición de alguno de los números.

Ejemplo 1.22. Calcular el máximo común divisor y el mínimo común múltiplo de 48 y 180.

Como $48 = 2^4 \cdot 3$ y $180 = 2^2 \cdot 3^2 \cdot 5$,

$$(48, 180) = 2^2 \cdot 3 = 12 \quad \text{y} \quad [48, 180] = 2^4 \cdot 3^2 \cdot 5 = 720.$$

Este algoritmo puede generalizarse a cualquier cantidad de números.

Podemos dar una fórmula general para calcular el máximo común divisor y el mínimo común múltiplo de dos números basada en la descomposición en números primos. Consideremos las descomposiciones

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \quad \text{y} \quad m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

de los números n y m, donde $0 \leq \alpha_i$ y $0 \leq \beta_i$, para $1 \leq i \leq k$, en las que si algún primo p_i no aparece en ambas descomposiciones hacemos $\alpha_i = 0$ ó $\beta_i = 0$, según corresponda. Entonces

$$(n, m) = p_1^{min\{\alpha_1,\beta_1\}} p_2^{min\{\alpha_2,\beta_2\}} \cdots p_k^{min\{\alpha_k,\beta_k\}},$$
$$[n, m] = p_1^{max\{\alpha_1,\beta_1\}} p_2^{max\{\alpha_2,\beta_2\}} \cdots p_k^{max\{\alpha_k,\beta_k\}}.$$

Como los divisores comunes tienen que estar constituidos por primos y obviamente no puede aparecer ningún primo que no esté en las descomposiciones de ambos números, el máximo común divisor deberá estar formado por el producto de aquellos primos que comparten ambos números. Esto es lo que dice la primera expresión. Algo análogo ocurre con el mínimo común múltiplo y la segunda expresión.

Ejemplo 1.23. Podemos usar la descomposición en factores primos para dar una demostración de que $\sqrt{2}$ no es racional. En efecto, supongamos que $\sqrt{2} = \frac{n}{m}$, donde $(m, n) = 1$ y usemos las descomposiciones

$$n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s} \quad \text{y} \quad m = q_1^{j_1} q_2^{j_2} \cdots q_t^{j_t}.$$

Vemos que como $(m, n) = 1$ los primos p_i y q_i son todos distintos. Entonces, elevando al cuadrado tendríamos

$$2\, q_1^{2j_1} q_2^{2j_2} \cdots q_t^{2j_t} = p_1^{2k_1} p_2^{2k_2} \cdots p_s^{2k_s}.$$

Vemos que 2 aparece un número impar de veces en la primera descomposición y un número par de veces en la segunda. Tendríamos entonces un número con dos descomposiciones distintas, lo que es imposible. □

Otro algoritmo aprendido en el colegio depende del Teorema Fundamental de la Aritmética. Consiste en buscar los primos que comparten las respectivas factorizaciones. El algoritmo entonces es una manera rápida de encontrar estos primos. Recordémoslo con un ejemplo, queremos calcular el máximo común divisor de 3276 y 2772.

3276	2772	2	primer primo que divide a ambos
1638	1386	2	vuelve a dividir a ambos
819	693	3	es el siguiente primo que divide a ambos
273	231	3	vuelve a dividir a ambos
91	77	7	es el siguiente primo que divide a ambos
13	11		no hay otros primos que dividan a ambos
		252	es el máximo común divisor de 3276 y 2772
			porque es el producto de todos los primos anteriores

Si lo calculamos con el Algoritmo de Euclides tenemos

$$\begin{aligned} 3276 &= 2772 \cdot 1 + 504 \\ 2772 &= 504 \cdot 5 + 252 \\ 504 &= 252 \cdot 1 + 0\,, \end{aligned}$$

o sea $252 = (3276, 2772)$. □

Terminamos esta sección con el siguiente corolario, uno de los más famosos y hermosos resultados de Euclides.

Corolario 1.24. *Existen infinitos números primos.*

Demostración. Supongamos que existe solamente una cantidad finita de primos p_1, p_2,..., p_n. Consideremos ahora el número

$$m = p_1 p_2 \cdots p_n + 1.$$

Obviamente m es mayor que todos los primos, luego no es primo. Por otra parte, m no es divisible por p_1, ni por p_2, ..., ni por p_n, o sea, m no es divisible por ningún primo. Pero por el teorema 1.21, m debe ser divisible por algún primo, lo cual es una contradicción, por lo tanto la lista finita debe ser incompleta. □

1.1.4 Ejercicios

1. Demuestre o de un contraejemplo de:
   a) Si $a \mid a + b$, entonces $a \mid b$.
   b) Si $a^2 \mid b^2$, entonces $a \mid b$.
   Inténtelo primero sin usar el teorema de descomposición prima. Luego hágalo haciendo uso del teorema.
   c) Si $a \mid b^2$, entonces $a^2 \mid b^2$.
2. Demuestre los criterios de divisibilidad que aprendió en el colegio. Recordemos que si un entero se escribe en notación decimal como

   $$a_n a_{n-1} \cdots a_2 a_1 a_0,$$

   a_0 es su *dígito de las unidades*, a_1 es su *dígito de las decenas*, etc.
   a) Un número es divisible por 2 si $2 \mid a_0$.
   b) Un número es divisible por 3 si la suma de sus dígitos es divisible por 3.
   c) Un número es divisible por 4 si $4 \mid a_1 a_0$. El número es también es divisible por 4 si $4 \mid 2a_1 + a_0$.
   d) Un número es divisible por 5 si su dígito de las unidades es 5 o 0.
   e) Un número es divisible por 6 si es divisible por 2 y por 3.
   f) Un número es divisible por 7 si

   $$a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - \cdots$$

   es divisible por 7.

g) Un número es divisible por 8 si $8 \mid a_2a_1a_0$. También es divisible por 8 si $8 \mid 4a_2 + 2a_1 + a_0$.

h) Un número es divisible por 9 si la suma de sus dígitos es divisible por 9.

i) Un número es divisible por 11 si

$$a_2a_1a_0 - a_5a_4a_3 + a_8a_7a_6 - \cdots$$

es divisible por 11.

3. Invente criterios de divisibilidad para otros números más grandes.
4. Probar que si a y b son impares, entonces $a^2 + b^2$ no puede ser un cuadrado perfecto.
5. Demuestre que hay infinitos enteros de la forma $5^n - 1$ que son divisibles por 7.
6. Demuestre que el cuadrado de cualquier número entero puede tener la forma $3k$ o bien $3k + 1$, pero no puede tener la forma $3k + 2$.
7. Demuestre que no existen enteros a y b tales que $(a, b) = 7$ y $2a + b = 50$.
8. Demuestre que si $(a, m) = 1$ y $(b, m) = 1$, entonces $(ab, m) = 1$.
9. Demuestre que si $(a, b) = 1$, entonces $(a + b, ab) = 1$.
10. Demuestre que el mínimo común múltiplo de dos números siempre existe.

1.2 Congruencias

En esta sección estudiaremos una importante relación definida sobre el conjunto de los números enteros. Esta relación tiene numerosas aplicaciones y sirve para introducir varios conceptos algebraicos que serán generalizados en capítulos posteriores.

Definición 1.25. Sea m un entero positivo. Decimos que a *es congruente con* b *módulo* m si y sólo si $m \mid a - b$.

Denotaremos este hecho por $a \equiv b \pmod{m}$.

Teorema 1.26. *La relación de congruencia módulo* m *es una relación de equivalencia.*

Demostración. Como $m \mid 0 = a - a$, $a \equiv a \pmod{m}$ y la relación es reflexiva.

Si $a \equiv b \pmod{m}$, entonces $m \mid a - b$, luego $m \mid -(a - b) = b - a$, o sea, $b \equiv a \pmod{m}$ y la relación es simétrica.

Supongamos que $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, es decir, $m \mid a - b$ y $m \mid b - c$. Entonces $m \mid (a - b) + (b - c) = a - c$, o sea, $a \equiv c \pmod{m}$ y la relación es transitiva. □

Teorema 1.27. *Si* $a \equiv b \pmod{m}$ *y* $c \equiv d \pmod{m}$, *entonces*

$$\begin{aligned} a + c &\equiv b + d \pmod{m}, \\ ac &\equiv bd \pmod{m} \text{ y} \\ -a &\equiv -b \pmod{m}. \end{aligned}$$

Demostración. Supongamos que $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, es decir, $m \mid a-b$ y $m \mid c-d$.

1. Sumando, $m \mid (a-b)+(c-d) = (a+c)-(b+d)$, o sea, $a+c \equiv b+d \pmod{m}$.
2. Multiplicando, $m \mid (a-b)c = ac-bc$ y $m \mid b(c-d) = bc-bd$, y sumando $m \mid (ac)-(bd)$, o sea, $ac \equiv bd \pmod{m}$.
3. Además $m \mid a-b = -b-(-a)$, o sea, $-a \equiv -b \pmod{m}$.

□

Observación 1.3.

1. Si $m = 1$, entonces $a \equiv b \pmod{1}$ para todo a y todo b. Como esta relación no es interesante, a menudo se exige que $m > 1$.
2. La ley de cancelación para la suma es válida para congruencias, es decir, si $a+c \equiv b+c \pmod{m}$, entonces $a \equiv b \pmod{m}$.
3. La ley de cancelación para el producto no es válida para congruencias como lo demuestra el ejemplo siguiente:
   $5 \cdot 6 \equiv 3 \cdot 6 \pmod{12}$, pero $5 \not\equiv 3 \pmod{12}$.

Teorema 1.28. *Si* $ab \equiv ac \pmod{m}$ *y* $d = (a,m)$, *entonces* $b \equiv c \pmod{\frac{m}{d}}$.

Demostración. Como $(a,m) = d$, existen r y s tales que $a = rd$ y $m = sd$, donde $(r,s) = 1$.

Por otra parte, como $ab \equiv ac \pmod{m}$, $a(b-c) = ab-ac = km$, para algún $k \in \mathbb{Z}$. Luego $rd(b-c) = ksd$ y cancelando d, $s \mid r(b-c)$, y por el Teorema 1.15, $s \mid b-c$ o sea, $b-c = ts = t\frac{m}{d}$, vale decir, $b \equiv c \pmod{\frac{m}{d}}$. □

Si bien la ley de cancelación no es siempre válida para congruencias, el siguiente corolario inmediato del teorema anterior nos indica cuándo se puede cancelar: podemos cancelar factores que sean primos relativos con el módulo.

Corolario 1.29. *Supongamos* $(a,m) = 1$. *Si* $ab \equiv ac \pmod{m}$, *entonces* $b \equiv c \pmod{m}$.

1.2.1 Ecuaciones

Teorema 1.30. *La ecuación* $ax \equiv b \pmod{m}$ *tiene solución si y solamente si* $(a,m) \mid b$.

Demostración. Si $ax \equiv b \pmod{m}$ tiene solución, existen enteros x e y tales que $ax-b = my$, luego $b = ax-my$, es decir, b es suma de múltiplos de a y de m, por lo tanto, $(a,m) \mid b$.

Por otra parte, si $(a,m) \mid b$, para algún k, $b = k(a,m)$. Ahora bien, como $(a,m) = ra+sm$, para ciertos enteros r y s, $b = k(a,m) = (kr)a+(ks)m$. Luego kr es solución de la ecuación $ax \equiv b \pmod{m}$. □

Observe que la solución a la ecuación $ax \equiv b \pmod{m}$ nunca es única ya que si x_0 es una solución, entonces para cualquier k, $x_0 + km$ también lo es.

Ejemplo 1.31. Consideremos la ecuación $42x \equiv 50 \pmod{76}$.

$$\begin{aligned} 42x &\equiv 50 \pmod{76} \\ 2 \cdot 21x &\equiv 2 \cdot 25 \pmod{76} \\ 21x &\equiv 25 \pmod{38} \\ 21x &\equiv 25 + 38 \pmod{38} \\ 21x &\equiv 63 \pmod{38} \\ 21x &\equiv 21 \cdot 3 \pmod{38} \\ x &\equiv 3 \pmod{38}. \end{aligned}$$

Es decir, las soluciones de la ecuación $42x \equiv 50 \pmod{76}$ son todos los enteros

$$\{\cdots, -73, -35, 3, 41, 79, \cdots\}.$$

Estas se pueden expresar en términos del módulo original 76. En efecto, como las soluciones obedecen la fórmula $x = 3 + 38k$, separando en dos casos, si k es par o si k es impar, tenemos $x = 3 + 38 \cdot 2n = 3 + 76n$ y $x = 3 + 38(2n+1) = 41 + 76n$. Observe que $41 \not\equiv 3 \pmod{76}$, por lo tanto las soluciones a esta ecuación módulo 76 son dos, a saber,

$$x \equiv 3 \pmod{76} \quad \text{y} \quad x \equiv 41 \pmod{76}.$$

Recordando[1] que una ecuación de primer grado en los enteros (o los racionales o los reales) tiene, a lo más una solución, la pregunta obvia es, ¿cuántas soluciones no congruentes entre sí puede tener una ecuación en congruencias?

Consideremos la ecuación $ax \equiv b \pmod{m}$ y sea x_0 una solución. Si x es otra solución, entonces $ax \equiv ax_0 \equiv b \pmod{m}$, luego por el Teorema 1.28

$$x \equiv x_0 \pmod{\frac{m}{d}},$$

donde $d = (a, m)$. Es decir, $x = x_0 + t\frac{m}{d}$, o sea, x pertenece al conjunto

$$\{\cdots, x_0 - 2\frac{m}{d}, x_0 - \frac{m}{d}, x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \cdots, x_0 + (d-1)\frac{m}{d}, x_0 + m, \cdots\}.$$

¿Cuántas de estas soluciones son "distintas", en el sentido de no ser congruentes módulo m entre sí?

Observemos que $x_0 + m \equiv x_0 \pmod{m}$. De la misma manera, $x_0 - \frac{m}{d} \equiv x_0 + (d-1)\frac{m}{d} \pmod{m}$, etc.

Es claro que cualquier solución de la ecuación será congruente módulo m con uno de los enteros

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \cdots, x_0 + (d-1)\frac{m}{d}.$$

[1] Esto lo veremos con mayor detalle en el próximo capítulo.

Por otra parte, no resulta difícil ver que ninguno de estos números es congruente módulo m con otro, porque las diferencias entre ellos son todas menores que m. Decimos que el conjunto anterior es un *conjunto completo de representantes* de las soluciones de $ax \equiv b \pmod{m}$.

En los párrafos anteriores hemos demostrado el siguiente teorema:

Teorema 1.32. *Si $(a, m) \mid b$, la ecuación $ax \equiv b \pmod{m}$ tiene (a, m) soluciones no congruentes módulo m entre sí.*

Ejemplo 1.33. Consideremos la ecuación $68x \equiv 100 \pmod{120}$. Entonces

$$\begin{aligned} 68x &\equiv 100 + 2 \cdot 120 \pmod{120} \\ 68x &\equiv 340 \pmod{120} \text{ y como } (68, 120) = 4, \\ x &\equiv 5 \pmod{30}. \end{aligned}$$

Por lo tanto $\{5, 35, 65, 95\}$ es un conjunto completo de representantes de las soluciones de $68x \equiv 100 \pmod{120}$.

1.2.2 Sistemas de Congruencias

Consideremos el siguiente problema.

En algún lugar del sur de Chile vive un pastor que cuida de su rebaño de ovejas con singular dedicación. Cierto día, acertó a pasar por este lugar un funcionario municipal, quien tenía por misión averiguar la cantidad exacta de ovejas de este pastor. Este es (resumidamente) el diálogo que tuvo lugar:

– Y, ¿cuántas ovejas tiene usted?

– Bueno, mire, en realidad no sé. Fíjese que yo aprendí a contar hasta cinco no más. Lo que sí le puedo decir es que si cuento las ovejas de tres en tres, me sobran dos, si las cuento de cuatro en cuatro, me sobra una, y si las cuento de cinco en cinco, me sobran tres.

El funcionario miró someramente el rebaño de ovejas y decidió que en ningún caso éste tenía más de cien ovejas. Hecho esto, se dio por satisfecho. ¿Cómo pudo averiguar cuántas ovejas formaban el rebaño?

Supongamos que el número de ovejas es x.

"Si cuento las ovejas de tres en tres, me sobran dos". O sea, $x \equiv 2 \pmod{3}$.

"Si cuento las ovejas de cuatro en cuatro, me sobra una". O sea,
$x \equiv 1 \pmod{4}$.

"Si cuento las ovejas de cinco en cinco, me sobran tres". O sea, $x \equiv 3 \pmod{5}$.

Se trata entonces de encontrar un número x que verifique las tres congruencias:

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 1 \pmod{4} \\ x &\equiv 3 \pmod{5}. \end{aligned}$$

Además nos dicen que x debe ser menor que 100.

Este tipo de problema recibe el nombre de *sistema de congruencias* y en esta sección veremos métodos para resolverlos. Veamos primero dos ejemplos algo más sencillos que el de nuestro funcionario.

Ejemplos 1.34. Queremos solucionar el siguiente problema, encontrar un número x que satisfaga las dos ecuaciones:

$$\begin{aligned} x &\equiv 3 \pmod 7 \\ 5x &\equiv 7 \pmod{12}. \end{aligned}$$

Sea x_0 una solución. Entonces $x_0 = 3 + 7s$, para algún s, por ser x_0 solución de la primera ecuación. Reemplazando en la segunda ecuación,

$$\begin{aligned} 5(3+7s) &\equiv 7 \pmod{12} \\ 35s &\equiv -8 \pmod{12} \\ 35s &\equiv -8+288 \pmod{12} \\ 35s &\equiv 280 \pmod{12} \\ s &\equiv 8 \pmod{12}. \end{aligned}$$

Esto es, $s = 8+12t$, para algún t, luego $x_0 = 3+7(8+12t)$, o bien, $x_0 = 59+84t$, es decir, toda solución del sistema anterior es congruente con 59 (mód 84).

Veamos ahora un segundo ejemplo. Consideremos el sistema:

$$\begin{aligned} x &\equiv 2 \pmod 4 \\ x &\equiv 5 \pmod 6. \end{aligned}$$

y procedamos como en el ejemplo anterior. Sea x_0 una solución del sistema.

$$\begin{aligned} x_0 = 2+4s &\equiv 5 \pmod 6 \\ 4s &\equiv 3 \pmod 6, \end{aligned}$$

por lo tanto $4s = 3 + 6t$, para algún t, lo que es claramente imposible. Luego este sistema no tiene solución. Observe que el punto importante aquí es que no podemos cancelar el 4, ya que $(4,6) \nmid 3$.

¿Cuáles sistemas tienen solución y cuáles no la tienen?

Teorema 1.35. *El sistema*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

tiene solución si y solamente si $(m_1, m_2) \mid a_1 - a_2$.

Si x_0 *es una solución, entonces toda solución es congruente con* x_0 *módulo* $[m_1, m_2]$.

Demostración. El número x_0 es solución del sistema si y sólo si existe un entero s tal que $x_0 = a_1 + s\,m_1 \equiv a_2 \pmod{m_2}$ si y sólo si existe un entero s tal que $s\,m_1 \equiv a_2 - a_1 \pmod{m_2}$.

Por el teorema 1.30, tal s existe si y sólo si $(m_1, m_2) \mid a_2 - a_1$.

Supongamos ahora que $(m_1, m_2) \mid a_2 - a_1$ y que x_0 es una solución del sistema. Entonces si x es otra solución,

$$\begin{aligned} x \equiv a_1 &\equiv x_0 \pmod{m_1} \\ x \equiv a_2 &\equiv x_0 \pmod{m_2} \end{aligned}$$

luego $m_1 \mid x - x_0$ y $m_2 \mid x - x_0$, o sea, $x - x_0$ es un múltiplo común de m_1 y de m_2, luego $[m_1, m_2] \mid x - x_0$, por lo tanto $x \equiv x_0 \pmod{[m_1, m_2]}$. □

El siguiente es uno de los más famosos teoremas de la Teoría de Números. Su nombre se debe a que la mención más antigua de este teorema aparece en un libro del matemático chino Sun Tzu, quien vivió alrededor del siglo III D.C.

Teorema 1.36. Teorema Chino del Resto.
Si $(m_i, m_j) = 1$, para $i \neq j$, $i, j \leq k$, entonces el sistema de congruencias

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

tiene solución.

Dos soluciones son congruentes módulo $m_1 \cdots m_k$.

Demostración. La demostración del teorema nos proporciona un método que nos permite calcular las soluciones del sistema.

Observemos que si $M = m_1 \cdot m_2 \cdots m_k$, entonces para todo $j \leq k$, $(\frac{M}{m_j}, m_j) = 1$. Por lo tanto, existen enteros α_j y β_j tales que $1 = \alpha_j \frac{M}{m_j} + \beta_j m_j$, es decir, $\alpha_j \frac{M}{m_j} \equiv 1 \pmod{m_j}$.

Consideremos ahora

$$x_0 = a_1 \left(\alpha_1 \frac{M}{m_1}\right) + a_2 \left(\alpha_2 \frac{M}{m_2}\right) + \cdots + a_k \left(\alpha_k \frac{M}{m_k}\right).$$

La segunda observación es que $\frac{M}{m_j}$ es múltiplo de m_i, para $i \neq j$, así, por ejemplo,

$$x_0 \equiv a_1 \left(\alpha_1 \frac{M}{m_1} \right) \pmod{m_1},$$

pero como $\alpha_1 \frac{M}{m_1} \equiv 1 \pmod{m_1}$,

$$a_1 \left(\alpha_1 \frac{M}{m_1} \right) \equiv a_1 \pmod{m_1},$$

luego $x_0 \equiv a_1 \pmod{m_1}$.

En forma análoga se obtiene que $x_0 \equiv a_i \pmod{m_i}$, para todo $i \leq k$, o sea, x_0 es una solución del sistema.

La demostración de que dos soluciones son congruentes módulo $m_1 \cdot m_2 \cdots m_k$ es análoga a la de la última parte del teorema 1.35 y se deja como ejercicio. □

Ejemplo 1.37. Encontremos la solución al problema de las ovejas y el funcionario.

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 1 \pmod{4} \\ x &\equiv 3 \pmod{5}. \end{aligned}$$

En este caso, $M = 3 \cdot 4 \cdot 5 = 60$. $\frac{M}{m_1} = 20$, $\frac{M}{m_2} = 15$ y $\frac{M}{m_3} = 12$. Como

$$\begin{aligned} 2 \cdot 20 &\equiv 1 \pmod{3} \\ 3 \cdot 15 &\equiv 1 \pmod{4} \\ 3 \cdot 12 &\equiv 1 \pmod{5}. \end{aligned}$$

$\alpha_1 = 2$, $\alpha_2 = 3$ y $\alpha_3 = 3$, luego

$$x_0 = 2 \cdot 2 \cdot 20 + 3 \cdot 15 + 3 \cdot 3 \cdot 12 \pmod{60}$$

o sea,

$$x_0 \equiv 233 \equiv 53 \pmod{60},$$

por lo tanto el rebaño tenía 53 ovejas.

1.2.3 Ejercicios

1. Encuentre enteros x e y que satisfagan las siguientes ecuaciones en dos variables. Si no existen soluciones diga por qué.
   a) $152x + 260y = 8$
   b) $432x - 378y = 18$
   c) $126x + 165y = 8$
   d) $48x + 105y = 1$
2. Demuestre que para cualquier entero positivo n, si $a \equiv b \pmod{m}$, entonces $a^n \equiv b^n \pmod{m}$

3. . Encuentre todas las soluciones de las ecuaciones

$$\begin{aligned} 3x &\equiv 1 \pmod 4 \\ 4x &\equiv 2 \pmod 6 \\ 3(x-8) &\equiv 18-x \pmod{10} \end{aligned}$$

4. Demuestre que si $13 \nmid a$ y $13 \nmid b$, entonces $a^{12} \equiv b^{12} \pmod{13}$.
5. Demuestre que si a y b son primos relativos con 91, entonces $a^{12} - b^{12}$ es divisible por 91.
6. Si de un canasto se saca huevos de a dos, de a tres y de a cinco, sobran uno, dos y tres, respectivamente, ¿cuántos huevos había en el canasto?
7. Para una fiesta se compraron galletas a 39 pesos y chicles a 47 pesos, gastándose un total de 4151 pesos, ¿cuántos paquetes de cada producto se compró?
8. Demuestre el siguiente teorema: **Teorema de Wilson.**
   Sea p un número primo. Entonces

$$(p-1)! \equiv -1 \pmod p.$$

1.3 Clases Residuales

Dijimos antes que la relación de congruencia módulo m es una relación de equivalencia. Las clases de equivalencia de esta relación juegan un papel muy importante, sobre todo en las conexiones con el álgebra.

Estudiaremos ahora estas clases de equivalencia a las que a menudo se les denomina *clases residuales* . ¿Cuántas clases de equivalencia hay?, ¿qué aspecto tienen?

Comencemos con un ejemplo, el caso $m = 4$, ¿cuál es la clase de equivalencia del entero n? Es fácil, son todos aquellos números enteros x tales que $n - x$ es divisible por 4. Si designamos por $\overline{n}$ la clase residual de n entonces

$$\begin{aligned} \overline{0} &= \{\dots, -8, -4, 0, 4, 8, \dots\} \\ \overline{1} &= \{\dots, -7, -3, 1, 5, 9, \dots\} \\ \overline{2} &= \{\dots, -6, -2, 2, 6, 10, \dots\} \\ \overline{3} &= \{\dots, -5, -1, 3, 7, 11, \dots\} \end{aligned}$$

Sabemos que las clases de equivalencia forman una partición del conjunto, por lo tanto, no hay más clases residuales que las anteriores, ya que $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ es una partición. Así por ejemplo, $\overline{47} = \overline{-1} = \overline{3}$.

En general, hay m clases residuales módulo m. En efecto, dado cualquier entero n, por el algoritmo de la división, $n = qm + r$, o sea, $n \equiv r \pmod m$, o lo que es lo mismo, $\overline{n} = \overline{r}$. Pero como sabemos que el resto o residuo (de ahí el nombre de clase residual) $0 \leq r < m$, tenemos sólo m clases residuales distintas, a saber,

$$\{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{m-1}\}.$$

Al conjunto $\{0, 1, 2, \ldots, m-1\}$ se le llama *conjunto completo de representantes* ya que contiene un elemento de cada clase residual. En general, cualquier conjunto de m números tal que ningún par de ellos es congruente modulo m, es un conjunto completo de representantes.

Volvamos a nuestro ejemplo. Observemos que si tomamos cualquier elemento de, digamos, $\overline{1}$, y lo sumamos a cualquier elemento de, digamos, $\overline{2}$ obtenemos un elemento de $\overline{3}$. Algo parecido ocurre con todas las combinaciones de clases: el resultado no depende del representante que usemos. Lo mismo ocurre si multiplicamos representantes. Este hecho no es fortuito ni una característica de las clases residuales módulo cuatro, sino una consecuencia del teorema 1.27. Este resultado nos permite definir operaciones de suma y multiplicación sobre el conjunto de todas las clases residuales módulo m, para cualquier m, como sigue:

Definición 1.38. Si $\overline{a}$ y $\overline{b}$ son dos clases residuales módulo m, definimos:

$$\begin{array}{rcrcl} \overline{a} & \oplus & \overline{b} & = & \overline{a+b} \\ \overline{a} & \otimes & \overline{b} & = & \overline{ab} \\ & \ominus & \overline{a} & = & \overline{-a} \end{array}$$

Hemos usado un símbolo nuevo para las operaciones de suma, multiplicación e inverso de clases residuales, para enfatizar el hecho de que estas son operaciones distintas de las correspondientes en los números enteros. En la mayoría de los textos se usan los mismos símbolos para operar enteros y para operar clases, porque con un poco de práctica, no hay riesgo de confundirse. Nosotros mantendremos la diferencia.

Ejemplos 1.39.

1. Consideremos las clases residuales módulo 2. Hay dos clases $\overline{0}$ y $\overline{1}$, (constituidas por los números pares y por los números impares, respectivamente). Podemos hacer tablas de las operaciones entre estas clases.

$\oplus$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\otimes$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

x	$\ominus x$
$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{1}$

2. Similarmente, las operaciones para las clases módulo 3 son:

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\otimes$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

x	$\ominus x$
$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{1}$

3. Las operaciones para las clases módulo 4 son:

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\otimes$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

x	$\ominus x$
$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{3}$
$\overline{2}$	$\overline{2}$
$\overline{3}$	$\overline{1}$

Definición 1.40. El conjunto de todas las clases residuales módulo m, dotado de las operaciones $\oplus$ y $\otimes$ lo denotaremos por $\mathbb{Z}_m$.

Es inmediato que las operaciones sobre $\mathbb{Z}_m$ heredan de $\mathbb{Z}$ algunas propiedades. Por ejemplo, al igual que la suma y la multiplicación entre números enteros, estas operaciones son asociativas y conmutativas, es decir, para cualesquiera clases $\overline{a}, \overline{b}, \overline{c}$.

$$\begin{aligned}(\overline{a} \oplus \overline{b}) \oplus \overline{c} &= \overline{a} \oplus (\overline{b} \oplus \overline{c}) \\ (\overline{a} \otimes \overline{b}) \otimes \overline{c} &= \overline{a} \otimes (\overline{b} \otimes \overline{c}) \\ \overline{a} \oplus \overline{b} &= \overline{b} \oplus \overline{a} \\ \overline{a} \otimes \overline{b} &= \overline{b} \otimes \overline{a} \\ (\overline{a} \oplus \overline{b}) \otimes \overline{c} &= (\overline{a} \otimes \overline{c}) \oplus (\overline{b} \otimes \overline{c})\end{aligned}$$

¿Será válida la ley de cancelación para clases residuales? Vale decir, si $\overline{a} \neq \overline{0}$ y $\overline{a} \otimes \overline{b} = \overline{a} \otimes \overline{c}$, ¿es cierto que $\overline{b} = \overline{c}$?

Veámoslo en $\mathbb{Z}_3$. Si $\overline{a} = \overline{1}$, entonces $\overline{b} = \overline{a} \otimes \overline{b} = \overline{a} \otimes \overline{c} = \overline{c}$.

Si $\overline{a} = \overline{2}$, entonces como $\overline{a} \otimes \overline{b} = \overline{2b}$, basta comprobar que $\overline{2b} = \overline{1}$ si y sólo si $\overline{b} = \overline{2}$ y $\overline{2b} = \overline{2}$ si y sólo si $\overline{b} = \overline{1}$, para saber que también puedo cancelar.

Esto puede fácilmente verificarse con la tabla de multiplicación anterior ya que no hay ninguna línea (o columna) en la que una misma clase se repite.

Si verificamos la tabla de multiplicación de $\mathbb{Z}_4$ en cambio, vemos que en la tercera fila se repite la clase residual $\overline{2}$ y tenemos que

$$\overline{2} \otimes \overline{1} = \overline{2} = \overline{2} \otimes \overline{3},$$

luego en $\mathbb{Z}_4$ no podemos cancelar.

La pregunta natural entonces es, ¿cuándo podemos cancelar y cuándo no podemos? Notemos que $x \otimes y = x \otimes z$ si y sólo si $x \otimes (y \ominus z) = \overline{0}$, luego $\otimes$ verifica la ley de cancelación si sólo si no existen clases residuales a y b tales que $a \otimes b = \overline{0}$. Esto motiva una definición importante.

Definición 1.41. Dos clases residuales x e y no nulas (o sea distintas de $\overline{0}$,) son divisores del cero si y sólo si $x \otimes y = \overline{0}$.

Observación 1.4. Podemos hacernos la misma pregunta respecto de los enteros, ¿existen divisores del cero en $\mathbb{Z}$? Bien sabemos que no. Tampoco hay divisores del cero en los números racionales, reales o complejos.

Entonces, dado m, existen divisores del cero en $\mathbb{Z}_m$ si y sólo si existen enteros a y b tales que $m \nmid a$ y $m \nmid b$ pero $ab \equiv 0 \pmod{m}$, o sea, $m \mid ab$.

Teorema 1.42. *En $\mathbb{Z}_n$ hay divisores del cero si y sólo si n no es primo.*

Demostración. Si n es primo y $\overline{a}$, $\overline{b}$ son clases no nulas tales que $\overline{a} \otimes \overline{b} = \overline{0}$, como vimos antes, $n \mid ab$, pero n es primo, luego $n \mid a$ o bien $n \mid b$, pero entonces $\overline{a} = \overline{0}$ o bien $\overline{b} = \overline{0}$, en cualquier caso, una contradicción. Luego si n es primo, no hay divisores del cero.

Si n no es primo, entonces existen enteros a y b tales que $n = ab$. Pero entonces $\overline{a} \otimes \overline{b} = \overline{ab} = \overline{n} = \overline{0}$, es decir, hay divisores del cero. □

Corolario 1.43. *La multiplicación en $\mathbb{Z}_n$ verifica la ley de cancelación si y sólo si n es primo.*

El teorema anterior nos indica para qué clases residuales puedo cancelar *cualquier* factor no nulo, sin embargo, es fácil ver de la tabla de $\mathbb{Z}_4$ que aunque no podemos cancelar un factor $\overline{2}$, sí podemos cancelar un factor $\overline{3}$. Dado n, ¿qué factores podemos cancelar en $\mathbb{Z}_n$?

Teorema 1.44. *Si $(a, n) = 1$, y $\overline{a} \otimes \overline{b} = \overline{a} \otimes \overline{c}$, entonces $\overline{b} = \overline{c}$*

Demostración. Es consecuencia inmediata del corolario 1.29. □

Observemos ahora que si $(a, n) = 1$, existen enteros b y c tales que $ba + cn = 1$, o lo que es lo mismo, $ba \equiv 1 \pmod{n}$, o bien $\overline{b} \otimes \overline{a} = \overline{ba} = \overline{1}$, es decir, la clase $\overline{a}$ tiene un *inverso multiplicativo.*

Definición 1.45. Una clase $\overline{a} \in \mathbb{Z}_n$ es una *unidad* si y sólo si existe una clase $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{a} \otimes \overline{b} = \overline{1}$.

Observación 1.5. De manera análoga, podemos preguntarnos cuáles son las unidades de $\mathbb{Z}$. Es claro que solamente 1 y -1 son unidades de $\mathbb{Z}$. Análogamente, las unidades de $\mathbb{Q}$ son todos los racionales distintos de 0. Lo mismo ocurre en $\mathbb{R}$ y $\mathbb{C}$.

1.3.1 Unidades de $\mathbb{Z}_n$. Función de Euler y Teorema de Euler–Fermat

Para cada n entonces, las unidades de $\mathbb{Z}_n$ son precisamente aquellas clases que son "primas relativas con" n, vale decir, todos sus elementos son primos relativos con n. Como sabemos, los enteros menores que n constituyen un conjunto completo de representantes de las clases residuales. Un conjunto de representantes de las unidades de $\mathbb{Z}_n$ se llama un *conjunto reducido de representantes.* En otras palabras, un conjunto reducido contiene un representante de cada clase que es una unidad de $\mathbb{Z}_n$. De lo anterior se deduce entonces que

$$A = \{k : 0 < k < n \text{ y } (k, n) = 1\}$$

es un sistema reducido de representantes para $\mathbb{Z}_n$.

Resulta interesante entonces saber el número de elementos de un conjunto reducido de representantes, o lo que es lo mismo, el número de enteros menores que n que son primos relativos con n. Este número tiene muchas aplicaciones interesantes pero sólo veremos la más elemental, el llamado Teorema de Euler–Fermat.

En adelante usamos la notación $|A|$ para denotar la cardinalidad del conjunto A.

Definición 1.46. Para todo entero positivo n, definimos

$$\varphi(n) = |\{m : 0 < m < n \text{ y } (m,n) = 1\}|.$$

φ se llama la *función de Euler*.

Ejemplos 1.47.

$$\begin{array}{rcccl} \varphi(12) & = & |\{1,5,7,11\}| & = 4 \\ \varphi(6) & = & |\{1,5\}| & = 2 \\ \varphi(7) & = & |\{1,2,3,4,5,6\}| & = 6 \\ \varphi(p) & = & |\{1,2,\ldots,p-1\}| & = p-1, \end{array}$$

para p primo.

Teorema 1.48.

1. *Si p es primo, entonces $\varphi(p^n) = p^n - p^{n-1}$.*
2. *Si $(m,n) = 1$, entonces $\varphi(mn) = \varphi(m)\varphi(n)$.*

Demostración.

1. Observemos que los números que no son primos relativos con p^n son los múltiplos de p. Como sólo nos interesan aquellos menores o iguales que p^n, hay p^{n-1} de ellos. Por lo tanto hay $p^n - p^{n-1}$ números menores que p^n que son primos relativos con éste.

2. Sean

$$r_1, r_2, \ldots, r_{\varphi(m)} \text{ y } s_1, s_2, \ldots, s_{\varphi(n)}$$

los residuos reducidos módulo m y módulo n, respectivamente.

Sea x un residuo módulo mn, primo relativo con mn, es decir, $(x, mn) = 1$. Luego $(x,m) = 1$ y $(x,n) = 1$, o sea,

$$\begin{array}{rcl} x & \equiv & r_i \pmod{m} \\ x & \equiv & s_j \pmod{n}, \end{array}$$

para algún $i \leq \varphi(m)$ y $j \leq \varphi(n)$. Entonces, por el Teorema Chino del Resto, existe una solución t_{ij} para este sistema, la que es única módulo mn. Es claro también que para cada i y j hay una solución distinta y que $(t_{ij}, mn) = 1$, por lo tanto hay exactamente $\varphi(m)\varphi(n)$ de estos t_{ij}, lo que termina la demostración. □

Corolario 1.49. *Si $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$, donde $p_1, \ldots, p_m$ son primos, entonces*

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_m}).$$

Teorema 1.50. Teorema de Euler–Fermat.
Si m es un entero positivo y $(a, m) = 1$, entonces

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Demostración. Sean $r_1, r_2, \ldots, r_{\varphi(m)}$ todos los residuos módulo m, que son primos relativos con m, o sea, son un conjunto reducido de representantes. Entonces $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ también son primos relativos con m.

Si $ar_i \equiv ar_j \pmod{m}$, para $i \neq j$, como $(a, m) = 1$, puedo cancelar a, obteniendo $r_i \equiv r_j \pmod{m}$, lo que es una contradicción. Luego los ar_1, ar_2, $\ldots$, $ar_{\varphi(m)}$ son todos distintos, por lo tanto también son un conjunto reducido de representantes. Pero entonces, para cada i, existe un único j tal que $ar_i \equiv r_j \pmod{m}$ y por lo tanto

$$ar_1 ar_2 \cdots ar_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m},$$

luego

$$a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m}.$$

Cancelando los r_i, obtenemos el resultado requerido. □

Un caso particular de este teorema es el llamado Pequeño Teorema de Fermat.

Corolario 1.51. Teorema de Fermat.
Sea p un número primo y a un entero tal que $p \nmid a$. Entonces

$$a^{p-1} \equiv 1 \pmod{p}.$$

Corolario 1.52. *Sea p un número primo y a un entero. Entonces*

$$a^p \equiv a \pmod{p}.$$

Demostración. Si $p \nmid a$, por el Teorema de Fermat, $a^{p-1} \equiv 1 \pmod{p}$. Multiplicando por a, queda $a^p \equiv a \pmod{p}$.

Si $p \mid a$, $a^p \equiv 0 \equiv a \pmod{p}$. □

Ejemplos 1.53.

Aplicaciones del Teorema de Fermat.

1. Calcule $5^{100} \pmod{8}$.
   Como $\varphi(8) = 4$, por el Teorema de Euler–Fermat,
   $$5^{100} = 5^{4 \cdot 25} \equiv 1 \pmod{8}.$$
2. Calcule $3^{1000} \pmod{7}$.
   Por el teorema de Fermat, $3^6 \equiv 1 \pmod{7}$, luego $3^{6k} \equiv 1 \pmod{7}$, para cualquier k, por lo tanto,
   $$\begin{aligned} 3^{1000} = 3^{6 \cdot 166 + 4} &\equiv 3^4 \pmod{7} \\ 3^{1000} &\equiv 81 \pmod{7} \\ 3^{1000} &\equiv 4 \pmod{7} \end{aligned}$$

3. Si p es primo, $(a \pm b)^p \equiv a^p \pm b^p \pmod{p}$.

   Por el teorema del binomio, sabemos que

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k,$$

   donde

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}.$$

   Observemos que p aparece en la descomposición en primos del numerador pero no en la del denominador, luego p no puede cancelarse, es decir, aparece en la descomposición de $\binom{p}{k}$, y por lo tanto, $p \mid \binom{p}{k}$, para cada $k \neq 0$ y $k \neq p$. Pero entonces

$$\binom{p}{k} \equiv 0 \pmod{p},$$

   para $1 \leq k < p$, de donde se obtiene el resultado pedido.

4. Sea p un primo mayor que 3. Demuestre que $a^p \equiv a \pmod{6p}$ para cualquier entero a.

   Los factores primos de $6p$ son 2, 3 y p. Veamos por separado cada uno. Es claro que $a^p \equiv a \pmod{2}$ para cualquier entero a, es cosa de ver que $a^p - a$ es siempre par.

   Por el corolario del teorema de Fermat, $a^p \equiv a \pmod{p}$.

   Si $3 \mid a$, entonces $a^p \equiv a \pmod{3}$. Si $3 \nmid a$, por el teorema de Fermat $a^2 \equiv 1 \pmod{2}$ pero p es impar, o sea $p = 2k+1$, así, $a^p = (a^2)^k\, a \equiv a \pmod{3}$.

   Hemos demostrado que $a^p \equiv a \pmod{2}$, $a^p \equiv a \pmod{3}$ y $a^p \equiv a \pmod{p}$, luego $a^p \equiv a \pmod{6p}$.

1.3.2 Ejercicios

1. Encuentre la intersección de la clase del 7 módulo 4 y la clase del 5 módulo 15.
2. Demuestre que si n es impar, en $\mathbb{Z}_n$, $\overline{0} + \overline{1} + \cdots + \overline{n-1} = \overline{0}$,
   ¿qué sucede si n es par?
3. Demuestre que para dos enteros positivos cualquiera n y m y para todo a, $a^n \equiv a^m \pmod{2}$.
4. Demuestre que para dos enteros positivos cualquiera n y m y para todo a,

$$a^{2n} \equiv a^{2m} \pmod{3}$$

5. a) Suponga que $17 \nmid a$. Demuestre que el número n más pequeño tal que $a^n \equiv 1 \pmod{17}$ puede ser 1, 2, 4, 8 ó 16.
   b) Suponga que $(a, 30) = 1$. Demuestre que el número n más pequeño tal que $a^n \equiv 1 \pmod{17}$ puede ser 1, 2, 4 u 8.
   c) Obtenga una regla general.
6. Encuentre el dígito de las unidades en 973^{145}.
7. Resuelva la ecuación $x^2 + x + 2 = 0$ en $\mathbb{Z}_5$. En $\mathbb{Z}_6$. En $\mathbb{Z}_p$, para p primo.
8. Demuestre que en $\mathbb{Z}_p$, con p primo, se tiene $(a+b)^p = a^p + b^p$.

Capítulo 2: Polinomios

En este capítulo estudiaremos las propiedades algebraicas de los polinomios en una variable. No desarrollaremos aquí una teoría formal de polinomios sino que, como en el caso de los números enteros, recurriremos a los conocimientos más o menos intuitivos que tenemos sobre estos desde la escuela secundaria o de cursos de álgebra elemental. Para un tratamiento más formal y riguroso, el lector puede consultar por ejemplo [**2**]. Supondremos entonces que estamos familiarizados con los conceptos de polinomio y las operaciones habituales entre ellos, suma, resta, producto, etc.

El propósito de este capítulo es hacer un paralelo entre las propiedades de las operaciones con polinomios y las operaciones entre números enteros. Aunque nos concentraremos en polinomios con coeficientes racionales y con coeficientes enteros, haremos notar cuáles de los teoremas son válidos también para polinomios con coeficientes reales, complejos o, incluso, clases residuales en $\mathbb{Z}_n$. La última sección estará dedicada al polinomios sobre los números reales y complejos para poder plantear el teorema más importante, el Teorema Fundamental del Álgebra, cuya demostración escapa a los límites de este libro.

2.1 Polinomios sobre los Racionales y los Enteros. Divisibilidad

Definición 2.1.

1. El conjunto de los *polinomios sobre* $\mathbb{Q}$ (o de los polinomios con coeficientes en $\mathbb{Q}$), denotado $\mathbb{Q}[x]$, es el conjunto de todas las expresiones

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

donde n es un entero positivo o cero y $a_0, a_1, \ldots, a_n \in \mathbb{Q}$.

Los racionales a_i se llaman los *coeficientes* del polinomio. El polinomio 0, es decir, aquel cuyos coeficientes son todos cero, se llama el *polinomio nulo*. Los polinomios tales que todos sus coeficientes, salvo eventualmente a_0, son cero se llaman *polinomios constantes*.

2. El *grado* de un polinomio $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, es el mayor k tal que $a_k \neq 0$. Este se llama el *coeficiente principal* del polinomio. Al polinomio nulo no se le asigna un grado. Todos los otros polinomios constantes no nulos tienen por lo tanto grado 0. El grado de $p(x)$ se denota por $\partial p(x)$.

De manera análoga a la anterior, podemos definir polinomios sobre $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Z}_n$, etc., los que denotaremos respectivamente $\mathbb{Z}[x]$, $\mathbb{R}[x]$, $\mathbb{Z}_n[x]$, etc.

Recordemos que dos polinomios $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ y $q(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$ son iguales siempre y cuando $n = m$ y todos los coeficientes respectivos sean iguales. Así mismo, las operaciones se definen como sigue:

$$p(x) + q(x) = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_0 + b_0),$$

aquí, si $n > m$ hacemos $b_k = 0$ para $m < k \leq n$, y similarmente si $m > n$.

$$p(x) \cdot q(x) = c_r x^r + c_{r-1}x^{r-1} + \cdots + c_0\,,$$

donde $r = n + m$ y

$$c_k = \sum_{i+j=k} a_i b_j = a_k b_0 + a_{k-1}b_1 + \cdots + a_0 b_k,$$

para $k \leq r$.

Lema 2.2.

1. *Si* $p(x) + q(x) \neq 0$, *entonces* $\partial(p(x) + q(x)) \leq \max\{\partial p(x), \partial q(x)\}$.
2. *Si* $p(x)\, q(x) \neq 0$, *entonces* $\partial(p(x)\, q(x)) = \partial p(x) + \partial q(x)$.

De la definición de las operaciones, se desprende que el polinomio nulo 0 actúa sobre los polinomios igual que el número 0 sobre los enteros, vale decir, si lo sumamos a cualquier polinomio $p(x)$, la suma es igual a este último. Por otra parte, si lo multiplicamos por un polinomio, obtenemos 0.

Algo similar se puede decir del polinomio 1, es decir, aquel cuyos coeficientes son todos 0, salvo a_0 que es 1. Si lo multiplicamos por cualquier polinomio $p(x)$, el resultado será este último. Es decir, el polinomio 1 tiene el mismo comportamiento que el entero 1.

Si consideramos ahora el polinomio

$$-p(x) = -a_n x^n - a_{n-1}x^{n-1} - \cdots - a_0,$$

notaremos que $p(x) + -p(x) = -p(x) + p(x) = 0$, o sea, $-p(x)$ es el equivalente del inverso aditivo de los números enteros.

Al igual que en las clases residuales o en los enteros, podemos decir que un polinomio $p(x)$ es una *unidad* si existe un polinomio $q(x)$ tal que $p(x)\, q(x) = 1$.

Por último, podemos observar que las operaciones entre polinomios gozan de varias de las propiedades de las operaciones entre enteros: tanto suma como multiplicación son asociativas y conmutativas, además, la segunda es distributiva respecto de la primera, el polinomio 0 juega un papel similar al del entero 0, etc.

2.1.1 Divisibilidad

Ya que contamos con una multiplicación tan parecida a la de los números enteros, es natural preguntarse hasta dónde podemos repetir las ideas sobre divisibilidad que desarrollamos en el capítulo anterior. Como bien sabemos, podemos usar la misma definición para divisibilidad entre polinomios que la usada para números enteros.

Definición 2.3. Sean $p(x)$ y $q(x)$ dos polinomios. Decimos que $p(x)$ *divide* a $q(x)$ si existe un polinomio $r(x)$ tal que $p(x)\,r(x) = q(x)$. También decimos que $q(x)$ es un *múltiplo* de $p(x)$. Denotamos este hecho por $p(x) \mid q(x)$.

Ejemplo 2.4. $x + 1 \mid x^2 - 1$, ya que $(x + 1)(x - 1) = x^2 - 1$.

Otras propiedades de $\mathbb{Q}[x]$ y sus operaciones que son similares a las de los enteros y de las clases residuales son las siguientes. Como vimos en el caso de las clases residuales, decimos que dos polinomios $p(x)$ y $q(x)$ son divisores del cero si y sólo si $p(x)\,q(x) = 0$ pero $p(x) \neq 0$ y $q(x) \neq 0$.

Teorema 2.5.

1. *En $\mathbb{Q}[x]$ no hay divisores del cero.*
2. *La multiplicación en $\mathbb{Q}[x]$ verifica la ley de cancelación.*
3. *Las unidades de $\mathbb{Q}[x]$ son los polinomios constantes no nulos.*

Demostración.

1. Si $p(x) \neq 0$ y $q(x) \neq 0$, entonces $\partial(p(x)\,q(x)) = \partial p(x) + \partial q(x) \geq 0$.

2. Esto es consecuencia inmediata de 1. En efecto, si $p(x)\,q(x) = p(x)\,r(x)$, entonces $p(x)(\,q(x) - r(x)) = p(x)\,q(x) - p(x)\,r(x) = 0$, pero como $p(x) \neq 0$ y no hay divisores del cero, uno de los dos factores es 0, por lo tanto $q(x) - r(x) = 0$, o sea, $q(x) = r(x)$.

3. Si $p(x)\,q(x) = 1$, entonces, en particular, $0 = \partial(p(x)\,q(x)) = \partial p(x) + \partial q(x)$.
Luego $\partial p(x) = \partial q(x) = 0$, o sea, las unidades de $\mathbb{Q}[x]$ deben ser polinomios constantes no nulos.
Por otra parte, si $\partial p(x) = 0$, $p(x) = a_0 \neq 0$. Si tomamos $q(x) = \frac{1}{a_0}$, tendremos $p(x)q(x) = 1$, o sea, todo polinomio constante no nulo es una unidad de $\mathbb{Q}[x]$. □

Observe que el teorema también es cierto para $\mathbb{R}[x]$ y $\mathbb{C}[x]$, sin embargo, sólo las dos primeras son ciertas para $\mathbb{Z}[x]$. Aquí las unidades son sólo los polinomios constantes 1 y -1.
¿Cuáles de las propiedades anteriores serán ciertas en $\mathbb{Z}_5[x]$?, ¿en $\mathbb{Z}_6[x]$?, ¿en $\mathbb{R}[x]$?, ¿en $\mathbb{C}[x]$?

Teorema 2.6. Algoritmo de la División.
Sean $f(x)$ y $g(x)$ polinomios en $\mathbb{Q}[x]$ y $\partial g(x) \geq 0$. Entonces existen dos únicos polinomios $q(x)$ y $r(x)$ tales que

$$f(x) = q(x)g(x) + r(x)$$

y

$$r(x) = 0 \quad \textit{o bien} \quad \partial r(x) < \partial g(x).$$

Demostración. Invitamos al lector a verificar, a medida que avanza la demostración, que los mismos argumentos pueden usarse para polinomios en $\mathbb{R}[x]$ y en $\mathbb{C}[x]$.

Consideremos el conjunto

$$S = \{f(x) - p(x)g(x) : p(x) \in \mathbb{Q}[x]\}.$$

Si $0 \in S$, entonces $g(x) \mid f(x)$ y el teorema se cumple con $r(x) = 0$. En caso contrario, los grados de los polinomios de S son un conjunto no vacío de enteros positivos o 0. Este conjunto debe tener un menor elemento, luego existe un polinomio $r(x) \in S$ que tiene grado minimal y tal que

$$r(x) = f(x) - q(x)g(x),$$

para algún polinomio $q(x)$, o lo que es lo mismo,

$$f(x) = q(x)g(x) + r(x).$$

Observemos que $r(x) \neq 0$. Debemos demostrar ahora que $\partial r(x) < \partial g(x)$.

Para una demostración por contradicción, sean

$$r(x) = c_m x^m + c_{m-1}x^{m-1} + \cdots + c_0,$$
$$g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0,$$

con $c_m \neq 0$ y $b_n \neq 0$ y supongamos que $m \geq n$.

En este caso consideramos el polinomio

$$\begin{aligned} s(x) &= r(x) - \frac{c_m}{b_n}x^{m-n}g(x) \\ &= (\underline{c_m x^m} + c_{m-1}x^{m-1} + \cdots + c_0) - (\underline{c_m x^m} + c_m\frac{b_{n-1}}{b_n}x^{m-1} + \cdots + c_m\frac{b_0}{b_n}x^{m-n}). \end{aligned}$$

Como vemos, hemos escogido los polinomios para que los términos subrayados se cancelen, de modo que el grado de $s(x)$ sea menor que el de $r(x)$. Pero además

$$\begin{aligned} s(x) = r(x) - \frac{c_m}{b_n}x^{m-n}g(x) &= f(x) - q(x)g(x) - \frac{c_m}{b_n}x^{m-n}g(x) \\ &= f(x) - (q(x) + \frac{c_m}{b_n}x^{m-n})g(x) \in S. \end{aligned}$$

Es decir, $s(x)$ es un polinomio que pertenece a S y que tiene grado menor que $r(x)$, lo que contradice la minimalidad del grado de $r(x)$. Por lo tanto, la suposición es incorrecta y debe cumplirse que $m < n$, es decir, $\partial r(x) < \partial g(x)$.

Para terminar la demostración, debemos verificar que $q(x)$ y $r(x)$ son únicos. Supongamos entonces que

$$f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$$

, o sea,

$$(q_1(x) - q_2(x))g(x) = r_2(x) - r_1(x).$$

Si estos polinomios no son nulos, entonces por el lema 2.2, el grado del polinomio de la derecha es menor que n, en cambio el de la izquierda es mayor o igual que n, lo

que es una contradicción, luego estos polinomios son nulos, es decir, $r_1(x) = r_2(x)$ y como no hay divisores del cero y $g(x) \neq 0$, se sigue que $q_1(x) = q_2(x)$. □

El algoritmo de la división no es cierto para $\mathbb{Z}[x]$, el lector podrá fácilmente verificar que para $f(x) = x^2 + 1$ y $g(x) = 3x + 2$, no se puede encontrar polinomios $q(x)$ y $r(x)$ en $\mathbb{Z}[x]$ que verifiquen el teorema 2.6.

Como es habitual, denotaremos por $p(a)$ al número que resulta de reemplazar la variable x en $p(x)$ por el número a. El número $p(a)$ se llama la *evaluación* de $p(x)$ en a.

Definición 2.7. Un racional a es una *raíz* (o un *cero*) del polinomio $p(x)$ si y sólo si $p(a) = 0$.

Teorema 2.8. *El número a es un cero de $p(x)$ si y sólo si $x - a$ es un factor de $p(x)$.*

Demostración. Aplicamos el Teorema 2.6 a $p(x)$ y $x - a$ obteniendo

$$p(x) = q(x)(x - a) + r(x),$$

con $r(x) = 0$ o bien $\partial r(x) < 1 = \partial(x - a)$, o sea, $p(x) = q(x)(x - a) + b$, para algún $b \in \mathbb{Q}$. Evaluando en a,

$$0 = p(a) = q(a)(a - a) + b = b,$$

por lo tanto, $p(x)$ es un múltiplo de $x - a$.

Recíprocamente, si $x - a \mid p(x)$, entonces $p(a) = q(a)(a - a) = 0$. □

Nuevamente observamos, que como el resultado se obtiene por aplicación del Teorema 2.6, el que como indicamos es válido sobre $\mathbb{R}$ y $\mathbb{C}$, este teorema también vale en esos contextos. De la primera parte de la demostración se desprende el siguiente corolario.

Corolario 2.9. *El resto al dividir un polinomio $p(x)$ por $x - a$ es $p(a)$.*

Corolario 2.10. *Un polinomio de grado $n \geq 1$ tiene a lo más n ceros.*

Demostración. La demostración la haremos por inducción sobre el grado del polinomio $p(x)$.

Si $\partial p(x) = 1$, $p(x) = ax + b = a(x + \frac{b}{a})$ y el único cero es $-\frac{b}{a}$.

Supongamos que todo polinomio de grado n tiene a lo más n ceros y supongamos que $\partial p(x) = n + 1$. Si $p(x)$ no tiene ceros, el teorema se cumple. Si a es un cero de $p(x)$, entonces $p(x) = q(x)(x - a)$, donde $\partial q(x) = n$. Luego los ceros de $p(x)$ son a y los ceros de $q(x)$, por lo tanto hay a lo más $n + 1$ ceros de $p(x)$. □

El siguiente teorema es muy útil para encontrar las raíces racionales de un polinomio con coeficientes enteros.

Teorema 2.11. *Sea* $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. *Si* $a = \frac{b}{c} \in \mathbb{Q}$, *donde* $(b, c) = 1$, *es una raíz de* $p(x)$, *entonces*

$$b \mid a_0 \quad y \quad c \mid a_n \,.$$

Demostración. Como a es raíz de $p(x)$,

$$p(a) = a_n \left(\frac{b}{c}\right)^n + a_{n-1}\left(\frac{b}{c}\right)^{n-1} + \cdots + a_1 \frac{b}{c} + a_0 = 0$$

y multiplicando por c^n, tenemos

$$a_n b^n + a_{n-1}b^{n-1}c + \cdots + a_1 bc^{n-1} + a_0 c^n = 0.$$

O sea,

$$b(a_n b^{n-1} + a_{n-1}b^{n-2}c + \cdots + a_1 c^{n-1}) = -a_0 c^n,$$

es decir, $b \mid a_0 c^n$ y como $(b, c) = 1$, $b \mid a_0$.

Análogamente,

$$c(a_{n-1}b^{n-1} + \cdots + a_1 bc^{n-2} + a_0 c^{n-1}) = -a_n b^n,$$

es decir, $c \mid a_n b^n$ y como $(b, c) = 1$, $c \mid a_n$. □

Ejemplo 2.12. Encuentre las raíces racionales del polinomio

$$3x^5 - x^4 + 2x^3 - 5x^2 - x - 4 \,.$$

Según el último teorema, las raíces racionales de este polinomio tienen que tener como numerador a un divisor de 4 y como denominador a un divisor de 3. Esto nos da las siguientes posibilidades:

$$\pm 1,\ \pm 2,\ \pm 4,\ \pm\frac{1}{3},\ \pm\frac{2}{3},\ \pm\frac{4}{3} \,.$$

Luego de probar con todas ellas vemos que sólo $\frac{4}{3}$ es una raíz del polinomio. El teorema garantiza que no hay más raíces racionales.

Es interesante hacer notar que si el polinomio

$$3x^{100} - x^{80} + x^{60} - x^2 + 4$$

tuviera raíces racionales ellas estarían en la lista anterior, al igual que las de cualquier polinomio que imaginemos que comience con coeficiente ± 3 y termine con coeficiente ± 4, en resumen, el grado y los coeficientes intermedios son irrelevantes. □

Corolario 2.13. *Sea* $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$, *donde* $a_0 \neq 0$. *Si* $p(x)$ *tiene una raíz en* $\mathbb{Q}$, *entonces esa raíz es entera y divide a* a_0.

Demostración. Inmediato del teorema anterior. □

2.1.2 Ejercicios

1. ¿Cuáles de las propiedades de $\mathbb{Q}[x]$ descritas en el Teorema 2.5 son ciertas en $\mathbb{Z}_5[x]$?, ¿en $\mathbb{Z}_6[x]$? , ¿en $\mathbb{R}[x]$?, ¿en $\mathbb{C}[x]$?
2. Después del teorema 2.6 hicimos notar que éste no es válido para $\mathbb{Z}[x]$. Revise la demostración para ver qué paso no es posible llevar a cabo en $\mathbb{Z}[x]$. ¿Hay casos en $\mathbb{Z}[x]$ en los que sí es posible encontrar un cuociente y un resto?
3. Al dividir el polinomio $p(x) \in \mathbb{Q}[x]$ por $x-1$ el resto es 1 y al dividirlo por $x-2$, el resto es 3. ¿cuál es el resto al dividir $p(x)$ por x^2-3x+2?
4. Determine todos los racionales x para los cuales el polinomio $p(x) = 4x^2 - 5x$ toma un valor entero.
5. Sean $p(x)$ y $q(x)$ dos polinomios en $\mathbb{Q}[x]$ tales que para todo entero positivo n, $p(n) = q(n)$. Demuestre que $p(x) = q(x)$.
6. Pruebe que si a es un raíz racional del polinomio $p(x) = a_0+a_1x+\cdots+a_{n-1}x^{n-1}+a_nx^n$ entonces $\frac{1}{a}$ es raíz de $q(x) = a_n + a_{n-1}x + \cdots + a_1x^{n-1} + a_0x^n$.
7. Determine todos los valores de a para los cuales $30x^2 - a$ tiene raíces racionales. Generalice al polinomio $30x^n - a$.

2.2 Irreducibilidad sobre los Racionales. El Criterio de Eisenstein

Definición 2.14. Un polinomio $p(x)$ no constante se dice *irreducible sobre* $\mathbb{Q}[x]$ si toda vez que $p(x) = q(x)\, r(x)$, entonces o bien $q(x)$ es una unidad de $\mathbb{Q}[x]$ o bien $r(x)$ es una unidad $\mathbb{Q}[x]$.

De manera análoga podemos definir polinomio irreducible sobre $\mathbb{Z}[x]$ o $\mathbb{R}[x]$, etc.

Teorema 2.15. *En $\mathbb{Q}[x]$ un polinomio es irreducible si y sólo si no es el producto de dos polinomios de grado menor.*

Demostración. Supongamos que $p(x)$ es irreducible y que $p(x) = q(x)\, r(x)$. Entonces uno de estos factores digamos $r(x)$ es una unidad, por lo tanto $\partial r(x) = 0$ luego $\partial p(x) = \partial q(x)$, es decir, $p(x)$ no es el producto de polinomios de grado menor.

Para demostrar la implicación en el otro sentido usaremos el contrarrecíproco. Supongamos que $p(x)$ no es irreducible. Entonces $p(x) = q(x)\, r(x)$, para ciertos polinomios ninguno de los cuales es una unidad, es decir, sus grados son distintos de cero. Como $\partial p(x) = \partial q(x) + \partial r(x)$, quiere decir que tanto $\partial p(x) > \partial q(x)$ como $\partial p(x) > \partial r(x)$. Vemos entonces que $p(x)$ se factoriza como producto de polinomios de menor grado. □

Ejemplos 2.16.

1. Debe tenerse en cuenta que el concepto de irreducibilidad es relativo al conjunto de polinomios del que estamos hablando, así, el polinomio $x^2 - 2$ es irreducible sobre $\mathbb{Q}[x]$, pero no lo es sobre $\mathbb{R}[x]$ ya que aquí,

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}),$$

y los dos últimos no son unidades de $\mathbb{R}[x]$.

2. Consideremos $p(x) = 2x^2 - 4$ en $\mathbb{Q}[x]$. Si bien $p(x)$ se puede factorizar como $p(x) = 2(x^2 - 2)$, estos factores no tienen grado menor que el de $p(x)$, por lo que $2x^2 - 4$ es irreducible sobre $\mathbb{Q}[x]$.

   En general, si $p(x)$ es irreducible sobre $\mathbb{Q}[x]$ y $0 \neq a \in \mathbb{Q}$, entonces $a \cdot p(x)$ es irreducible sobre $\mathbb{Q}[x]$.
3. Todo polinomio de primer grado es irreducible sobre $\mathbb{Q}[x]$.
4. El teorema 2.15 es válido para polinomios en $\mathbb{R}[x]$ y en $\mathbb{C}[x]$, ¿será cierto sobre $\mathbb{Z}[x]$?

El concepto de polinomio irreducible es central en la teoría de polinomios ya que ellos ocupan dentro de ésta el lugar que tienen números primos en la teoría de números; resulta, por lo tanto, importante contar con métodos para determinar si un polinomio es o no irreducible. Eso es lo que estudiaremos a continuación.

Teorema 2.17. *Sea $p(x) \in \mathbb{Q}[x]$ de grado 2 ó 3. Entonces $p(x)$ es irreducible si y sólo si $p(x)$ no tiene un cero en $\mathbb{Q}$.*

Demostración. Si a es un cero de $p(x)$, $p(x) = q(x)(x-a)$ y $\partial(x-a) = 1 < \partial p(x)$ y $\partial q(x) = \partial p(x) - 1 < \partial p(x)$. Luego por el Teorema 2.15, $p(x)$ no es irreducible.

Recíprocamente, si $p(x)$ no es irreducible, existen factores $q(x)$ y $r(x)$ de menor grado que el de $p(x)$, o sea, de grado menor que 3. Pero $\partial q(x) + \partial r(x) \leq 3$, luego uno de los dos factores es de grado 1, digamos, $r(x) = ax + b$, o sea, $-\frac{b}{a}$ es un cero de $r(x)$ y por lo tanto también de $p(x)$. □

Veremos ahora el principal criterio para ver si un polinomio es irreducible. Para ello necesitamos de algún trabajo previo.

Definición 2.18. Sea $p(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$, $p(x)$ es *primitivo* si y sólo si $(a_0, \ldots, a_n) = 1$.

Lema 2.19. *Dado un polinomio $p(x) \in \mathbb{Z}[x]$, existe un único polinomio primitivo $q(x)$ y un único entero positivo c tales que $p(x) = cq(x)$.*

Demostración. Es obvio que basta tomar $c = (a_0, \ldots, a_n)$, el máximo común divisor de los coeficientes, y factorizar c. El polinomio resultante será primitivo. □

Observe que en el teorema anterior, $p(x)$ y $q(x)$ tienen el mismo grado.

Lema 2.20. *El producto de dos polinomios primitivos es primitivo.*

Demostración. Sean

$$\begin{aligned} p(x) &= a_n x^n + \cdots + a_0 \\ q(x) &= b_m x^m + \cdots + b_0 \\ p(x)q(x) &= c_{m+n} x^{m+n} + \cdots + c_0, \end{aligned}$$

donde c_j se define en la forma usual.

Supongamos que $p(x)\,q(x)$ no es primitivo. Entonces existe un número primo p tal que $p \mid c_j$, para $0 \leq j \leq m+n$.

Pero como $(a_0, \ldots, a_n) = 1$ y $(b_0, \ldots, b_m) = 1$, existe el menor j y el menor k tales que $p \nmid a_j$ y $p \nmid b_k$, y como p es primo, $p \nmid a_j b_k$.

Ahora bien,

$$c_{j+k} = a_0 b_{j+k} + a_1 b_{j+k-1} + \cdots + a_{j-1} b_{k+1} + \underline{a_j b_k} + a_{j+1} b_{k-1} + \cdots + a_{j+k} b_0,$$

luego

$$\underline{a_j b_k} = c_{j+k} - a_0 b_{j+k} - a_1 b_{j+k-1} - \cdots - a_{j-1} b_{k+1} - a_{j+1} b_{k-1} + \cdots - a_{j+k} b_0.$$

Como $p \mid a_i$ para $i < j$, $p \mid b_i$ para $i < k$ y por hipótesis $p \mid c_{j+k}$, todos los términos del lado derecho son divisibles por p, luego $a_j b_k$ también lo es y esto es una contradicción. □

El siguiente teorema nos dice algo interesante. Un polinomio con coeficientes enteros que es irreducible en $\mathbb{Z}[x]$ también lo es en $\mathbb{Q}[x]$, a pesar de que en el segundo conjunto hay muchos más polinomios y por lo tanto podría haber muchas más descomposiciones.

Teorema 2.21. Lema de Gauss.
Sea $p(x) \in \mathbb{Z}[x]$, $\partial p(x) > 0$. Si $p(x)$ es irreducible en $\mathbb{Z}[x]$, entonces $p(x)$ también es irreducible en $\mathbb{Q}[x]$.

Demostración. Demostraremos el contrarrecíproco. Supongamos que $p(x) = q(x)\,r(x)$, para ciertos polinomios $q(x), r(x) \in \mathbb{Q}[x]$ tales que $\partial q(x), \partial r(x) < \partial p(x)$. O sea,

$$p(x) = \left(\frac{a_k}{b_k}x^k + \cdots + \frac{a_1}{b_1}x + \frac{a_0}{b_0}\right)\left(\frac{c_m}{d_m}x^m + \cdots + \frac{c_1}{d_1}x + \frac{c_0}{d_0}\right).$$

Multiplicando por $a = [b_0, \ldots, b_k][d_0, \ldots, d_m]$, el producto de los mínimo común múltiplos de los denominadores de los respectivos coeficientes, obtenemos

$$a \cdot p(x) = \left(a'_k x^k + \cdots + a'_0\right)\left(c'_m x^m + \cdots + c'_0\right),$$

donde los dos polinomios de la derecha, llamémoslos $q'(x)$ y $r'(x)$, están en $\mathbb{Z}[x]$.

Por el Lema 2.19 existen enteros positivos b, c y d y polinomios primitivos $\hat{p}(x)$, $\hat{q}(x)$ y $\hat{r}(x)$, tales que $p(x) = b \cdot \hat{p}(x)$, $q'(x) = c \cdot \hat{q}(x)$ y $r'(x) = d \cdot \hat{r}(x)$. Luego

$$a \cdot p(x) = ab \cdot \hat{p}(x) = cd \cdot \hat{q}(x)\hat{r}(x),$$

pero por el Lema 2.20 $\hat{q}(x)\hat{r}(x)$ es primitivo y $\hat{p}(x)$ también lo es, luego $ab = cd$, por la unicidad de las constantes del Lema 2.19, es decir, $\hat{p}(x) = \hat{q}(x)\hat{r}(x)$, pero entonces, multiplicando por b,

$$p(x) = b \cdot \hat{p}(x) = b\hat{q}(x)\hat{r}(x),$$

y $b \cdot \hat{q}(x)$, $\hat{r}(x) \in \mathbb{Z}[x]$, o sea, $p(x)$ se descompone como producto de polinomios de menor grado en $\mathbb{Z}[x]$. □

Ejemplo 2.22. Demostrar que $p(x) = x^4 - 2x^2 + 8x + 1$ es irreducible sobre $\mathbb{Q}[x]$.
Demostración. Por el Lema de Gauss, basta demostrar que $p(x)$ es irreducible sobre $\mathbb{Z}[x]$. Supongamos que $p(x) = q(x)\ r(x)$. Si $\partial r(x) = 1$, $p(x)$ tiene un cero en $\mathbb{Z}$ que divide a 1. Luego ese cero debe ser ± 1. Pero observamos que $p(1) = 8 \neq 0$ y $p(-1) = -8 \neq 0$, luego ni 1 ni -1 son ceros de $p(x)$, es decir, el grado de $r(x)$ no puede ser 1. En ese caso, la única posibilidad es que $p(x)$ se factorize como

$$p(x) = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + d + ac)x^2 + (bc + ad)x + bd,$$

es decir,

$$\begin{aligned} a + c &= 0 \\ b + d + ac &= -2 \\ bc + ad &= 8 \\ bd &= 1. \end{aligned}$$

La última ecuación implica que o bien $b = d = 1$, o bien $b = d = -1$ y reemplazando en la ecuación anterior, obtenemos $a + c = \pm 8 \neq 0$, lo que es una contradicción. Por lo tanto $p(x)$ no se puede descomponer como producto de polinomios de menor grado luego es irreducible. □

Las ideas desarrolladas más arriba sirven para polinomios de grados muy pequeños o para casos en los que se puede encontrar una raíz. El siguiente es uno de los teoremas más generales para determinar la irreducibilidad de polinomios de grados grandes mediante un simple análisis de sus coeficientes.

Teorema 2.23. Criterio de Eisenstein.

Sean $q(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ *y* p *un número primo tal que:*

1. $p \nmid a_n$,
2. $p \mid a_i$, *para* $0 \leq i < n$ *y*
3. $p^2 \nmid a_0$.

Entonces $q(x)$ *es irreducible en* $\mathbb{Q}[x]$.

Demostración. Por el Teorema 2.21, basta ver que $q(x)$ es irreducible en $\mathbb{Z}[x]$.

Supongamos entonces que $q(x)$ no es irreducible. Entonces

$$q(x) = (b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0)(c_k x^k + c_{k-1}x^{k-1} + \cdots + c_0),$$

en donde $m < n$ y $k < n$.

Como $a_0 = b_0 c_0$ y el primo $p \mid a_0$, entonces o bien $p \mid b_0$ o bien $p \mid c_0$ pero no a ambos ya que $p^2 \nmid a_0$. Digamos que $p \mid c_0$ y $p \nmid b_0$.

Por otra parte, como $p \nmid a_n = b_m c_k$, tenemos $p \nmid b_m$ y $p \nmid c_k$.

Sea r el menor índice i tal que $p \nmid c_i$. Por la discusión anterior, tal índice existe y $0 < r \leq k$. Observe que esto significa que $p \mid c_0, p \mid c_1, \ldots, p \mid c_{r-1}$.

Por lo tanto si consideramos

$$a_r = b_0c_r + b_1c_{r-1} + \cdots + b_rc_0,$$

como $p \nmid b_0c_r$, entonces $p \nmid a_r$, pero por las hipótesis 1 y 2, esto sólo puede ocurrir si $r = n$, lo que es una contradicción. □

Ejemplos 2.24.

1. Considere el polinomio $p(x) = 3x^3 + 6x^2 + 4x + 2$. Entonces $p(x)$ es irreducible al aplicar el criterio de Eisenstein con $p = 2$.
2. Así mismo, $x^n + p$ es irreducible para todo entero positivo n y primo p. Esto prueba que hay polinomios de cualquier grado que son irreducibles sobre $\mathbb{Q}$.
3. Si p es primo, el polinomio $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, es irreducible.

   El criterio de Eisenstein no puede ser aplicado directamente en este caso. Sin embargo, si notamos que

   $$\Phi_p(x) = \frac{x^p - 1}{x - 1},$$

   y consideramos

   $$\begin{aligned} q(x) = \Phi_p(x+1) &= \frac{(x+1)^p - 1}{x+1-1} = \frac{x^p + \binom{p}{p-1}x^{p-1} + \cdots + \binom{p}{2}x^2 + \binom{p}{1}x^1}{x} \\ &= x^{p-1} + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{2}x + \binom{p}{1}. \end{aligned}$$

   Observamos que p no divide al coeficiente principal. Todos los otros coeficientes son de la forma

   $$\binom{p}{k} = \frac{p!}{k!(p-k)!},$$

   con $0 < k < p$. Vemos que el primo p no puede aparecer entre los factores del denominador, luego p sí es uno de los factores primos del número $\binom{p}{k}$. Por lo tanto p divide a todos los otros coeficientes de $q(x)$. Por último, $a_0 = \binom{p}{1} = p$, o sea, $p^2 \nmid a_0$. Por lo tanto $q(x)$ es irreducible por el criterio de Eisenstein.

   Si $\Phi_p(x)$ fuese reducible, $q(x)$ también lo sería.

2.2.1 Teorema de Factorización Única

Si bien en el caso de dos polinomios $p(x)$ y $q(x)$ en $\mathbb{Q}[x]$ existen divisores comunes, no podemos hablar de un "máximo común divisor" por la sencilla razón de que los polinomios no están bien ordenados, al menos no de una manera obvia. Podemos entonces pensar en el polinomio de mayor grado que es divisor común de los dos polinomios $p(x)$ y $q(x)$. Resulta obvio que el concepto anterior no está bien definido, consideremos el ejemplo siguiente:

$$p(x) = 2x^3 + x^2 + 2x + 1 \quad \text{y} \quad q(x) = 2x^2 + x\,.$$

Un simple cálculo nos permitirá determinar que $2x+1$ divide a ambos polinomios y que ningún polinomio de grado mayor los dividirá a ambos. Sin embargo, este polinomio no es el único con esa propiedad ya que, por ejemplo, $x+\frac{1}{2}$ tiene el mismo grado y también es un divisor común de $p(x)$ y $q(x)$. De hecho, para cada $a \in \mathbb{Q}$, $a \neq 0$, el polinomio $2ax+a$ es otro divisor común de $p(x)$ y $q(x)$ del mismo grado. De entre todos estos (infinitos) polinomios, podemos individualizar uno, aquel cuyo primer coeficiente es 1.

Definición 2.25. El polinomio $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}[x]$ se dice *mónico* si y sólo si $a_n = 1$.

El siguiente lema es inmediato.

Lema 2.26. *El producto de polinomios mónicos es mónico.*

Definición 2.27. Definimos el *máximo común divisor*, $MCD\{p(x), q(x)\}$, de los polinomios $p(x)$ y $q(x)$ en $\mathbb{Q}[x]$, como el polinomio mónico de mayor grado que divide a ambos polinomios.

Veremos a continuación que esta definición tiene sentido, es decir, dados dos polinomios no nulos, su máximo común divisor siempre existe. Más aún, veremos que éste tiene muchas de las propiedades del máximo común divisor para números enteros.

Teorema 2.28.

1. *Si $p(x)$ y $q(x)$ pertenecen a $\mathbb{Q}[x]$, entonces $MCD\{p(x), q(x)\}$ es el polinomio mónico de grado más pequeño que puede escribirse como $\alpha(x)p(x)+\beta(x)q(x)$, donde $\alpha(x)$, $\beta(x) \in \mathbb{Q}[x]$.*
2. *Cualquier divisor común de $p(x)$ y $q(x)$ divide a $MCD\{p(x), q(x)\})$.*
3. *Si $r(x)$ es un divisor común de $p(x)$ y de $q(x)$ y es del mismo grado que $MCD\{(p(x), q(x)\}$, entonces existe $a \in \mathbb{Q}$ tal que $r(x) = a\, MCD\{p(x), q(x)\}$.*

Demostración. Nuevamente hacemos notar que la demostración que sigue puede perfectamente llevarse a cabo con polinomios en $\mathbb{R}[x]$ o en $\mathbb{C}[x]$.

Sólo demostraremos 1 ya que 2 y 3 son inmediatas. Para este efecto definimos el conjunto

$$S = \{r(x) \in \mathbb{Q}[x] : r(x) = \alpha(x)p(x) + \beta(x)q(x),\ \alpha(x), \beta(x) \in \mathbb{Q}[x] \text{ y } \partial r(x) \geq 0\}.$$

Consideremos un polinomio de grado minimo que pertenezca a este conjunto. Si dividimos por el coeficiente principal, obtendremos un polinomio mónico de grado minimo que pertenece a S. Este debe ser único ya que si $d_1(x)$ y $d_2(x)$ son dos tales polinomios, $d_1(x) - d_2(x) \in S$ es un polinomio de menor grado.

Denotemos $d(x)$ al único polinomio mónico de grado minimal en S. Demostraremos a continuación que $d(x) = MCD\{p(x), q(x)\}$. La demostración sigue fielmente las ideas usadas en el teorema análogo para $\mathbb{Z}$ (ver Teorema 1.9 en el Capítulo 1).

Por el algoritmo de la división, existen polinomios $r(x), s(x) \in \mathbb{Q}[x]$ tales que o bien $r(x) = 0$ o bien $\partial r(x) < \partial d(x)$ y

$$p(x) = s(x)d(x) + r(x).$$

Pero entonces

$$\begin{aligned} r(x) &= p(x) - s(x)d(x) \\ &= p(x) - s(x)[\alpha(x)p(x) + \beta(x)q(x)] \\ &= [1 - s(x)\alpha(x)]p(x) - [s(x)\beta(x)]q(x) \in S\,. \end{aligned}$$

Si $r(x) \neq 0$, se contradice la minimalidad del grado de $d(x)$, por lo tanto $r(x) = 0$ y $d(x) \mid p(x)$.

Análogamente, demostramos que $d(x) \mid q(x)$.

Para verificar que $d(x)$ es el polinomio de mayor grado que divide a $p(x)$ y $q(x)$, basta notar que si $r(x)$ es otro divisor común, entonces divide a todos los elementos de S, en particular divide a $d(x)$, y por lo tanto $\partial r(x) \leq \partial d(x)$. □

El siguiente teorema es similar al Lema 1.13, Lema de Euclides, para los enteros.

Teorema 2.29. *Si $p(x)$ es un polinomio irreducible sobre $\mathbb{Q}[x]$ y $p(x) \mid r(x)s(x)$, entonces $p(x) \mid r(x)$ o bien $p(x) \mid s(x)$.*

Demostración. Supongamos que $p(x) \nmid r(x)$. Entonces, como el polinomio $p(x)$ es irreducible, $MCD\{p(x), r(x)\} = 1$. Luego existen $\alpha(x)$, $\beta(x) \in \mathbb{Q}[x]$ tales que

$$\begin{aligned} 1 &= \alpha(x)p(x) + \beta(x)r(x) \\ s(x) &= \alpha(x)p(x)s(x) + \beta(x)r(x)s(x) \\ s(x) &= [\alpha(x)s(x) + \beta(x)q(x)]p(x), \end{aligned}$$

donde $q(x)p(x) = r(x)s(x)$. Por lo tanto $p(x) \mid s(x)$. □

Observación 2.1. Algoritmo de Euclides.
El lector puede comprobar que el máximo común divisor entre dos polinomios puede encontrarse usando *exactamente* el mismo algoritmo de Euclides que se usó en el Capítulo 1. Lo ilustraremos con un ejemplo.

Ejemplo 2.30. Encuentre el máximo común divisor de los polinomios

$$p(x) = 2x^6 + x^5 - 2x^4 + 3x^3 + x + 1 \quad \text{y} \quad q(x) = 2x^4 + x^3 - 4x^2 + 2x + 2\,.$$

$$\begin{aligned} 2x^6 + x^5 - 2x^4 + 3x^3 + x + 1 &= (2x^4 + x^3 - 4x^2 + 2x + 2)(x^2 + 1) + 2x^2 - x - 1 \\ 2x^4 + x^3 - 4x^2 + 2x + 2 &= (2x^2 - x - 1)(x^2 + x - 1) + 2x + 1 \\ 2x^2 - x - 1 &= (2x + 1)(x - 1) + 0 \end{aligned}$$

Observamos que el último resto que es diferente de cero es el polinomio $2x+1$ por lo tanto, el máximo común divisor de los polinomios anteriores es el polinomio mónico asociado $x + 1/2$.

El siguiente teorema, el más importante de esta sección, nos indica el rol de los polinomios irreducibles dentro de la teoría de polinomios.

Teorema 2.31. Teorema de Factorización Única.
Todo polinomio en $\mathbb{Q}[x]$ de grado mayor que 1 se puede factorizar como una constante por un producto de polinomios mónicos irreducibles. Tal factorización es única salvo por el orden de los factores.

Demostración. Haremos la demostración por inducción sobre el grado del polinomio $p(x)$. Nuevamente hacemos notar que los mismos argumentos pueden usarse para polinomios en $\mathbb{R}[x]$ y en $\mathbb{C}[x]$.

Si $\partial p(x) = 1$, $p(x) = ax + b$, donde $a \neq 0$, entonces

$$p(x) = a\left(x + \frac{b}{a}\right),$$

y como sabemos, los polinomios de primer grado son irreducibles.

Supongamos entonces que el teorema es válido para polinomios de grado menor que n y sea $\partial p(x) = n$.

Si $p(x)$ es irreducible, factorizamos por el coeficiente principal, como en el caso de primer grado.

Si no, existen polinomios $p_1(x)$ y $p_2(x)$, de grado menor que n, tales que $p(x) = p_1(x)\, p_2(x)$.

Por hipótesis de inducción, existen constantes a y b y polinomios mónicos irreducibles $q_1(x), \ldots, q_k(x)$ y $r_1(x), \ldots, r_m(x)$ tales que

$$p_1(x) = aq_1(x) \cdots q_k(x) \quad \text{y} \quad p_2(x) = br_1(x) \cdots r_m(x),$$

y por lo tanto

$$p(x) = abq_1(x) \cdots q_k(x) r_1(x) \cdots r_m(x),$$

que es lo que queríamos demostrar.

Para demostrar unicidad, supongamos que

$$aq_1(x) \cdots q_k(x) = br_1(x) \cdots r_m(x).$$

son dos descomposiciones de $p(x)$.

En primer lugar, como todos los polinomios son mónicos, $a = b$ y lo podemos cancelar. Además $q_1(x) \mid r_1(x) \cdots r_m(x)$, y por el teorema 2.29, existe algún i tal que $q_1(x) \mid r_i(x)$. Como el orden de los factores no interesa, podemos suponer que $i = 1$. Ahora bien, $r_1(x)$ es irreducible y mónico, por lo tanto $q_1(x) = r_1(x)$. Cancelando,

$$q_2(x) \cdots q_k(x) = r_2(x) \cdots r_m(x).$$

Vemos que si aplicamos el procedimiento anterior un número finito de veces, se cancelan todos los polinomios, luego $k = m$ y para $i \leq m$, $q_i(x) = r_i(x)$, lo que completa la demostración de unicidad de la descomposición. □

2.2.2 Ejercicios

1. Dé un ejemplo en el cual el teorema 2.15 no es válido para polinomios en $\mathbb{Z}[x]$.
2. Diga si los siguientes polinomios son irreducibles sobre $\mathbb{Q}$.
   a) x^3+3x^2-x-3, *b)* x^3+3x^2-x+3,
   c) $2x^5+6x^4-12x+15$, *d)* x^4+4.
3. Diga si el polinomio x^2+x+1 es irreducible sobre $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$.
4. Demuestre que hay infinitos polinomios de la forma $x^5+12x^4-21x^3+63x+k$ que son irreducibles sobre $\mathbb{Q}[x]$.
5. Demuestre que si $n\geq 2$, entonces $\sqrt[n]{p}$ es irracional para todo número primo p.
6. Sea $p(x)\in\mathbb{Q}[x]$ y suponga que $p(x+c)$ es irreducible sobre $\mathbb{Q}[x]$. Demuestre que $p(x)$ es irreducible sobre $\mathbb{Q}[x]$.
7. Encuentre el máximo común divisor de los siguientes pares de polinomios y exprése-lo como combinación de ellos.
   a) $p(x)=2x^3-4x^2+x+2$ y $q(x)=x^3-x^2-x-2$,
   b) $p(x)=x^4+x^3+x^2+x+1$ y $q(x)=x^3-1$,
   c) $p(x)=x^2-x+4$ y $q(x)=x^4+x+1$,
   d) $p(x)=x^3-1$ y $q(x)=x^5-x^4+x^3-x^2+x-1$.
8. Factorize los siguientes polinomios en sus factores irreducibles en $\mathbb{Q}[x]$.
   a) $x^5+2x^4+x^3$, *b)* $2x^4-x^3-x^2-x+-2$,
   c) x^4+2x^2-24, *d)* $x^6-x^5+x^4-2x^3+x^2-x+1$.

2.3 Irreducibilidad sobre los Reales y sobre los Complejos

Como vimos en la Sección 2, la irreducibilidad de un polinomio depende del conjunto de referencia, es decir, del conjunto del cual estamos tomando los coeficientes. Así, x^2-2 es irreducible si lo consideramos como un polinomio en $\mathbb{Z}[x]$ o $\mathbb{Q}[x]$, pero no lo es si lo consideramos como polinomio en $\mathbb{R}[x]$ o $\mathbb{C}[x]$.

En secciones anteriores hemos visto lo que sucede con polinomios en $\mathbb{Q}[x]$. Veremos ahora que podemos describir explícitamente todos lo polinomios irreducibles en $\mathbb{R}[x]$ y en $\mathbb{C}[x]$. Esto se logra usando un teorema muy importante cuya demostración requiere de herramientas matemáticas más avanzadas de las que disponemos. La primera demostración la dio Gauss en 1799.

Supondremos en esta sección que el lector está familiarizado con los conceptos elementales acerca de los números complejos, así como con su aritmética. Usaremos también los teoremas que hemos demostrado en el contexto de los polinomios sobre $\mathbb{Q}$, pero que como hemos indicado, también son válidos aquí. Invitamos al lector a asegurarse que esas demostraciones valen para reales y complejos.

Teorema 2.32. Teorema Fundamental del Álgebra.
Todo polinomio no constante de $\mathbb{C}[x]$ *tiene una raíz en* $\mathbb{C}$.

Corolario 2.33. *Un polinomio es irreducible sobre* $\mathbb{C}[x]$ *si y sólo si es de primer grado.*

Demostración. Si $p(x) \in \mathbb{C}[x]$ es de grado mayor que 1, como tiene una raíz, por el teorema 2.8, $p(x)$ no es irreducible. Es claro que los polinomios de primer grado son irreducibles. □

Corolario 2.34. *Todo polinomio* $p(x) \in \mathbb{C}[x]$ *de grado* n *se puede escribir en la forma*

$$p(x) = c(x - a_1)(x - a_2)\cdots(x - a_n)\,,$$

donde $c, a_1, a_2, \ldots, a_n \in \mathbb{C}$. *Esta descomposición es única salvo por el orden de los factores.*

Demostración. Esto se obtiene usando el teorema 2.31 y el corolario anterior. □

Debe observarse que los números complejos a_i de este corolario no son necesariamente distintos. También es obvio que cada uno de ellos es una raíz del polinomio. Resumimos esto en el siguiente corolario.

Corolario 2.35. *Un polinomio* $p(x) \in \mathbb{C}[x]$ *de grado* n *tiene exactamente* n *raíces complejas considerando las repeticiones.*

Estudiaremos a continuación los polinomios irreducibles sobre $\mathbb{R}[x]$, para ello necesitamos previamente algunos resultados sobre raíces complejas de estos polinomios.

Lema 2.36. *Si* $p(x) \in \mathbb{R}[x]$ *y* $a + bi$ *es una raíz compleja de* $p(x)$, *entonces su conjugado* $a - bi$ *también es una raíz de* $p(x)$.

Demostración. Recordemos que si z_1 y z_2 son complejos entonces sus conjugados verifican

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2} \quad \text{y} \quad \overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2},$$

por lo tanto, si

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

y $z = a + bi$ es una raíz de $p(x)$,

$$0 = \overline{0} = \overline{p(z)} = \overline{a_n}\overline{z^n} + \overline{a_{n-1}}\overline{z^{n-1}} + \cdots + \overline{a_1 z} + \overline{a_0},$$

pero como los a_i son reales, $\overline{a_i} = a_i$, luego

$$0 = \overline{p(z)} = a_n \overline{z}^n + a_{n-1}\overline{z}^{n-1} + \cdots + a_1\overline{z} + a_0 = p(\overline{z}),$$

por lo tanto $\overline{z} = a - bi$ también es raíz de $p(x)$. □

Teorema 2.37. *Un polinomio $p(x) \in \mathbb{R}[x]$ es irreducible sobre $\mathbb{R}[x]$ si y sólo si se verifica una de las siguientes condiciones:*

1. *$p(x)$ es de primer grado,*
2. *$p(x) = ax^2 + bx + c$, donde $b^2 - 4ac < 0$.*

Demostración. Es obvio que los polinomios de primer grado son irreducibles. Si $p(x)$ es del tipo indicado en 2, sabemos que tiene dos raíces complejas conjugadas α y $\overline{\alpha}$ luego

$$p(x) = a(x - \alpha)(x - \overline{\alpha}),$$

y como esta descomposición es única en $\mathbb{C}[x]$, $p(x)$ no puede descomponerse como producto de otros factores en $\mathbb{R}[x]$, luego es irreducible sobre $\mathbb{R}[x]$. Esto demuestra que estos dos tipos de polinomio son irreducibles sobre $\mathbb{R}[x]$.

Veamos ahora que si $p(x)$ no es de esa forma, entonces es reducible.

Si $p(x) = ax^2 + bx + c$ y $b^2 - 4ac \geq 0$, entonces $p(x)$ tiene dos raíces reales a_1 y a_2 luego $p(x) = a(x - a_1)(x - a_2)$, o sea $p(x)$ no es irreducible sobre $\mathbb{R}[x]$. Podemos entonces concentrarnos en polinomios de grado mayor que 2.

Supongamos que $\partial(p(x)) \geq 3$. Por el teorema 2.32, $p(x)$ tiene una raíz compleja $\alpha = a + bi$ y por el lema anterior, $\overline{\alpha} = a - bi$ es también una raíz de $p(x)$, por lo tanto

$$p(x) = (x - (a + bi))(x - (a - bi))h(x),$$

donde $h(x) \in \mathbb{C}[x]$ y $\partial(h(x)) > 0$. Demostraremos ahora que $h(x) \in \mathbb{R}[x]$.

Observamos que

$$g(x) = (x - (a + bi))(x - (a - bi)) = x^2 - 2ax + (a^2 + b^2),$$

o sea, $g(x) \in \mathbb{R}[x]$ y

$$p(x) = g(x)h(x). \qquad (*)$$

Recordemos que el algoritmo de la división también es válido para polinomios en $\mathbb{R}[x]$ y en $\mathbb{C}[x]$. Lo aplicamos primero en $\mathbb{R}[x]$. Dados $p(x)$ y $g(x)$ existen polinomios únicos $q(x)$ y $r(x)$ en $\mathbb{R}[x]$ tales que

$$p(x) = g(x)q(x) + r(x), \qquad (**)$$

con $r(x) = 0$ ó $\partial(r(x)) < \partial(g(x))$.

Observemos que $p(x)$, $g(x)$, $q(x)$ y $r(x)$ son también polinomios en $\mathbb{C}[x]$, luego comparando $(*)$ y $(**)$, si aplicamos la unicidad del cuociente y el resto en algoritmo de la división en $\mathbb{C}[x]$, tenemos

$$r(x) = 0 \quad \text{y} \quad h(x) = q(x) \in \mathbb{R}[x]\,,$$

como queríamos. Por lo tanto $p(x)$ no es irreducible. □

Corolario 2.38. *Todo polinomio de* $\mathbb{R}[x]$ *de grado impar tiene una raíz real.*

Demostración. Por el teorema 2.31, que también es válido para polinomios en $\mathbb{R}[x]$,

$$p(x) = p_1(x)p_2(x)\cdots p_k(x),$$

donde los polinomios $p_i(x)$ son irreducibles en $\mathbb{R}[x]$, luego de grado 1 o 2.

Como

$$\partial(p(x)) = \partial(p_1(x)) + \partial(p_2(x)) + \cdots + \partial(p_k(x))$$

es impar, uno de los factores $p_i(x)$ tiene que ser de primer grado, luego $p(x)$ tiene una raíz en $\mathbb{R}$. □

2.3.1 Ejercicios

1. Verifique que todos los teoremas sobre polinomios en $\mathbb{Q}[x]$ que fueron usados en esta sección para polinomios sobre $\mathbb{R}[x]$ y $\mathbb{C}[x]$, son efectivamente válidos en estos contextos.
2. Factorize los siguientes polinomios en sus factores irreducibles en $\mathbb{C}[x]$.

   a) $x^2 + i\,,$ *b)* $x^3 - 1\,,$

   c) $x^3 - i\,,$ *d)* $x^2 + x + 1 + i\,.$
3. Demuestre que un polinomio en $\mathbb{R}[x]$ de grado impar y sin raíces múltiples debe tener un número impar de raíces reales.
4. Encuentre polinomios en $\mathbb{R}[x]$ con las siguientes características:
   a) Mónico, de grado 3 y con 1 y $2+3i$ como raíces.
   b) Mónico, de grado mínimo con i y $1+i$ como raíces.
   c) Con raíces $1+i$, 2 y -3 (esta última es raíz doble), ¿es único el resultado?, ¿cambia el resultado si el polinomio puede pertenecer a $\mathbb{C}[x]$?

Capítulo 3: Anillos

En este capítulo, desarrollaremos algunos aspectos de una teoría general que englobe a todos los ejemplos que hemos visto en los capítulos anteriores, a otros que el lector ha estudiado en distinto contexto y nuevos ejemplos de conjuntos dotados de operaciones con las que se puede establecer una aritmética similar a la de los números enteros. La idea entonces, es que todos estos ejemplos tienen una misma "estructura" algebraica a la que se ha dado el nombre de *anillo*. El concepto de anillo fue introducido por R. Dedekind. También Hilbert empleó la palabra *Zahlring*, anillo de números en alemán, en el contexto de las clases residuales, probablemente en alusión a su naturaleza "cíclica". El primero en dar una definición abstracta del concepto de anillo fue A. Fraenkel en 1914 y la axiomatización actual que veremos a continuación apareció tres años más tarde.

3.1 Definiciones y Ejemplos

Definición 3.1. Un *anillo* es un conjunto no vacío A dotado de dos operaciones que denotamos $+$ y $\cdot$ que satisfacen las siguientes condiciones:

Para todo $a, b, c \in A$

1. $(a+b)+c = a+(b+c)$. *asociatividad de la suma*
2. Existe un elemento $\mathbf{0} \in A$ tal que, *neutro aditivo*
$$a + \mathbf{0} = \mathbf{0} + a = a.$$
3. Para cada $a \in A$ existe $b \in A$ tal que *inverso aditivo*
$$a + b = b + a = \mathbf{0}.$$
4. $a + b = b + a$. *conmutatividad de la suma*
5. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. *asociatividad del producto*
6. $a \cdot (b+c) = a \cdot b + a \cdot c$.
$(b+c) \cdot a = b \cdot a + c \cdot a$. *distributividad del producto sobre la suma*

El anillo se dice *conmutativo* si

7. $a \cdot b = b \cdot a$. *conmutatividad del producto*

Si existe un elemento $\mathbf{1} \in A$ tal que

8. $a \cdot \mathbf{1} = \mathbf{1} \cdot a$. *neutro multiplicativo*

el anillo se dice *unitario*.

Demostraremos después de los ejemplos que hay un único neutro aditivo. Análogamente, si el neutro multiplicativo existe, este es único. Observe que en virtud de

la definición, si b es inverso aditivo de a entonces a es a su vez inverso aditivo de b. Después de los ejemplos demostraremos también que cada elemento tiene un único inverso aditivo y por lo tanto podemos denotarlo por $-a$, asimismo, abreviaremos la expresión $a + (-b)$ por $a - b$ y la llamaremos la *diferencia* entre a y b.

Como veremos en los ejemplos, sobre un mismo conjunto A puede definirse distintas operaciones y por lo tanto obtener distintos anillos. Debemos entonces hacer explícitas las operaciones sobre A de las que estamos hablando, así, en estricto rigor, un anillo es una terna $\langle A, +, \cdot \rangle$. Sin embargo, es habitual hablar del anillo A cuando no hay posibilidad de confusión respecto de las operaciones.

Seguiremos la convención de escribir $a\,b$ en lugar de $a \cdot b$.

Ejemplos 3.2.

1. En los dos capítulos anteriores hemos estudiado los ejemplos clásicos de anillos. Todos ellos son conmutativos y unitarios.
   Los enteros $\langle \mathbb{Z}, +, \cdot \rangle$.
   Las clases residuales $\langle \mathbb{Z}_n, \oplus, \otimes, \rangle$.
   Los polinomios $\langle \mathbb{Q}[x], +, \cdot \rangle$. También $\mathbb{Z}[x]$, $\mathbb{R}[x]$, etc.
2. Los conjuntos de números $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ dotados de las operaciones habituales también son anillos conmutativos y unitarios.
3. Definimos $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$ y lo dotamos de la suma y producto de $\mathbb{Z}$. Este es un anillo conmutativo y *no* unitario.
   Análogamente, para cualquier entero positivo k podemos definir el anillo $k\mathbb{Z} = \{k\,n \ : \ n \in \mathbb{Z}\}$.
4. Dado un anillo cualquiera A, podemos generalizar el trabajo del Capítulo 2 y definir el conjunto $A[x]$ de los polinomios sobre A.

$$A[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \ : \ n \in \mathbb{N},\, a_0, a_1, \ldots, a_n \in A\},$$

   y las operaciones se definen como para polinomios sobre $\mathbb{Q}$. $A[x]$ es el *anillo de los polinomios sobre A*.
5. El conjunto $M_2(\mathbb{R})$, de las matrices cuadradas de orden 2 sobre los reales, con las operaciones de suma y producto matricial habituales, es un anillo no conmutativo y unitario, donde

$$\mathbf{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \qquad \mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

   Naturalmente, podemos extender esta idea a matrices cuadradas de orden n. También podemos cambiar el conjunto de las componentes. Por ejemplo, $M_5(\mathbb{C})$ son las matrices de orden 5 con elementos complejos.
6. El siguiente ejemplo requiere de ciertas nociones elementales de cálculo. Consideramos el conjunto $C[0,1]$ de todas las funciones continuas

$$f : [0,1] \longrightarrow \mathbb{R},$$

donde las operaciones $f+g$ y $f\cdot g$ están definidas punto a punto:

$$\begin{aligned}(f+g)(x) &= f(x)+g(x),\\ (f\cdot g)(x) &= f(x)g(x).\end{aligned}$$

Este es un anillo conmutativo y unitario, ¿cuáles son sus neutros aditivo y multiplicativo?

7. Los llamados *enteros de Gauss*, $\mathbb{Z}[i]=\{m+ni : m,n\in\mathbb{Z}\}$, con las operaciones habituales de los números complejos es también un anillo.
8. Consideremos ahora el conjunto $\mathbb{Z}$ de los números enteros pero con nuevas operaciones definidas como sigue:

$$\begin{aligned}a\oplus b &= a+b,\\ a\otimes b &= 0.\end{aligned}$$

Éste es un anillo conmutativo, no unitario.

9. Definimos $\mathbb{Z}\times\mathbb{Z}=\{(a,b) : a,b\in\mathbb{Z}\}$ con operaciones por coordenadas, es decir,

$$\begin{aligned}(a,b)+(c,d) &= (a+c,b+d),\\ (a,b)\cdot(c,d) &= (ac,bd).\end{aligned}$$

$\mathbb{Z}\times\mathbb{Z}$ así definido es un anillo.

Resulta obvio que este ejemplo es un caso particular de una construcción mucho más general. Dados dos anillos cualquiera A y B, podemos definir el anillo $A\times B$, llamado el *producto directo de A y B*, con las operaciones definidas de manera análoga a la anterior.

Teorema 3.3. *En todo anillo A se verifica:*

1. *Existe un único neutro aditivo.*
2. *El inverso aditivo de a es único.*
3. $a\,\mathbf{0}=\mathbf{0}\,a=\mathbf{0}$.
4. $a(-b)=(-a)b=-(ab)$.
5. $(-a)(-b)=ab$.
6. $-(-a)=a$.
7. *Si A es unitario, entonces el neutro multiplicativo es único.*
8. *Si A es unitario,* $(-\mathbf{1})\,a=-a$.
9. $(a+b)^2=a^2+ab+ba+b^2$.

Demostración.

1. Supongamos que existe un elemento c tal que para todo $a\in A$, $a+c=c+a=a$, entonces en particular para $a=\mathbf{0}$,

$$c=\mathbf{0}+c=\mathbf{0}.$$

La primera igualdad se verifica por la definición de $\mathbf{0}$ y la segunda es por hipótesis.

2. Supongamos que a tiene dos inversos aditivos b y c. Entonces

$$\begin{aligned} b &= b + \mathbf{0} \\ &= b + (a + c) \\ &= (b + a) + c \\ &= \mathbf{0} + c \\ &= c. \end{aligned}$$

   Luego el inverso es único. Observe que es esta unicidad la que nos da derecho a hablar de *el* inverso aditivo de a y llamarle $-a$. El lector debe revisar cuáles reglas de la definición de anillo se ha usado en cada línea de la demostración.
3.

$$\begin{aligned} a\,\mathbf{0} &= a(\mathbf{0} + \mathbf{0}) \\ &= a\,\mathbf{0} + a\,\mathbf{0}, \end{aligned}$$

   sumando $-(a\,\mathbf{0})$ a cada miembro de la ecuación anterior, tenemos

$$\begin{aligned} -(a\,\mathbf{0}) + a\,\mathbf{0} &= -(a\mathbf{0}) + (a\,\mathbf{0} + a\,\mathbf{0}) \\ \mathbf{0} &= (-(a\,\mathbf{0}) + a\,\mathbf{0}) + a\,\mathbf{0} \\ \mathbf{0} &= \mathbf{0} + a\,\mathbf{0} \\ \mathbf{0} &= a\,\mathbf{0}, \end{aligned}$$

   lo que termina la demostración. De manera análoga se demuestra que $\mathbf{0} = \mathbf{0}\,a$.
4. Observemos que

$$\begin{aligned} ab + a(-b) &= a(b + (-b)) \\ &= a\,\mathbf{0} \\ &= \mathbf{0}. \end{aligned}$$

   Análogamente, $a(-b) + ab = \mathbf{0}$, es decir, $a(-b)$ es un inverso aditivo de ab, pero éste es único, luego $a(-b) = -(ab)$.

   De la misma manera, $(-a)b = -(ab)$, luego son todos iguales entre sí.
5. Idem 4.
6. Tanto $-(-a)$ como a son inversos aditivos de $-a$ y como el inverso es único, ellos deben ser iguales.
7. Similar a la prueba de 1.
8. Verificamos que $(-\mathbf{1})\,a$ es inverso aditivo a, luego $(-\mathbf{1})\,a = -a$.
9.

$$\begin{aligned} (a + b)^2 &= (a + b)(a + b) \\ &= a(a + b) + b(a + b) \\ &= aa + ab + ba + bb, \end{aligned}$$

   que es lo que queríamos demostrar.

□

Los puntos 5 y 6 corresponden al famoso principio de que "menos por menos da más", que de seguro le produjo problemas a más de un lector durante la escuela secundaria. Como vemos este es un resultado natural de los axiomas, particularmente de la distributividad del producto sobre la suma.

Recordaremos aquí conceptos que introdujimos en capítulos anteriores pero ahora dentro de este contexto más general.

Definición 3.4.

1. Sea A un anillo. Decimos que $a \in A$ es *divisor del cero* si $a \neq \mathbf{0}$ y existe $b \neq \mathbf{0}$ tal que $ab = \mathbf{0}$.
2. Un anillo conmutativo y unitario que no tiene divisores del cero es un *dominio de integridad* o simplemente un *dominio*.
3. En un anillo unitario A con neutro multiplicativo $\mathbf{1}$, decimos que un elemento u es una *unidad* si existe un elemento v tal que
$$uv = vu = \mathbf{1}.$$
Tal elemento se llama *inverso multiplicativo* de u. El conjunto de todas las unidades de A se denota A^*.
4. Un *cuerpo* es un anillo conmutativo y unitario tal que todos sus elementos distintos del cero son unidades. Por ejemplo, los racionales $\mathbb{Q}$, los reales $\mathbb{R}$ y los complejos $\mathbb{C}$, dotados de sus operaciones usuales son cuerpos. En este libro sólo haremos comentarios menores acerca de los cuerpos, allí donde ayuden a aclarar aspectos de la teoría de anillos. Si bien podemos pensar los cuerpos como un tipo particular de anillo, lo cierto es que los cuerpos son estructuras algebraicas tanto o más importantes que los anillos. El lector puede consultar [**10**], [**2**] y otras obras para información sobre cuerpos.

Ya hemos visto ejemplos de anillos que son dominios: $\mathbb{Z}$, $\mathbb{Z}_5$ y $\mathbb{Q}[x]$. También otros de anillos conmutativos que no son dominios, por ejemplo, $\mathbb{Z}_4$.

Los anillos no conmutativos también pueden tener divisores del cero. Consideremos, por ejemplo, el anillo $M_2(\mathbb{R})$. Aquí
$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$
luego estas matrices son divisores del cero.

En $\mathbb{Z}$, las únicas unidades son 1 y -1. En general, en cualquier anillo unitario, el neutro multiplicativo $\mathbf{1}$ es una unidad.

3.1.1 Ejercicios

1. Diga cuáles de los siguientes conjuntos son anillos con respecto a las operaciones habituales.
   a) $\{m + n\sqrt{2} : m, n \in \mathbb{Z}\}$,
   b) $\{m + n\sqrt[3]{2} : m, n \in \mathbb{Z}\}$,
   c) $\{m + n\sqrt[3]{2} + p\sqrt[3]{4} : m, n, p \in \mathbb{Z}\}$,
   d) $\{\frac{m}{n} : m, n \in \mathbb{Z},\ (m, n) = 1 \text{ y } n \text{ es impar}\}$,
   e) $\{\frac{m}{p^r} : m \in \mathbb{Z},\ r \geq 1,\ p \text{ un primo fijo}\}$.
2. En $\mathbb{Z} \times \mathbb{Z}$ definimos las siguientes operaciones.

$$\begin{aligned}(a, b) + (c, d) &= (a + c, b + d),\\ (a, b) \cdot (c, d) &= (ac + bd, ad + bc + bd).\end{aligned}$$

   Verifique que este es un anillo conmutativo, ¿es este un dominio de integridad?
3. En $\mathbb{Z}$ definimos las nuevas operaciones:

$$\begin{aligned}a \oplus b &= a + b - 1,\\ a \otimes b &= a + b - ab.\end{aligned}$$

   Verifique que este es un anillo conmutativo y unitario. Encuentre sus neutros aditivo y multiplicativo, ¿es este un dominio de integridad?
4. Verifique que los siguientes conjuntos de números enteros, con las operaciones habituales, satisfacen todos los axiomas de anillos excepto uno.
   a) El conjunto de todos los números impares más 0.
   b) El conjunto de todos los enteros no negativos.
5. Dé dos ejemplos de anillos unitarios en los que $\mathbf{1} = -\mathbf{1}$.
6. Encuentre todas las unidades de los anillos
   a) $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$,
   b) $\mathbb{Z}_3$, $\mathbb{Z}_6$, $\mathbb{Z}_{11}$, $\mathbb{Z}_{12}$ y en general, $\mathbb{Z}_n$,
   c) $M_2(\mathbb{R})$.
7. Demuestre que el inverso de una unidad es una unidad.
8. Demuestre que las unidades se pueden cancelar, es decir, si u es una unidad y $ua = ub$ o bien $au = bu$, entonces $a = b$.

3.2 Subanillos e Ideales

En la sección anterior vimos ejemplos de anillos que están contenidos en otros anillos más grandes, por ejemplo, $\mathbb{Z}$ está contenido en $\mathbb{Q}$. Formalizaremos aquí estas ideas.

3.2.1 Definiciones y Ejemplos

Definición 3.5. Si A es un anillo, un subconjunto no vacío B de A es un *subanillo* de A si y sólo si B es un anillo si se le considera dotado de las mismas operaciones de A restringidas a B. Esto significa que si a y $b \in B$, entonces $a + b \in B$ y $a\,b \in B$.

Escribimos en este caso $B \leq A$.

Esta definición implica que B está cerrado bajo las dos operaciones, contiene al neutro $\mathbf{0}$ y contiene los inversos aditivos de todos sus elementos.

Teorema 3.6. *B es un subanillo de A si sólo si $B \subseteq A$, $B \neq \emptyset$ y B es cerrado bajo la diferencia y el producto, i.e., para todo $x, y \in B$,*

$$x - y \in B \quad y \quad xy \in B.$$

Demostración. Que la primera afirmación implica la segunda es obvio.
Supongamos entonces que para todo $x, y \in B$, $x - y \in B$ y $xy \in B$.
Como B no es vacío, tomemos $a \in B$. Por la primera propiedad,

$$\mathbf{0} = a - a \in B,$$

es decir, B tiene elemento neutro. Además, usando nuevamente la primera propiedad,

$$-a = \mathbf{0} - a \in B,$$

o sea, B contiene los inversos aditivos de todos sus elementos. Por último, para todo $a, b \in B$

$$a + b = a - (-b) \in B,$$

o sea, B es cerrado bajo la suma. Como por hipótesis B también es cerrado bajo el producto, las operaciones están bien definidas.

Observemos ahora que las propiedades de asociatividad de la suma y del producto, la conmutatividad de la suma y la distributividad del producto sobre la suma se verifican en todo el anillo A, luego con mayor razón se verifican sobre B. Por último, como vimos antes, el neutro $\mathbf{0} \in B$ y B es cerrado bajo inversos aditivos. Por lo tanto, B es un anillo. □

Ejemplos 3.7.

1. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.
2. Para cualquier entero positivo k, $k\mathbb{Z} \leq \mathbb{Z}$.
3. $\mathbb{Z}[i] \leq \mathbb{C}$.
4. $\{\overline{0}, \overline{2}\} \leq \mathbb{Z}_4$.
5. Todo anillo A tiene por lo menos dos subanillos, $\{\mathbf{0}\}$ y A. El anillo $\{\mathbf{0}\}$ es conocido como el *anillo trivial*.
6. Definimos $\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$. Entonces $\mathbb{Q} \leq \mathbb{Q}[\sqrt{3}] \leq \mathbb{R}$.

Definición 3.8. Si A es un anillo, un subconjunto no vacío $\mathcal{I}$ de A es un *ideal* de A si y sólo si

1. Para todo a,$b \in \mathcal{I}$, $a - b \in \mathcal{I}$.
2. Para todo $a \in \mathcal{I}$ y $r \in A$, $ar \in \mathcal{I}$ y $ra \in \mathcal{I}$.

Esta última propiedad es conocida como *absorción*, decimos que los ideales son absorbentes.

Observe que todo ideal de A es un subanillo. El recíproco no es cierto, por ejemplo, $\mathbb{Z}$ es un subanillo de $\mathbb{Q}$, pero no es ideal de $\mathbb{Q}$ ya que

$$3 \in \mathbb{Z} \text{ y } \frac{2}{5} \in \mathbb{Q}, \quad \text{pero } 3 \cdot \frac{2}{5} = \frac{6}{5} \notin \mathbb{Z}.$$

Ejemplos 3.9.

1. El ejemplo clásico de ideal de $\mathbb{Z}$ es $k\mathbb{Z}$ para algún entero positivo k.
2. Sea $\mathcal{I} = \{p(x) \in \mathbb{Q}[x] : \text{el término constante de } p(x) \text{ es } 0\}$. Entonces $\mathcal{I}$ es un ideal de $\mathbb{Q}[x]$.
3. $\mathbb{Z} \times \{0\}$ es un ideal de $\mathbb{Z} \times \mathbb{Z}$. (Con las operaciones por coordenadas definidas más arriba en los ejemplos 3.2).
4. $\Delta = \{(n, n) : n \in \mathbb{Z}\}$ es un subanillo de $\mathbb{Z} \times \mathbb{Z}$ que no es un ideal de $\mathbb{Z} \times \mathbb{Z}$.
5. Todo anillo A tiene por lo menos dos ideales, $\{\mathbf{0}\}$ y A. Estos se conocen como los *ideales triviales* de A.
6. Un cuerpo no tiene ideales no triviales. En efecto, si $\mathcal{I}$ es un ideal no trivial de un cuerpo K, entonces existe $k \in K$, con $k \neq \mathbf{0}$. Pero entonces existe $k^{-1} \in K$ y por absorción, $\mathbf{1} = k^{-1}\, k \in \mathcal{I}$.

   Sea $a \in A$, entonces por absorción nuevamente $a = a\mathbf{1} \in \mathcal{I}$, o sea, $A \subseteq \mathcal{I}$ y por lo tanto $A = \mathcal{I}$ y el ideal es trivial.

En el último ejemplo se demuestra el siguiente lema que es a veces útil.

Lema 3.10. *Si $\mathcal{I}$ es un ideal del anillo unitario A y $\mathbf{1} \in \mathcal{I}$, entonces $\mathcal{I} = A$.*

3.2.2 Ideales Principales e Ideales Maximales

El siguiente teorema nos dice que la intersección de (un conjunto arbitrario de) ideales de un anillo es también un ideal.

Teorema 3.11. *Sea J un conjunto cualquiera de índices. Si para cada $j \in J$, $\mathcal{I}_j$ es un ideal, entonces $\mathcal{I} = \bigcap_{j \in J} \mathcal{I}_j$ es un ideal.*

Demostración. Como $\mathbf{0} \in \mathcal{I}_j$, para todo j, tenemos que $\mathbf{0} \in \bigcap_{j \in J} \mathcal{I}_j$, luego este último es no–vacío.

Si x e $y \in \mathcal{I}$, entonces x e $y \in \mathcal{I}_j$ para todo j, tenemos que $x - y \in \mathcal{I}_j$, para todo j, luego $x - y \in \bigcap_{j \in J} \mathcal{I}_j$, luego este último es cerrado bajo diferencias.

Si $a \in A$ y $x \in \mathcal{I}$, entonces $x \in \mathcal{I}_j$ para todo j, tenemos que $a\,x$ y $x\,a \in \mathcal{I}_j$, para todo j, luego $a\,x$ y $x\,a \in \bigcap_{j \in J} \mathcal{I}_j$, luego este último es absorbente por ambos lados.

Por lo tanto, $\mathcal{I}$ es un ideal de A. □

Resulta natural preguntarse si la unión de ideales es o no un ideal. El siguiente ejemplo demuestra que ni siquiera la unión de tan sólo dos ideales tiene que ser un ideal.

Consideremos los ideales $2\mathbb{Z}$ y $3\mathbb{Z}$ de $\mathbb{Z}$. Entonces como $2,\ 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$, si éste fuera un ideal,

$$1 = 3 - 2 \in 2\mathbb{Z} \cup 3\mathbb{Z},$$

ya que los ideales son cerrados bajo diferencias, pero $1 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$, luego $2\mathbb{Z} \cup 3\mathbb{Z}$ no es un ideal de $\mathbb{Z}$, de hecho ni siquiera es un subanillo de $\mathbb{Z}$.

Definición 3.12. Si X es un subconjunto de un anillo A, llamamos *ideal generado por* X al ideal más pequeño de A que contiene a X. Lo denotaremos $\langle X \rangle$.

Si $X = \{a\}$ el ideal generado por X se llama *ideal principal* generado por a y se le denota $\langle a \rangle$.

Es fácil ver que si $X \subseteq A$ entonces el ideal de A generado por X siempre existe, para ello basta considerar

$$\bigcap \{\mathcal{I} :\ \mathcal{I} \text{ es ideal de } A \text{ y } X \subseteq \mathcal{I}\}.$$

Por el teorema 3.11 esta intersección es un ideal que obviamente contiene a X. Falta sólo ver que este es el ideal más pequeño que contiene a X. Esto es inmediato.

Teorema 3.13. *Si A es un anillo conmutativo y unitario, entonces el ideal principal generado por a es*

$$\langle a \rangle = \{xa : x \in A\}.$$

Demostración. Sea $\mathcal{I} = \{xa : x \in A\}$. Es claro que $\mathcal{I} \neq \emptyset$ ya que $a = \mathbf{1}a \in \mathcal{I}$.

Si $u = xa$ y $v = ya$ son elementos de $\mathcal{I}$, entonces $u - v = xa - ya = (x - y)a \in \mathcal{I}$.

Si $u = xa \in \mathcal{I}$ y $b \in A$, entonces $bu = ub = b(xa) = (bx)a \in \mathcal{I}$. Es decir, $\mathcal{I}$ es no vacío, cerrado bajo diferencias y absorbente, luego $\mathcal{I}$ es un ideal de A que además contiene a a. Es claro que cualquier ideal que contenga a a, deberá contener a $\mathcal{I}$, luego este es el ideal más pequeño que contiene a a, por lo tanto, $\mathcal{I} = \langle a \rangle$. □

Teorema 3.14.

1. *Todos los ideales de $\mathbb{Z}$ son principales.*
2. *Todos los ideales de $\mathbb{Q}[x]$ son principales.*

Demostración. Probaremos sólo 1, ya que la demostración de 2 es totalmente análoga.

Sea $\mathcal{I}$ un ideal de $\mathbb{Z}$. Si $\mathcal{I} = \{0\}$, entonces $\mathcal{I} = 0\ \mathbb{Z}$ es un ideal principal.

Si no, existe $a \in \mathcal{I}$, $a \neq 0$ y podemos suponer que a es positivo pues si no lo es, su inverso, que también pertenece a $\mathcal{I}$, es positivo. Por lo tanto $A = \{m \in \mathcal{I} : m > 0\}$ es un conjunto no vacío de enteros positivos y, por lo tanto, tiene un menor elemento al que llamaremos n.

Demostraremos ahora que todo elemento de $\mathcal{I}$ es un múltiplo de n.

Sea $m \in \mathcal{I}$. Por el algoritmo de la división, existen enteros q y r, donde $0 \leq r < n$, tales que $m = nq + r$.

Supongamos que $r \neq 0$. Entonces por la definición de ideal, como $n \in \mathcal{I}$, $nq \in \mathcal{I}$ y por lo tanto

$$0 < r = m - nq \in \mathcal{I}.$$

Pero esto contradice la minimalidad de n. Luego $r = 0$ y m es un múltiplo de n.

Observe que en esta demostración se ocupan las dos condiciones que definen un ideal: la absorción y que es cerrado bajo diferencias. □

El lector podría quedarse con la idea de que todos lo ideales de cualquier anillo son principales, en efecto, no hemos dado todavía un ejemplo de un ideal no principal.

Ejemplo 3.15. Consideremos el anillo $\mathbb{Z}[x]$ y el ideal generado por $\{2, x\}$. Es fácil comprobar que

$$\langle\{2, x\}\rangle = \{2p(x) + xq(x) : p(x), q(x) \in \mathbb{Z}[x]\}.$$

En particular esto implica que, $\langle\{2, x\}\rangle \neq \mathbb{Z}[x]\}$, ya que, por ejemplo, $1 \notin \langle\{2, x\}\rangle$.

Supongamos que $\langle\{2, x\}\rangle$ es principal. Entonces existe un polinomio $p(x) \in \mathbb{Z}[x]$ tal que

$$\langle\{2, x\}\rangle = \langle p(x)\rangle.$$

Como $2 \in \langle\{2, x\}\rangle$, $p(x) \mid 2$, lo que implica que $p(x)$ es un polinomio constante. Es más, o bien $p(x) = 1$ o $p(x) = 2$.

Por otra parte, $x \in \langle\{2, x\}\rangle$, luego $p(x) \mid x$, vale decir, $p(x)$ debe ser 1. Pero entonces $\langle p(x)\rangle = \mathbb{Z}[x]$, lo que es una contradicción.

Definición 3.16. Un ideal $\mathcal{M}$ de un anillo A se dice *maximal* si y sólo si $\mathcal{M} \neq A$ y para todo ideal $\mathcal{N}$ de A, si $\mathcal{M} \subsetneq \mathcal{N} \subseteq A$, entonces $\mathcal{N} = A$.

En otras palabras, un ideal es maximal si no está contenido en ningún otro ideal no trivial.

Ejemplos 3.17.
1. El ideal $3\mathbb{Z}$ de $\mathbb{Z}$ es maximal.
2. El ideal $\langle x^2 + 1\rangle$ de $\mathbb{Q}[x]$ es maximal.
3. El ideal $4\,\mathbb{Z}$ de $\mathbb{Z}$ no es maximal ya que $4\,\mathbb{Z} \subsetneq 2\,\mathbb{Z} \neq \mathbb{Z}$.

Más generalmente podemos demostrar el siguiente teorema.

Teorema 3.18.
1. *Si $\mathcal{M}$ es un ideal de $\mathbb{Z}$, entonces $\mathcal{M}$ es maximal si sólo si $\mathcal{M} = p\,\mathbb{Z}$, para algún primo p.*
2. *Si $\mathcal{M}$ es ideal de $\mathbb{Q}[x]$, entonces $\mathcal{M}$ es maximal si y sólo si $\mathcal{M} = \langle p(x)\rangle$, para algún polinomio irreducible $p(x)$.*

Demostración. 1. Sea $\mathcal{M}$ un ideal de $\mathbb{Z}$. Sabemos que todo ideal de $\mathbb{Z}$ es principal, o sea, $\mathcal{M} = m\,\mathbb{Z}$, para algún m.

Si m no es primo, digamos $m = pq$, donde $p \neq \pm 1$, $q \neq \pm 1$, entonces $p\,\mathbb{Z}$ es un ideal de $\mathbb{Z}$ tal que

$$\mathcal{M} \subsetneqq p\,\mathbb{Z} \neq \mathbb{Z},$$

luego $\mathcal{M}$ no es maximal.

Si m es primo y $\mathcal{N} = n\,\mathbb{Z}$ es otro ideal de $\mathbb{Z}$ tal que

$$\mathcal{M} = m\,\mathbb{Z} \subsetneqq n\,\mathbb{Z},$$

entonces $m \in n\mathbb{Z}$, por lo tanto $n \mid m$, pero m es primo, luego $n = 1$, y por lo tanto, $\mathcal{N} = \mathbb{Z}$, o sea $\mathcal{M}$ es maximal.

2. La demostración es análoga a la de 1 y se deja como ejercicio. □

3.2.3 Anillos Cuociente

En el Capítulo 1 vimos que las clases residuales podían dotarse de operaciones que heredan las principales propiedades de los enteros, pero adquieren otras, por ejemplo, pueden aparecer divisores del cero, o nuevas unidades. Sucede que ese no es más que un ejemplo de una construcción totalmente general que se puede hacer en cualquier anillo. Esta consiste en definir una relación de equivalencia y luego dotar al conjunto de clases de equivalencia de operaciones que le den estructura de anillo con propiedades especiales, que no tiene el anillo original. Esta construcción se hace no sólo con anillos sino con grupos, esto lo veremos en el Capítulo 5, y con otras estructuras algebraicas. Más aún, se construyen estructuras cuociente en todos los campos de la matemática, no sólo en el álgebra. En la próxima subsección veremos su aplicación más notable en el contexto de los anillos.

Teorema 3.19. *Sea A un anillo, $\mathcal{I}$ un ideal de A, entonces la relación*

$$a \sim b \;\; \textit{si y sólo si} \;\; a - b \in \mathcal{I},$$

es una relación de equivalencia.

Más aún, si $a_1 \sim b_1$ y $a_2 \sim b_2$, entonces

$$\begin{aligned} -a_1 &\sim -b_1, \\ a_1 + a_2 &\sim b_1 + b_2, \\ a_1 a_2 &\sim b_1 b_2. \end{aligned}$$

Demostración. Para todo $a \in A$, $a - a = \mathbf{0} \in \mathcal{I}$, luego $\sim$ es reflexiva.

Si $a - b \in \mathcal{I}$, entonces $b - a \in \mathcal{I}$, luego $\sim$ es simétrica.

Si $a - b \in \mathcal{I}$ y $b - c \in \mathcal{I}$, su suma, $a - c \in \mathcal{I}$, luego, $\sim$ es transitiva.

Supongamos ahora que $a_1 \sim b_1$. O sea, $a_1 - b_1 \in \mathcal{I}$. Entonces $-(a_1 - b_1) \in \mathcal{I}$, luego $(-a_1) - (-b_1) \in \mathcal{I}$, o sea, $-a_1 \sim -b_1$.

Si $a_1 \sim b_1$ y $a_2 \sim b_2$, entonces

$$(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) \in \mathcal{I},$$

ya que $\mathcal{I}$ es cerrado bajo sumas.

Por último, si $a_1 \sim b_1$ y $a_2 \sim b_2$, entonces por absorción,

$$\begin{aligned} a_1a_2 - b_1a_2 &= (a_1 - b_1)a_2 \in \mathcal{I} \\ b_1a_2 - b_1b_2 &= b_1(a_2 - b_2) \in \mathcal{I}, \end{aligned}$$

y sumando,

$$a_1a_2 - b_1b_2 \in \mathcal{I}.$$

□

Observe que en la demostración anterior hemos usado toda la fuerza de la definición de ideal.

También debemos notar que la clase de equivalencia de un elemento $a \in A$ es

$$\{b \in A : a \sim b\} = \{b \in A : a - b \in \mathcal{I}\} = \{a + i : i \in \mathcal{I}\}.$$

Esto motiva la siguiente notación.

Definición 3.20. Sea A un anillo, $\mathcal{I}$ un ideal de A, denotaremos $a + \mathcal{I}$ la clase de equivalencia de a y la llamaremos *clase de a módulo* $\mathcal{I}$. El conjunto de todas las clases de equivalencia se denotará $A \mid \mathcal{I}$.

Teorema 3.21. *Sea A un anillo, $\mathcal{I}$ un ideal de A, entonces $A \mid \mathcal{I}$ dotado de las operaciones*

$$\begin{aligned} (a + \mathcal{I}) + (b + \mathcal{I}) &= (a + b) + \mathcal{I} \\ (a + \mathcal{I}) \cdot (b + \mathcal{I}) &= ab + \mathcal{I}, \end{aligned}$$

es un anillo.[1] *Este se llama el* anillo cuociente *de A por $\mathcal{I}$.*

En este anillo, el neutro aditivo es la clase de $\mathbf{0}$ *es decir* $\mathbf{0} + \mathcal{I} = \mathcal{I}$. *Además el inverso aditivo es* $-(a + \mathcal{I}) = -a + \mathcal{I}$.

Si A es conmutativo, entonces $A \mid \mathcal{I}$ es conmutativo. Si A es unitario, entonces $A \mid \mathcal{I}$ es unitario.

Demostración. Lo importante de demostrar aquí es que las operaciones están bien definidas. En efecto, definimos la suma de dos clases cuyos representantes son a y b, respectivamente, como la clase cuyo representante es $a+b$. Lo mismo para el producto, ¿cómo sabemos que si cambiamos de representantes vamos a tener la misma clase como resultado?

[1] Es necesario hacer notar que en la definición de la suma, el símbolo "+" es usado en tres sentidos distintos. En la primera, tercera y quinta apariciones, por ejemplo en $a + \mathcal{I}$, $+$ no indica una suma en absoluto, es sólo un símbolo útil para denotar la clase. En la segunda aparición, $(a + \mathcal{I}) + (b + \mathcal{I})$ denota la suma de clases que estamos definiendo. En la cuarta aparición $(a+b) + \mathcal{I}$, denota la suma en el anillo original A.

Supongamos que $a \sim a'$ y que $b \sim b'$. Entonces sus clases $a+\mathcal{I} = a'+\mathcal{I}$ y $b+\mathcal{I} = b'+\mathcal{I}$. Pero por el Teorema 3.19, $a+b \sim a'+b'$ y, por lo tanto, sus clases son iguales, o sea, $(a+b)+\mathcal{I} = (a'+b')+\mathcal{I}$, por lo tanto

$$(a+\mathcal{I})+(b+\mathcal{I}) = (a+b)+\mathcal{I} = (a'+b')+\mathcal{I} = (a'+\mathcal{I})+(b'+\mathcal{I})$$

y la suma está bien definida pues no depende de los representantes de las clases.

Algo análogo se puede hacer para la multiplicación.

Ahora que tenemos operaciones bien definidas debemos demostrar que $A \mid \mathcal{I}$ es un anillo. Vemos que las propiedades de A son heredadas por $A \mid \mathcal{I}$. Por ejemplo, la asociatividad de ambas operaciones se sigue inmediatamente porque es traspasada por la asociatividad de las operaciones respectivas de los representantes.

$$\begin{aligned}(\,(a+\mathcal{I})+(b+\mathcal{I})\,)+(c+\mathcal{I}) &= (\,(a+b)+\mathcal{I})+(c+\mathcal{I}) = \\ (\,((a+b)+c)+\mathcal{I}) &= (\,(a+(b+c))+\mathcal{I}) = \\ (a+\mathcal{I})+(\,(b+c)+\mathcal{I}) &= (a+\mathcal{I})+(\,(b+\mathcal{I})+(c+\mathcal{I})\,)\,.\end{aligned}$$

□

Debemos observar que la relación definida anteriormente, en el caso del anillo $\mathbb{Z}$ y del ideal $\mathcal{I} = n\,\mathbb{Z}$, coincide con las congruencias módulo n. Así mismo, $\mathbb{Z} \mid n\,\mathbb{Z} = \mathbb{Z}_n$ y $\overline{m} = m + n\mathbb{Z}$.

3.2.4 Cuociente módulo un ideal maximal

Probablemente el caso más importante, es aquel en que el cuociente se hace módulo un ideal maximal. En este caso se obtiene una estructura mucho más rica, la de cuerpo, es decir un anillo conmutativo y unitario en el que todos los elementos no nulos tienen inverso multiplicativo

Teorema 3.22. *Sea A un dominio y $\mathcal{M}$ un ideal de A. Entonces $\mathcal{M}$ es maximal si y sólo si $A \mid \mathcal{M}$ es un cuerpo.*

Demostración. Supongamos que $\mathcal{M}$ es un ideal maximal de A. Sea $a+\mathcal{M}$ un elemento no nulo del cuociente $A \mid \mathcal{M}$. Esto quiere decir que $a \notin \mathcal{M}$ pues si no, $a+\mathcal{M} = \mathcal{M}$ que es el neutro en el cuociente.

Consideremos ahora el ideal $\mathcal{N}$ generado por $\mathcal{M} \cup \{a\}$. Es claro que $\mathcal{M} \subsetneq \mathcal{N}$, pero como $\mathcal{M}$ es maximal, necesariamente $\mathcal{N} = A$. En particular esto implica que $\mathbf{1} \in \mathcal{N}$.

Veamos ahora la estructura de $\mathcal{N}$. Es fácil ver que $\mathcal{N}$ es igual a

$$\mathcal{N}' = \{xa+m \,:\, x \in A\,, m \in \mathcal{M}\}\,.$$

En efecto, el conjunto así definido es no vacío ya que contiene tanto a a como $\mathcal{M}$. $\mathcal{N}'$ es cerrado bajo diferencias porque $(xa+m_1)-(ya+m_2) = (x-y)a+(m_1-m_2)$. Por último, $\mathcal{N}'$ absorbe, ya que $y(xa+m) = yxa+ym = za+m'$ ya que $\mathcal{M}$ absorbe. Como $\mathcal{N}$ es el más pequeño ideal que contiene a $\mathcal{M} \cup \{a\}$, $\mathcal{N}' = \mathcal{N}$.

Pero entonces $\mathbf{1} = xa + m$ para algún $\in A$ y algún $m \in \mathcal{M}$ esto equivale a decir que $\mathbf{1} - xa \in \mathcal{M}$, o sea, $\mathbf{1} + \mathcal{M} = xa + \mathcal{M} = (x + \mathcal{M})(a + \mathcal{M})$. Pero esto nos dice que $x + \mathcal{M}$ es el inverso de $a + \mathcal{M}$ en $A \mid \mathcal{M}$. Hemos demostrado que todo elemento no nulo de $A \mid \mathcal{M}$ es una unidad, es decir, $A \mid \mathcal{M}$ es un cuerpo.

Supongamos ahora que $A \mid \mathcal{M}$ es un cuerpo pero que $\mathcal{M}$ no es un ideal maximal. Entonces existe un ideal $\mathcal{N}$ de A tal que $\mathcal{M} \subsetneq \mathcal{N} \subsetneq A$.

Observemos que $\mathcal{N}$ es en particular un anillo, más aún, $\mathcal{M}$ es también un ideal de $\mathcal{N}$, por lo tanto podemos formar el cuociente $\mathcal{N} \mid \mathcal{M}$. Todo esto es inmediato de las definiciones, lo interesante para esta demostración es que $\mathcal{N} \mid \mathcal{M}$ es un ideal de $A \mid \mathcal{M}$.

En efecto, es claro que $\mathcal{N} \mid \mathcal{M}$ no es vacío. Si $(n_1 + \mathcal{M})$, y $(n_2 + \mathcal{M}) \in \mathcal{N} \mid \mathcal{M}$, entonces $n_1 - n_2 \in \mathcal{N}$ y por lo tanto $(n_1 + \mathcal{M}) - (n_2 + \mathcal{M}) = (n_1 - n_2) + \mathcal{M} \in \mathcal{N} \mid \mathcal{M}$, o sea, $(n_1 + \mathcal{M})$, y $(n_2 + \mathcal{M}) \in \mathcal{N} \mid \mathcal{M}$ es cerrado bajo diferencias. Para ver que también absorbe, vemos que el producto de $(x + \mathcal{M}) \in A \mid \mathcal{M}$ por $(n + \mathcal{M}) \in \mathcal{N} \mid \mathcal{M}$ es $(x + \mathcal{M})(n + \mathcal{M}) = (xn + \mathcal{M}) \in \mathcal{N} \mid \mathcal{M}$, porque $xn \in \mathcal{N}$. Esto demuestra que $\mathcal{N} \mid \mathcal{M}$ es un ideal de $A \mid \mathcal{M}$.

Ahora recordamos que, como vimos en Ejemplos 3.9, 6, como $A \mid \mathcal{M}$ es un cuerpo, no tiene ideales no triviales, por lo tanto, o bien $\mathcal{N} \mid \mathcal{M} = \{\mathbf{0} + \mathcal{M}\} = \{\mathcal{M}\}$ o bien $\mathcal{N} \mid \mathcal{M} = A \mid \mathcal{M}$, o sea, $\mathcal{N} = \mathcal{M}$ o bien $\mathcal{N} = A$, lo que contradice nuestra hipótesis, por lo tanto $\mathcal{M}$ es ideal maximal. □

Ejemplo 3.23. Consideremos el anillo de polinomios $\mathbb{R}[x]$ y el ideal generado por $x^2 + 1$. Como x^2+1 es irreducible, $\langle x^2+1\rangle$ es maximal. Entonces el cuociente $\mathbb{R}[x] \mid \langle x^2+1\rangle$ es un cuerpo, ¿podemos adivinar a qué cuerpo conocido se parece?

Miremos primero el aspecto de los elementos de $\mathbb{R}[x] \mid \langle x^2 + 1\rangle$. Escribiremos $\mathcal{M} = \langle x^2 + 1\rangle$.

Dado cualquier $p(x) \in \mathbb{R}[x]$, por el algoritmo de la división,

$$p(x) = q(x)(x^2 + 1) + (bx + a)$$

luego

$$p(x) + \mathcal{M} = (a + bx) + \mathcal{M}\,.$$

porque $q(x)(x^2 + 1) \in \langle x^2 + 1\rangle$. Veamos las operaciones.

$$(\,(a + bx) + \mathcal{M}) + (\,(c + dx) + \mathcal{M}\,) \;=\; (\,(a + c) + (b + d)x\,) + \mathcal{M}$$

$$\begin{aligned}(\,(a + bx) + \mathcal{M}) \cdot (\,(c + dx) + \mathcal{M}\,) &= (\,(ac) + (ad + cb)x + bdx^2\,) + \mathcal{M}\\ &= (\,(ac - bd) + (ad + cb)x + bd(x^2 + 1)\,) + \mathcal{M}\\ &= (\,(ac - bd) + (ad + cb)x\,) + \mathcal{M}\end{aligned}$$

porque $bd(x^2 + 1) \in \mathcal{M} = \langle x^2 + 1\rangle$.

Observemos además que

$$(x+\mathcal{M})^2 = x^2+\mathcal{M} = -1+(x^2+1)+\mathcal{M} = -1+\mathcal{M},$$

así, si llamamos $\mathbf{i} = x+\mathcal{M}$ tenemos que en $\mathbb{R}[x] \mid \langle x^2+1\rangle$, $\mathbf{i}^2 = -\mathbf{1}$ y que

$$\mathbb{R}[x] \mid \langle x^2+1\rangle = \{a+b\mathbf{i} : a,b \in \mathbb{R}\}.$$

Acabamos de construir un cuerpo que contiene en forma natural a $\mathbb{R}$ (como aquellos elementos de la forma $a+\mathcal{M}$) y que además contiene una raíz del polinomio $f(X) = X^2+\mathbf{1}$, (a saber, $\mathbf{i} = x+\mathcal{M}$). Cualquier parecido con el cuerpo de los números complejos no es una coincidencia.

Esta es una técnica estándar en la teoría de cuerpos. Consiste en tomar un polinomio $p(x)$ irreducible sobre $\mathbb{Q}[x]$ o $\mathbb{R}[x]$, (en realidad se puede hacer con anillos de polinomios más generales). Enseguida se toma el ideal (maximal) generado por ese polinomio y se construye el cuociente. El resultado será un cuerpo que contiene a $\mathbb{Q}$ o a $\mathbb{R}$ y que además contiene una raíz del polinomio $p(x)$.

3.2.5 Ejercicios

1. Diga cuáles de los siguientes conjuntos con las operaciones matriciales habituales son subanillos de $M_2(\mathbb{R})$.

$$a)\quad \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a,b \in \mathbb{Z}\right\}, \qquad b)\quad \left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a,b \in \mathbb{Z}\right\},$$

$$c)\quad \left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a,b \in \mathbb{Z}\right\}, \qquad d)\quad \left\{\begin{pmatrix} a & b \\ c & 0 \end{pmatrix} : a,b,c \in \mathbb{R}\right\},$$

$$e)\quad \left\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a,b \in \mathbb{R}\right\}, \qquad f)\quad \left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a,b \in \mathbb{R}\right\}.$$

2. . Encuentre todos los subanillos de $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_{12}$, $\mathbb{Z}$, ¿cuáles de estos son ideales?
3. Encuentre el menor subanillo de $\mathbb{R}$ que contiene a $\mathbb{Z}$ y al número π.
4. . ¿Es $\mathbb{Z}_3$ un subanillo de $\mathbb{Z}$?, ¿de $\mathbb{Z}_6$?, ¿por qué?
5. Encuentre un anillo de 17 elementos. Encuentre un anillo de 17 elementos que no sea unitario.
6. Suponga que S_1 es subanillo de A_1 y que S_2 es subanillo de A_2. Demuestre que $S_1 \times S_2$ es subanillo de $A_1 \times A_2$, ¿es cualquier subanillo de $A_1 \times A_2$ de esa forma?
7. En $\mathbb{Z}$ demuestre que $\langle m\rangle \cap \langle n\rangle = \langle [n,m]\rangle$, donde $[n,m]$ es el mínimo común múltiplo de n y m.
8. En el anillo $C[0,1]$ de todas las funciones reales continuas sobre $[0,1]$ demuestre que $\mathcal{I} = \{f \in C[0,1] : f(\frac{1}{2}) = 0\}$ es un ideal, ¿es este un ideal maximal?
9. Demuestre que en $M_2(\mathbb{R})$ no hay ideales no triviales.

10. Demuestre que en $\mathbb{Z}[x]$

$$\langle\{2, x\}\rangle = \{2p(x) + xq(x) : p(x), q(x) \in \mathbb{Z}[x]\},$$

como se afirma en el ejemplo 3.15 del texto.
11. Demuestre que el conjunto de los polinomios de $\mathbb{Z}[x]$ tales que todos sus coeficientes son divisibles por 3 es un ideal principal de $\mathbb{Z}[x]$.
12. En el ejemplo anterior construya el anillo cuociente, ¿a qué anillo conocido es isomorfo?
13. Repita los dos ejercicios anteriores con el anillo $\mathbb{Q}[x]$ y el ideal principal generado por el polinomio $x^2 - 2$.
14. Demuestre las afirmaciones que no se demostraron en el teorema 3.21.

3.3 Homomorfismos e Isomorfismos

Definición 3.24. Sean A y B dos anillos. Una función $f : A \longrightarrow B$ es un *homomorfismo* si y sólo si

$$\begin{aligned} f(x+y) &= f(x) + f(y), \\ f(xy) &= f(x)f(y). \end{aligned}$$

Decimos también que B es una *imagen homomorfa de* A.

Es importante notar que las operaciones que aparecen a la izquierda de las ecuaciones anteriores no son las mismas que aparecen en el lado derecho. Las primeras corresponden a las operaciones del anillo A y las segundas a las del anillo B. En rigor, deberíamos usar símbolos distintos, sin embargo, usamos los mismos, ya que, como en general no hay posibilidad de confusión, ésta es la práctica común.

Teorema 3.25. *Si f es un homomorfismo,*

1. $f(\mathbf{0}) = \mathbf{0}$
2. $f(-a) = -f(a)$

Demostración. Para demostrar 1,

$$f(\mathbf{0}) = f(\mathbf{0} + \mathbf{0}) = f(\mathbf{0}) + f(\mathbf{0}).$$

Restando $f(\mathbf{0})$ a cada lado, obtenemos $\mathbf{0} = f(\mathbf{0})$.

Para demostrar 2,

$$f(a) + f(-a) = f(a - a) = f(\mathbf{0}) = \mathbf{0},$$

$$f(-a) + f(a) = f(-a + a) = f(\mathbf{0}) = \mathbf{0},$$

luego por la unicidad del inverso aditivo, $f(-a) = -f(a)$. □

Ejemplos 3.26. Los siguientes son homomorfismos.
1.

$$\begin{array}{rcl} f:\mathbb{Z} & \longrightarrow & \mathbb{Z}_n \\ k & \longmapsto & \overline{k} \end{array}$$

2.

$$\begin{array}{rcl} f:\mathbb{Z} & \longrightarrow & \mathbb{Q}[x] \\ k & \longmapsto & k \end{array}$$

3.

$$\begin{array}{rcl} f:\mathbb{Z} & \longrightarrow & A \\ k & \longmapsto & \mathbf{0}_A, \end{array}$$

donde A es un anillo cualquiera y $\mathbf{0}_A$ es el neutro de A. Este se llama el *homomorfismo trivial*.
4.

$$\begin{array}{rcl} f:\mathbb{C} & \longrightarrow & \mathbb{C} \\ a+bi & \longmapsto & a-bi \end{array}$$

La siguiente definición introduce cierta nomenclatura muy usada.

Definición 3.27. Si $f : A \longrightarrow B$ es un homomorfismo, diremos que f es:

1. *Monomorfismo*, si f es inyectiva.
2. *Epimorfismo*, si f es sobreyectiva.
3. *Isomorfismo*, si f es biyectiva. Decimos en tal caso que los anillos A y B son *isomorfos*.
4. *Automorfismo*, si f es isomorfismo y $A = B$.

Ejemplos 3.28.

1. Consideremos la función

$$\begin{array}{rcl} f:\mathbb{Z} & \longrightarrow & \mathbb{Z}\times\mathbb{Z} \\ n & \longmapsto & (n,n)\,. \end{array}$$

Entonces

$$\begin{array}{rcl} f(n+m) & = & (n+m,n+m) = (n,n)+(m,m) = f(n)+f(m) \\ f(n\,m) & = & (n\,m,n\,m) = (n,n)\,(m,m) = f(n)\,f(m)\,, \end{array}$$

f es un homomorfismo y es inyectivo, o sea, f es un monomorfismo.
2. Consideremos el anillo de matrices

$$A = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \,:\, a,b\in\mathbb{R} \right\}.$$

Entonces A es isomorfo al anillo $\mathbb{C}$ de los números complejos. En efecto, la función

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \longmapsto a + bi$$

es un isomorfismo. Comprobemos que se comporta bien con respecto al producto.

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix}$$

Por lo tanto, la imagen del producto es el número complejo

$$ac - bd + (ad + bc)i\,,$$

que es igual al producto de las imágenes de los factores.

La suma también es respetada y también es claro que la función es una biyección. Ambos se dejan como ejercicio.

Observamos que A y $\mathbb{C}$ al ser isomorfos, son algebraicamente iguales, es decir, son "el mismo" anillo con distinta representación. Por ejemplo, las matrices

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{e} \qquad \mathbf{i} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

se comportan como los complejos 1 e i respectivamente, de forma que

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a\,\mathbf{1} + b\,\mathbf{i}\,,$$

representación en la que queda de manifiesto la correspondencia. □

Definición 3.29. Si $f : A \longrightarrow B$ es un homomorfismo,

1. $ker\ f = \{a \in A : f(a) = \mathbf{0}\}$ es el *núcleo* o *kernel* de f.
2. $Im\ f = \{f(a) \in B : a \in A\}$ es la *imagen* de A por f.

Teorema 3.30. *Si $f : A \longrightarrow B$ es homomorfismo, entonces*

1. *$ker\ f$ es un ideal de A.*
2. *$Im\ f$ es un subanillo de A.*

Demostración.

1. En primer lugar, como $\mathbf{0} \in ker\ f$, éste no es vacío.

Sean a y b dos elementos del kernel de f. Entonces

$$f(a - b) = f(a) - f(b) = \mathbf{0} - \mathbf{0} = \mathbf{0},$$

luego $a - b \in ker\ f$ y éste es cerrado bajo diferencias.

Si $a \in ker\ f$ y $r \in A$, entonces

$$f(ar) = f(a)f(r) = \mathbf{0}f(r) = \mathbf{0},$$

luego $ar \in ker\ f$. Análogamente, $ra \in ker\ f$, es decir $ker\, f$ es absorbente, por lo tanto $ker\ f$ es un ideal de A.

2. Como $f(\mathbf{0}) = \mathbf{0}$, $Im\ f$ no es vacío.

Sean r y s elementos de $Im\ f$. Entonces existen a, $b \in A$ tales que

$$r = f(a) \text{ y } s = f(b).$$

Por lo tanto

$$r - s = f(a) - f(b) = f(a - b) \in Im\ f$$

y

$$rs = f(a)f(b) = f(ab) \in Im\ f,$$

o sea, $Im\ f$ es cerrado bajo diferencias y productos, luego por el Teorema 3.6, $Im\ f \leq B$. □

Luego de demostrar el teorema anterior, resulta natural preguntarse si $Im\ f$ es o no un ideal de B. El siguiente ejemplo responde esta pregunta.

Ejemplo 3.31. Consideremos el homomorfismo

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

del ejercicio anterior. Vemos que $Im\ f$ no es un ideal de B ya que, por ejemplo,

$$(1, 0) \cdot (2, 2) = (2, 0) \notin Im\ f\,,$$

es decir, $Im\ f$ no absorbe y por lo tanto no es ideal.

Teorema 3.32. *Sea $f : A \longrightarrow B$ un homomorfismo, entonces*

$$f \text{ es 1–1 si y sólo si } ker\ f = \{\mathbf{0}\}.$$

Demostración. Supongamos primero que f es 1–1. Entonces, si $a \in ker\ f$, $f(a) = \mathbf{0} = f(\mathbf{0})$, y por lo tanto $a = \mathbf{0}$.

En la otra dirección, supongamos que $ker\ f = \{\mathbf{0}\}$. Entonces, si $f(a) = f(b)$ tenemos $f(a - b) = f(a) - f(b) = \mathbf{0}$, o sea, $a - b \in ker\ f$. Luego por hipótesis $a - b = \mathbf{0}$, o lo que es lo mismo, $a = b$, es decir f es 1–1. □

El siguiente teorema es una suerte de recíproco del Teorema 3.30,1. En él demostramos que todo ideal es el núcleo de algún homomorfismo.

Teorema 3.33. *Sea $\mathcal{I}$ un ideal de A, entonces*

$$\begin{aligned} \pi : A &\longrightarrow A \mid \mathcal{I} \\ a &\longmapsto a + \mathcal{I} \end{aligned}$$

es un homomorfismo. Este se llama el homomorfismo canónico.

Más aún, $ker\ \pi = \mathcal{I}$.

Demostración. Por la forma en que se definieron las operaciones de $A \mid \mathcal{I}$, π es obviamente un homomorfismo.

Para ver que $ker\ \pi = \mathcal{I}$, basta recordar que el neutro de $A \mid \mathcal{I}$ es $\mathcal{I}$, luego

$$\begin{array}{lll} a \in ker\ \pi & \text{si y sólo si} & \pi(a) = \mathcal{I} \\ & \text{si y sólo si} & a + \mathcal{I} = \mathcal{I} \\ & \text{si y sólo si} & a \in \mathcal{I}. \end{array}$$

□

El último teorema de este capítulo es conocido como el Primer Teorema de Isomorfismo porque en las presentaciones habituales de la teoría de anillos siempre se incluyen otros dos teoremas (ver ejercicios). Su mayor utilidad es que permite identificar ciertos anillos cuociente como anillos ya conocidos, y a la inversa, permite observar que dos anillos aparentemente distintos están relacionados de una manera natural, a saber, uno es un cuociente del otro por algún ideal.

Un ejemplo de esta aplicación es el Ejercicio 3.23. En él se toma un anillo y un ideal y se comprueba que ese cuociente es nada menos que el cuerpo (en particular es un anillo) de los números complejos.

Teorema 3.34. Primer Teorema de Isomorfismo.
Sea $f : A \longrightarrow B$ un epimorfismo, entonces

$$\begin{array}{rcl} \varphi : A \mid ker\ f & \longrightarrow & B \\ a + ker\ f & \longmapsto & f(a) \end{array}$$

es un isomorfismo.

Demostración. Debemos demostrar primero que φ es una función bien definida, es decir, no depende del representante de la clase de equivalencia que estemos usando.

Tenemos que

$$\begin{array}{lll} a + ker\ f = b + ker\ f & \text{si y sólo si} & a - b \in ker\ f \\ & \text{si y sólo si} & f(a) - f(b) = f(a - b) = \mathbf{0} \\ & \text{si y sólo si} & f(a) = f(b) \\ & \text{si y sólo si} & \varphi(a + ker\ f) = \varphi(b + ker\ f) \end{array}$$

y esto demuestra no sólo que φ está bien definida ($\Rightarrow$), sino también que es inyectiva ($\Leftarrow$).

Por otra parte,

$$\begin{aligned}\varphi((a+ker\ f)+(b+ker\ f)) &= \varphi((a+b)+ker\ f)\\ &= f(a+b)\\ &= f(a)+f(b)\\ &= \varphi(a+ker\ f)+\varphi(b+ker\ f),\end{aligned}$$

$$\begin{aligned}\varphi((a+ker\ f)\cdot(b+ker\ f)) &= \varphi((ab)+ker\ f)\\ &= f(ab)\\ &= f(a)f(b)\\ &= \varphi(a+ker\ f)\varphi(b+ker\ f),\end{aligned}$$

es decir, φ es un homomorfismo.

Por último, si $b \in B$, como f es sobreyectiva, existe $a \in A$ tal que $b = f(a)$, luego

$$b = \varphi(a + ker\ f).$$

Por lo tanto φ es sobreyectiva. □

Ejemplo 3.35. Sea A el anillo de todas las funciones continuas $f : [0,1] \longrightarrow \mathbb{R}$ con las operaciones definidas como en el ejemplo 3.2,6 y sea

$$\mathcal{I} = \{f \in A : f(\frac{1}{2}) = 0\}.$$

Podemos fácilmente verificar que $\mathcal{I}$ es un ideal de A. Si definimos

$$\begin{aligned}\varphi : A &\longrightarrow \mathbb{R}\\ f &\longmapsto f(\frac{1}{2}),\end{aligned}$$

entonces

$$\varphi(f+g) = (f+g)(\frac{1}{2}) = f(\frac{1}{2}) + g(\frac{1}{2}) = \varphi(f) + \varphi(g)$$

$$\varphi(f\cdot g) = (f\cdot g)(\frac{1}{2}) = f(\frac{1}{2})\ g(\frac{1}{2}) = \varphi(f)\ \varphi(g),$$

es decir, φ es un homomorfismo.

Obviamente φ es sobreyectiva, en efecto, si $r \in \mathbb{R}$ consideramos la función constante $f(x) = r$. Entonces $f \in A$ y $r = \varphi(f)$.

Sea $f \in ker\ \varphi$, entonces $f(\frac{1}{2}) = 0$, y por lo tanto $ker\ \varphi = \mathcal{I}$. Luego, en virtud del teorema anterior, $A \mid \mathcal{I}$ y $\mathbb{R}$ son isomorfos.

Ejemplo 3.36. Otra aplicación del teorema es la identificación de las imágenes homomorfas posibles de un anillo. En efecto, como todas las imágenes homomorfas de un anillo son isomorfas a algún cuociente y, a su vez, estos dependen de los ideales, habrá a lo más tantas imágenes isomorfas como ideales tiene el anillo. Por ejemplo

consideremos el anillo $\mathbb{Z}_{12}$. Los ideales y sus respectivos cuocientes están dados en la siguiente tabla

Ideal	Cuociente	Isomorfo con
$\{0\}$	$\mathbb{Z}_{12} \mid \{0\}$	$\mathbb{Z}_{12}$
$\langle 2\rangle$	$\mathbb{Z}_{12} \mid \langle 2\rangle$	$\mathbb{Z}_2$
$\langle 3\rangle$	$\mathbb{Z}_{12} \mid \langle 3\rangle$	$\mathbb{Z}_3$
$\langle 4\rangle$	$\mathbb{Z}_{12} \mid \langle 4\rangle$	$\mathbb{Z}_4$
$\langle 6\rangle$	$\mathbb{Z}_{12} \mid \langle 6\rangle$	$\mathbb{Z}_6$
$\mathbb{Z}_{12}$	$\mathbb{Z}_{12} \mid \mathbb{Z}_{12}$	$\{0\}$,

por lo tanto sólo los anillos de la última columna (o isomorfos a ellos) pueden ser imágenes homomorfas de $\mathbb{Z}_{12}$. Dejamos como ejercicio la verificación de estos resultados. Para efectuar los cálculos se sugiere escribir las clases y hacer una tabla de las respectivas operaciones. Verificar enseguida que estas corresponden a las operaciones de los anillos indicados.

3.3.1 Ejercicios

1. Para cada uno de los siguientes casos, determine si $\varphi : \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3$ es inyectiva, sobreyectiva, homomorfismo, isomorfismo.
   a) $\varphi(x) = 2x$,
   b) $\varphi(x) = 2 + x$,
   c) $\varphi(x) = -x$,
   d) $\varphi(x) = x^2$,
   e) $\varphi(x) = x^3$.
2. Repita el ejercicio anterior con $\mathbb{Z}_3$ reemplazado por $\mathbb{Z}_5$, $\mathbb{Z}_6$, $\mathbb{Z}_m$.
3. Para cada $r \in \mathbb{R}$ definimos la función $f_r : \mathbb{Q}[x] \longrightarrow \mathbb{R}$ por $f_r(p(x)) = p(r)$. Demuestre que este es un homomorfismo. Este se llama *homomorfismo de evaluación.* Encuentre el kernel de f_r.
4. Verifique que la función
$$\begin{array}{rcl} \varphi : \mathbb{Z}_{18} & \longrightarrow & \mathbb{Z}_6 \\ \overline{a}_{18} & \longmapsto & \overline{a}_6, \end{array}$$
donde $\underline{a}_m$ es la clase de a módulo m, es un homomorfismo, ¿es φ sobreyectiva?, ¿cuál es su kernel?
5. Suponga que $m \mid n$. Generalizamos el problema anterior definiendo
$$\begin{array}{rcl} \varphi : \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_m \\ \overline{a}_n & \longmapsto & \overline{a}_m. \end{array}$$
Demuestre que este es un epimorfismo. Encuentre su kernel, ¿qué sucede si $m \nmid n$?
6. Encuentre todos los homomorfismos de $\mathbb{Z}$ en $\mathbb{Z}$. De $\mathbb{Z}$ en $\mathbb{Z}_6$. De $\mathbb{Z}$ en $\mathbb{Z}_m$. De $\mathbb{Z}_n$ en $\mathbb{Z}_m$.

   Indicación: Demuestre primero que todo homomorfismo φ con dominio $\mathbb{Z}$ o $\mathbb{Z}_n$ está determinado por $\varphi(1)$, ¿es esto cierto si el dominio es otro anillo?

7. Considere los anillos

$$\begin{aligned}\mathbb{Z}[i] &= \{a+bi : a,b \in \mathbb{Z}\},\\ \mathbb{Z}[\sqrt{2}] &= \{a+b\sqrt{2} : a,b \in \mathbb{Z}\},\\ \mathbb{Z}[\sqrt{3}] &= \{a+b\sqrt{3} : a,b \in \mathbb{Z}\}.\end{aligned}$$

   ¿Son algunos de estos isomorfos?

8. **El segundo teorema de isomorfismo.** Sean I y J ideales del anillo A y sea $I+J$ el ideal generado por $I \cup J$. Demuestre que
   a) $I \cap J$ es ideal de I,
   b) J es ideal de $I+J$,
   c) $\varphi : I \longrightarrow I+J \mid J$
      $a \longmapsto a+J$
      es un epimorfismo,
   d) $ker\ \varphi = I \cap J$,
   e) Concluya que $I \mid I \cap J \cong I+J \mid J$.

Capítulo 4: Permutaciones, Isometrías, Simetrías

En este capítulo estudiaremos ciertos conjuntos de biyecciones de un conjunto A en sí mismo, dotados de la operación natural, la composición de funciones. Como sabemos, sin importar cuál es el conjunto A, la composición de dos biyecciones es también una biyección. Habitualmente nos referiremos a la composición de dos biyecciones σ y τ como el *producto* de σ y τ.

Como veremos, estos conjuntos de funciones dotados de esta operación tienen una serie de propiedades que pueden ser analizadas desde el punto de vista algebraico. El propósito de este capítulo es estudiar en forma intuitiva algunos de estos ejemplos, que suponemos más o menos conocidos por el lector y hacer notar algunas propiedades comunes a todos ellos. En el próximo capítulo se desarrollará una teoría general, la *teoría de grupos* que los abarca a todos. De hecho, los trabajos de Lagrange, Abel y Galois a fines del siglo XVIII y comienzos del XIX sobre grupos de permutaciones, son el origen de toda la teoría abstracta de grupos desarrollada más tarde por Cauchy y Cayley.

Nos referiremos en primer lugar a algunas propiedades de todos estos ejemplos. En primer lugar, si f, g y h son funciones de un conjunto cualquiera en sí mismo, entonces

$$f \circ (g \circ h) = (f \circ g) \circ h,$$

es decir, la composición de funciones es asociativa, sin embargo, en general

$$f \circ g \neq g \circ f,$$

es decir, la composición de funciones no es conmutativa.

También sabemos que existe una biyección, la función identidad Id, que no produce ningún efecto en el conjunto A y que, por lo tanto, al componerla con cualquier otra biyección σ, el resultado sobre A es el mismo que si hiciéramos actuar sólo a σ, esto es,

$$\sigma \circ Id = Id \circ \sigma = \sigma.$$

Nos referiremos a ella como la *identidad* o la biyección *trivial*.

Por último, toda biyección tiene una inversa, es decir, dada una biyección σ, existe otra, habitualmente denotada σ^{-1}, que invierte la acción de σ sobre A, es decir, si $\sigma(a) = b$, entonces $\sigma^{-1}(b) = a$, esto se resume en las siguientes ecuaciones

$$\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = Id.$$

Estas tres propiedades, asociatividad de la composición, existencia de un elemento que no altera el resultado al ser operado con cualquier otro, (similar al 0 en la suma de

los números enteros), y la existencia para cada elemento de otro que, por así decirlo, actúa al revés, son las propiedades que nos interesarán en el próximo capítulo. Por el momento sólo tendremos presente estos hechos ya conocidos y los usaremos sin mencionarlos.

4.1 Permutaciones

En esta sección estudiaremos el conjunto de todas las biyecciones de un conjunto en sí mismo. Nos limitaremos aquí al caso de un conjunto finito $A = \{a_1, a_2, \ldots, a_n\}$, de hecho, sin pérdida de generalidad, nos basta con considerar las permutaciones de los índices de los elementos del conjunto A, es decir, estudiar todas las permutaciones del conjunto

$$\{1, 2, \ldots, n\},$$

es decir,

$$S_n = \{f : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\} : f \text{ es biyectiva}\}.$$

Como vimos en la introducción, la composición de dos permutaciones es también una permutación, es decir, S_n es cerrado bajo composición de funciones. Más aún, S_n es también cerrado bajo inversas. Además existe un elemento distinguido de S_n, la identidad. Estudiaremos ahora algunas propiedades de S_n dotado de esta operación, para ello desarrollaremos algunas herramientas que facilitarán la exposición..

Existe una notación muy práctica para representar un elemento σ de S_n. Simplemente escribimos dos renglones con los números $\{1, 2, \ldots, n\}$, de tal manera que debajo de k aparece la imagen $\sigma(k)$ de k:

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

Así, por ejemplo, la permutación

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

corresponde a la función

$$\begin{aligned} \tau(1) &= 2 \\ \tau(2) &= 4 \\ \tau(3) &= 3 \\ \tau(4) &= 1. \end{aligned}$$

Es claro también que el orden en que se escriban los elementos de la permutación no es importante mientras la imagen de cada número aparezca debajo del mismo, así,

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

Usando esta notación, la función identidad es:

$$Id = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix},$$

mientras que la inversa de

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

es

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

El lector probablemente ha visto el siguiente resultado en algún curso de álgebra elemental.

Teorema 4.1. *S_n tiene $n!$ elementos.*

4.1.1 Ciclos y Transposiciones

Entre las permutaciones hay algunas que merecen un estudio especial, se trata de los ciclos y el caso particular de éstos, las transposiciones.

Si σ una permutación de S_n diremos que σ *mueve* a x si $\sigma(x) \neq x$. Por ejemplo, la identidad no mueve ningún elemento, en cambio la permutación

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 3 & 1 & 4 & 6 \end{pmatrix}$$

mueve a los números 1,2,4 y 5, pero no mueve a 3 ni a 6. Esto puede ser resumido en el diagrama

$$1 \overset{\sigma}{\longmapsto} 2 \overset{\sigma}{\longmapsto} 5 \overset{\sigma}{\longmapsto} 4 \overset{\sigma}{\longmapsto} 1$$

Toda la información relevante acerca de la permutación está codificada en ese diagrama. Este ejemplo da origen a una definición y una notación importantes.

Definición 4.2. Una permutación σ de S_n cuyos valores sobre $\{a_1, a_2, \ldots, a_k\} \subseteq \{1, 2, \ldots, n\}$ están dados por

$$a_1 \overset{\sigma}{\longmapsto} a_2 \overset{\sigma}{\longmapsto} a_3 \overset{\sigma}{\longmapsto} \cdots \overset{\sigma}{\longmapsto} a_k \overset{\sigma}{\longmapsto} a_1$$

y tal que para todo otro $x \in \{1, 2, \ldots, n\}$, $\sigma(x) = x$, se denomina *ciclo de largo k*. Un ciclo de largo dos es una *transposición*. Intuitivamente, el largo de un ciclo es el número de elementos que son movidos.

El ciclo anterior lo denotaremos

$$(a_1\, a_2\, \cdots\, a_k).$$

Por ejemplo, la permutación τ de S_4 que escribimos antes, es un ciclo de largo tres ya que

$$1 \overset{\tau}{\longmapsto} 2 \overset{\tau}{\longmapsto} 4 \overset{\tau}{\longmapsto} 1$$

y $\tau(3) = 3$. De acuerdo con esta nueva notación,

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (1\,2\,4).$$

Debemos observar que esta notación simplificada para un ciclo es ambigua. En efecto, el ciclo $(1, 2, 4)$ representa también a la permutación

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

de S_5 y también a una de S_6 o a una permutación de cualquier número de elementos mayor o igual que 5. Sólo sabiendo de antemano el contexto en el que se está trabajando se podrá determinar si el ciclo anterior representa a una permutación de S_4 o de S_5 o de S_n, para algún n.

Al igual que en la notación anterior, más completa, no nos interesa cuál es el primer elemento del ciclo sino sólo el orden en que aparecen,

$$(1\,2\,4) = (2\,4\,1) = (4\,1\,2).$$

Resulta claro que no toda permutación es un ciclo, por ejemplo

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

no es un ciclo.

Definición 4.3. Dos ciclos se dicen *disjuntos*, si no comparten ningún elemento.

Por ejemplo

$$(1\,3\,4\,6) \text{ y } (2\,7\,8),$$

son ciclos disjuntos.

El próximo teorema es más o menos obvio.

Teorema 4.4. *La composición de ciclos disjuntos es conmutativa.*

Demostración. Sean $(a_1\,a_2\,\cdots\,a_r)$ y $(b_1\,b_2\,\cdots\,b_s)$ dos ciclos disjuntos de S_n. Para verificar que conmutan, basta ver cuál es la acción sobre $1, 2, \ldots, n$ de las permutaciones $(a_1\,a_2\,\cdots\,a_r)(b_1\,b_2\,\cdots\,b_s)$ y $(b_1\,b_2\,\cdots\,b_s)(a_1\,b_2\,\cdots\,a_r)$ es fácil ver que

$$(a_1\,a_2\,\cdots\,a_r)(b_1\,b_2\,\cdots\,b_s)(k) = \begin{cases} b_{i+1}, & \text{si } k = b_i \text{ con } 1 \leq i < s \\ b_1, & \text{si } k = b_s \\ a_{i+1}, & \text{si } k = a_i \text{ con } 1 \leq i < r \\ a_1, & \text{si } k = a_r \\ k, & \text{en cualquier otro caso,} \end{cases}$$

y que $(b_1\, b_2\, \cdots\, b_s)(a_1\, a_2\, \cdots\, a_r)$ toma los mismos valores, luego ambas permutaciones son iguales. □

Los ciclos juegan dentro de la teoría de permutaciones un papel similar al de los números primos en la teoría de números, son los ladrillos con los que se construyen todas las permutaciones. Esto lo precisaremos en el próximo teorema.

Teorema 4.5. *Toda permutación no trivial es un ciclo o se puede descomponer como producto de ciclos disjuntos. Tal descomposición es única salvo por el orden de los ciclos.*

Demostración. Sea σ una permutación no trivial de S_n. Procederemos por inducción sobre el número de elementos de $\{1, 2, \ldots, n\}$ que son movidos por σ. Sean $\{a_1, a_2, \ldots, a_k\}$ los elementos movidos por σ.

Observemos que por tratarse de una biyección, el número mínimo de elementos que una permutación no trivial mueve es dos y esto ocurre cuando se trata de una transposición. Nuestra inducción comienza entonces en $k = 2$, o sea, σ mueve sólo dos elementos, es una transposición y por lo tanto es un ciclo. Esto da cuenta del primer paso de la inducción.

Supongamos ahora nuestra hipótesis de inducción, a saber, toda permutación que mueve menos de k elementos, $k \geq 2$, se descompone como producto de ciclos disjuntos.

Sea a_1 uno cualquiera de los elementos movidos por σ. Si observamos la siguiente sucesión

$$a_1 \longmapsto \sigma(a_1) = a_2 \longmapsto \sigma(\sigma(a_1)) = a_3 \longmapsto \cdots \longmapsto \sigma^m(a_1) = a_m \longmapsto \cdots$$

entonces, como el conjunto es finito y σ es una biyección, para algún $m \leq k$, $\sigma^m(a_1) = a_1$. Notemos que $m \geq 2$.

Tenemos entonces dos posibilidades, si $m = k$, entonces σ es un ciclo y el teorema se verifica. Si $m < k$ entonces consideramos la permutación definida por

$$\hat{\sigma} = \begin{cases} x, & \text{si } x \in \{a_1, a_2, \ldots, a_m\}, \\ \sigma(x) & \text{en otro caso.} \end{cases}$$

Como vemos, $\hat{\sigma}$ es una permutación de S_n que difiere de σ sólo en los valores que toma sobre $\{a_1, a_2, \ldots, a_m\}$. También es fácil comprobar que

$$\sigma = (a_1\, a_2\, \ldots\, a_m)\, \hat{\sigma}.$$

Pero ahora podemos aplicar nuestra hipótesis de inducción ya que $\hat{\sigma}$ obviamente mueve menos de k elementos, luego es el producto de ciclos disjuntos. Como estos necesariamente son disjuntos de $(a_1, a_2, \ldots, a_m)$, el teorema queda demostrado.

Para probar la unicidad de la descomposición supongamos que hay alguna permutación σ que tiene dos representaciones como producto de ciclos, podemos tomar una que mueve el menor número de puntos posible. Entonces

$$\sigma = \sigma_1\, \sigma_2 \cdots \sigma_r = \tau_1\, \tau_2 \cdots \tau_s\,.$$

Tomamos a_1 el primer número que es movido por σ. Por el Teorema 4.4, podemos suponer que a_1 es movido por σ_1 y por τ_1 y sólo por ellos. Pero como σ es una biyección, debe suceder que $\sigma_1(a_1) = \tau_1(a_1) = \sigma(a_1) = a_2$ y $\sigma_1(a_2) = \tau_1(a_2) = \sigma(a_2) = a_3$, etc., de modo que $\sigma_1 = \tau_1$. Esto implica que

$$\sigma_1{}^{-1}\,\sigma = \sigma_2 \cdots \sigma_r = \tau_2 \cdots \tau_s\,,$$

pero $\sigma_1{}^{-1}\,\sigma$ es una permutación que mueve menos puntos que σ por lo tanto no tiene dos descomposiciones como producto de ciclos. Esto completa la demostración. □

La demostración del teorema anterior nos da una suerte de algoritmo para calcular la descomposición en ciclos de una permutación σ. Tomamos un elemento a cualquiera. Si $\sigma(a) = a$, no nos interesa y tomamos otro. Si $\sigma(a) \neq a$, procedemos con el teorema definiendo el ciclo

$$(a\,\sigma(a) \cdots \sigma^{m-1}(a)).$$

De los elementos que aún no han sido considerados, escogemos otro y procedemos como con a. Eventualmente ya no quedarán elementos por considerar, ya sea porque ya aparecieron en un ciclo o porque no son movidos por σ.

Ejemplo 4.6.

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

Existe otro interesante teorema de descomposición de permutaciones como producto de transposiciones. Intuitivamente, esto significa que podemos ordenar un conjunto finito de cualquier manera intercambiando sucesivamente sólo dos de ellos cada vez. En este caso no se tiene unicidad ya que si multiplicamos cualquier permutación por

$$(1\,2)(1\,2) = Id,$$

tendremos una descomposición distinta.

Tampoco esta descomposición es independiente del orden en que aparecen las transposiciones ya que, en general, éstas no son disjuntas.

Teorema 4.7. *Toda permutación se puede descomponer como producto de transposiciones.*

Demostración. En virtud del teorema anterior basta demostrar que todo ciclo se puede descomponer como producto de transposiciones. Es fácil comprobar que la siguiente descomposición sirve para nuestro propósito.

$$(a_1\,a_2 \cdots, a_k) = (a_1\,a_k) \cdots (a_1\,a_3)(a_1\,a_2).$$

□

Así por ejemplo, $(2\,5\,6\,8) = (2\,8)(2\,6)(2\,5)$.

Usando la descomposición como producto de transposiciones es muy sencillo encontrar la permutación inversa. Baste observar que la inversa de una transposición es ella misma, en efecto, calcule el producto de $(k\,l)$ por sí misma y se obtendrá la identidad. Ahora bien, si

$$\sigma = (a_1\,b_1)(a_2\,b_2)\cdots(a_k\,b_k),$$

entonces

$$\sigma^{-1} = (a_k\,b_k)(a_{k-1}\,b_{k-1})\cdots(a_1\,b_1),$$

como se puede verificar fácilmente al calcular el producto de ambas permutaciones.

La descomposición de una permutación como producto de transposiciones, si bien no es única, tiene una interesante propiedad, que no es en absoluto fácil de detectar (¡ni de demostrar!), el número de transposiciones de una descomposición de una permutación es siempre par o siempre impar, dicho de otra manera, ninguna permutación se descompone como producto de, por ejemplo, tres transposiciones y también como producto de ocho transposiciones, pero sí podría tenerse una descomposición de nueve y otra de treinta y siete transposiciones. Para demostrar este hecho necesitamos una serie de pequeños trucos técnicos. En el próximo capítulo, una vez que hayamos desarrollado la teoría general que incluya a todos los ejemplos de este capítulo, daremos una demostración mucho más intuitiva y elegante.

Dada una permutación $\sigma \in S_n$ y números $k_1, \ldots, k_n \in \{1, 2, \ldots, n\}$, definimos

$$\sigma^* \prod_{1\le i<j\le n}(k_j - k_i) = \prod_{1\le i<j\le n}(\sigma(k_j) - \sigma(k_i)) =$$
$$= (\sigma(k_2) - \sigma(k_1))(\sigma(k_3) - \sigma(k_1))(\sigma(k_3) - \sigma(k_2))\cdots(\sigma(k_n) - \sigma(k_{n-1})).$$

Entonces si

$$\Delta = \prod_{1\le i<j\le n}(j - i) = (2-1)(3-1)(3-2)\cdots(n-(n-1)),$$

$$\sigma^*\Delta = \prod_{1\le i<j\le n}(\sigma(j)-\sigma(i)) = (\sigma(2)-\sigma(1))(\sigma(3)-\sigma(1))(\sigma(3)-\sigma(2))\cdots(\sigma(n)-\sigma(n-1)).$$

Es fácil ver que si σ, $\tau \in S_n$, entonces

$$\sigma^*\tau^*\Delta = (\sigma\tau)^*\Delta,$$

es decir, aplicar una permutación compuesta a Δ es lo mismo que aplicar sucesivamente las permutaciones correspondientes. Luego si σ es el producto de ciertas transposiciones, $\sigma^*\Delta$ se calcula aplicando una a una esas transposiciones en el orden adecuado.

De lo anterior se desprende que para saber como actúa una permutación sobre Δ, nos basta saber como actúan las transposiciones sobre Δ.

Lema 4.8. *Si $\tau \in S_n$ es una transposición, entonces $\tau^*\Delta = -\Delta$.*

Demostración. Sea $\tau = (k, l)$, sin pérdida de generalidad supongamos que $k < l$. Tenemos que calcular $\tau(j) - \tau(i)$ para $1 \leq i < j \leq n$. Hay varios casos. Observemos primero que si i,$j \notin \{k, l\}$, entonces

$$\tau(j) - \tau(i) = j - i,$$

por lo tanto el producto no se altera.

Si $j \notin \{k, l\}$, tenemos tres casos.

1. Si $j < k < l$, entonces $k - j$ y $l - j$ aparecerán en Δ, pero en este caso

$$\tau(k) - \tau(j) = l - j \quad \text{y} \quad \tau(l) - \tau(j) = k - j,$$

por lo que Δ no se ve alterado, τ sólo intercambia dos factores.

2. Algo análogo ocurre si $k < l < j$, ya que, en este caso, $j - k$ y $j - l$ aparecerán en Δ, sin embargo τ sólo los intercambia sin alterar el producto.

3. El último caso es $k < j < l$. Ahora son $j - k$ y $l - j$ los factores que aparecerán en Δ. Aquí vemos que

$$\tau(j) - \tau(k) = j - l = -(l - j) \quad \text{y} \quad \tau(l) - \tau(j) = k - j = -(j - k),$$

por lo tanto, el producto no se altera ya que hay dos cambios de signo.

Nos queda un sólo factor por analizar, a saber $l - k$. Como

$$\tau(l) - \tau(k) = k - l = -(l - k),$$

vemos que en cualquier caso, el resultado de hacer actuar τ sobre Δ sólo produce un cambio de signo. □

Corolario 4.9. *Toda permutación se descompone o bien como producto de un número par de transposiciones, o bien como producto de un número impar de transposiciones.*

Demostración. Como vimos en el lema anterior, al aplicar sucesivamente transposiciones a Δ, sólo cambio el signo, luego si

$$\sigma = \tau_1 \tau_2 \cdots \tau_m,$$

donde las τ_i son transposiciones, por los comentarios previos al lema,

$$\sigma^*\Delta = (-1)^m \Delta.$$

Si σ tuviera una descomposición como producto de un número par de transposiciones y otra como producto de un número impar de transposiciones llegaríamos a una contradicción. □

Definición 4.10. Diremos que una permutación es *par* si se puede descomponer como producto de un número par de transposiciones. En caso contrario diremos que la permutación es impar.

El conjunto de las permutaciones pares de S_n se denotará A_n.

El conjunto A_n tiene características que lo hacen interesante y lo estudiaremos con detención. Un resultado que no debe sorprender demasiado es que la mitad de las permutaciones son pares y la mitad son impares.

Teorema 4.11. *Si $n > 1$, la cardinalidad de A_n es $\frac{n!}{2}$.*

Demostración. Sea B el conjunto de las permutaciones impares y consideremos la siguiente función:

$$\begin{array}{ccc} f : A_n & \longrightarrow & B \\ \sigma & \longmapsto & \sigma\,(1,2) \end{array}$$

La función está bien definida ya que si σ es par, el producto de σ por una transposición es impar.

La función es inyectiva, ya que si

$$\begin{aligned} \sigma(1,2) &= \tau(1,2), \\ \sigma(1,2)(1,2) &= \tau(1,2)(1,2), \\ \sigma Id &= \tau Id, \\ \sigma &= \tau. \end{aligned}$$

La función es sobreyectiva, puesto que si τ es una permutación impar, $\tau(1,2)$ es par, luego

$$f(\tau(1,2)) = \tau(1,2)(1,2) = \tau.$$

Esta función demuestra que hay tantas permutaciones pares como impares, y como toda permutación es par o impar, hay la mitad de cada una. □

Resulta interesante notar también que el producto de dos permutaciones pares es también par, decimos que el conjunto A_n es *cerrado* bajo productos. Es decir, si operamos dos elementos de A_n, el resultado también pertenece a A_n. Lo mismo puede decirse de las permutaciones inversas. La inversa de una permutación par también es par, ya que como vimos más arriba, la inversa de un producto de transposiciones es el producto de las mismas transposiciones pero en el orden inverso, luego su número no varía.

Por otra parte, el producto de permutaciones impares es par, es decir, el conjunto de las permutaciones impares no es cerrado bajo productos.

4.1.2 Ejercicios

1. Considere la permutación $\tau = (1\,2\,3\,4\,5)$, ¿cuántas permutaciones distintas hay en el conjunto $\ldots\tau^{-2}, \tau^{-1}, \tau^0, \tau, \tau^2 \ldots$? Repita el ejercicio con $\tau = (1\,2\,3)\,(4\,5)$. Haga lo mismo con otras permutaciones elegidas por usted. ¿Qué puede conjeturar?
2. Escriba una permutación en S_{10}. Descompóngala como producto de ciclos disjuntos. Descompóngala como producto de transposiciones. Hágalo de dos maneras distintas. Haga variaciones de este ejercicio hasta que sienta que lo domina.

3. Definimos el orden de una permutación τ como el menor entero positivo n tal que $\tau^n = Id$.
   a) Demuestre que el orden de un ciclo es igual a su largo.
   b) Encuentre el orden de $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$.
   c) Encuentre el orden de $(1\,3)(2\,5)$, de $(1\,3)(3\,5)$ y de $(1\,3)(4\,5\,6\,2)$.
   d) ¿Cuál es el orden de un producto de ciclos? Haga varios ejemplos y conjeture un teorema. Demuéstrelo.
   e) ¿Cuáles son los órdenes posibles para una permutación en S_6?, ¿en S_7?
4. a) Escriba la permutación $(a\,b\,c)^2$ como un ciclo de largo tres.
   b) Encuentre un ciclo τ de largo tres tal que $\tau^2 = (a\,b)$.
   c) Escriba la permutación $(a\,b\,c\,d\,e)^2$ como un ciclo de largo cinco.
   d) Encuentre un ciclo τ de largo cinco tal que $\tau^2 = (a\,b\,c\,d\,e)$.
5. Sean σ una permutación y $(a_1\,a_2\cdots a_k)$ un ciclo. Demuestre que

$$\sigma(a_1\,a_2\cdots a_k)\sigma^{-1} = (\sigma(a_1)\,\sigma(a_2)\cdots(a_k)\,).$$

6. Demuestre que no existe una permutación σ tal que $\sigma\,(1\,3\,5) = (1\,2\,3\,4)\sigma$.

4.2 Isometrías

En esta sección estudiaremos otro conjunto de biyecciones, esta vez se trata de aplicaciones del plano euclidiano en sí mismo que preservan distancias. Tales funciones se llaman *isometrías*. Este es un interesante ejemplo de cómo el álgebra aparece también dentro de la geometría.

Definición 4.12. Una *isometría* del plano $\mathbb{R}^2$ en sí mismo es una función

$$\sigma : \mathbb{R}^2 \longrightarrow \mathbb{R}^2,$$

tal que para todo par de puntos P y Q del plano,

$$d(\sigma(P), \sigma(Q)) = d(P, Q),$$

donde $d(P, Q)$ es la distancia euclidiana habitual, vale decir, si

$$P = P(x_1, y_1) \ \text{ y } \ Q = Q(x_2, y_2),$$

$$d(P, Q) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}.$$

Debemos observar que la función identidad es obviamente una isometría. Además si σ y τ son isometrías, entonces

$$d(\sigma\tau(P), \sigma\tau(Q)) = d(\sigma(\tau(P)), \sigma(\tau(Q))) = d(\tau(P), \tau(Q)) = d(P, Q),$$

luego $\sigma\,\tau$ es también una isometría, en otras palabras, el conjunto de todas las isometrías del plano es cerrado bajo productos. Así mismo, es cerrado bajo inversos, ya que como para cualquier $P \in \mathbb{R}^2$

$$\sigma\sigma^{-1}(P) = P\,,$$

si σ es una isometría,

$$d(\sigma^{-1}(P), \sigma^{-1}(Q)) = d(\sigma\sigma^{-1}(P), \sigma\sigma^{-1}(Q)) = d(P, Q).$$

Ejemplos 4.13.
1. **Traslaciones.** Una traslación es una función que mueve todos los puntos del plano una cierta distancia en una dirección dada. Analíticamente,

$$(x, y) \longmapsto (x + a, y + b)\,,$$

donde el vector (a, b) fija la dirección y distancia de la traslación.
2. **Rotaciones.** Consiste en rotar el plano en un ángulo dado θ en torno a un punto fijo O. Analíticamente, si fijamos el origen de nuestro sistema de coordenadas en el punto O,

$$(x, y) \longmapsto (x\cos\theta - y\text{sen}\theta, x\text{sen}\theta + y\cos\theta).$$

Un poco de trigonometría elemental nos ayudará a demostrar que toda rotación es una isometría.
3. **Reflexiones.** Consiste en reflejar los puntos del plano con respecto a una recta arbitraria. Es decir, el punto P es enviado en el punto P' que se encuentra sobre la perpendicular por P a la recta y a la misma distancia de ella que P, del otro lado de la recta.

Como veremos un poco más adelante, esencialmente, estas son las únicas isometrías del plano. En efecto, toda isometría es el producto de una traslación, una rotación y una reflexión.

No es del todo obvio que una isometría es, como hemos insinuado, una biyección en $\mathbb{R}^2$. Para demostrarlo, empezaremos con un lema que se desprende directamente de la definición de isometría.

Lema 4.14. *La imagen del triángulo ABC por una isometría es un triángulo congruente con ABC.*

De hecho, se puede demostrar que la imagen de cualquier figura plana es congruente con la figura original.

Teorema 4.15. *Toda isometría del plano es una biyección que queda determinada por la imagen de tres puntos no colineales.*

Demostración. Sea s una isometría. Si $s(P) = s(Q)$, entonces

$$d(P, Q) = d(s(P), s(Q)) = 0,$$

luego $P = Q$, ya que están a distancia cero. Por lo tanto, s es inyectiva.

Para ver que s es sobreyectiva, sea P un punto cualquiera del plano. Sean A y B dos puntos arbitrarios distintos. Si $P \neq s(A)$ y $P \neq s(B)$, sean $d_1 = d(P, s(A))$ y $d_2 = d(P, s(B))$. Observemos que P está en la intersección del círculo de centro en $s(A)$ y radio d_1 con el círculo de centro en $s(B)$ y radio d_2.

Ahora miramos las preimágenes. Como s es una isometría, la intersección del círculo de centro en A y radio d_1 con el círculo de centro en B y radio d_2 es no

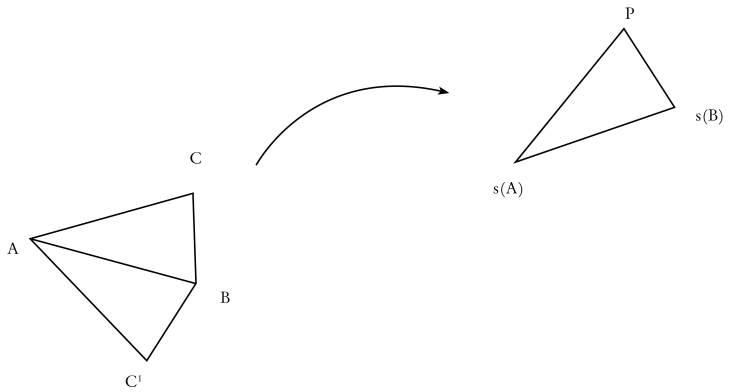


FIGURA 4.1. Demostración Teorema 4.15

vacía y consta de un punto C, si P está en la recta $\overline{s(A)s(B)}$, o de dos puntos C y C'.

En cualquier caso, o bien $P = s(C)$ o bien $P = s(C')$, luego la función es sobreyectiva.

Para demostrar que s queda determinada por la imagen de tres puntos no colineales, sean A, B y C estos tres puntos del plano. Por el lema 4.14 los triángulos ABC y $s(A)s(B)s(C)$ son congruentes. Sea P un punto cualquiera del plano distinto de A, B y C. Consideremos

$$\begin{aligned} d_1 &= d(P,A)\,, \\ d_2 &= d(P,B)\,, \\ d_3 &= d(P,C)\,. \end{aligned}$$

Los círculos de centro A y radio d_1, de centro B y radio d_2 y de centro C y radio d_3 se intersectan en P y solamente en P, ya que si se intersectaran en dos puntos, sus centros A, B y C serían colineales.

La imagen de P por s es entonces el único punto que está en la intersección de los círculos de centro $s(A)$ y radio d_1, de centro $s(B)$ y radio d_2 y de centro $s(C)$ y radio d_3. Esto concluye nuestra demostración. □

Teorema 4.16. *Toda isometría es el producto de una traslación, una rotación y una reflexión.*

Demostración. Como hemos visto, una isometría σ queda determinada por su acción sobre tres puntos no colineales.

Sean A, B, y C tres puntos no colineales cualquiera del plano, y sea $\sigma(A)\sigma(B)\sigma(C)$ el triángulo congruente correspondiente.

Sea τ_A la traslación que lleva el punto A en el punto $\sigma(A)$. Tenemos entonces que

$$\tau_A(A) = \sigma(A),$$

y que por lo tanto los triángulos (¡congruentes!) $\sigma(A)\sigma(B)\sigma(C)$ y $\tau_A(A)\tau_A(B)\tau_A(C)$ comparten un vértice.

Sea ρ_θ la rotación de centro en $\sigma(A)$ y que lleva el lado $\overline{\tau_A(A)\tau_A(B)}$ sobre el lado $\overline{\sigma(A)\sigma(B)}$.

Ahora tenemos que

$$\rho_\theta(\tau_A(A)) = \sigma(A),$$

y

$$\rho_\theta(\tau_A(B)) = \sigma(B),$$

es decir, los triángulos $\sigma(A)\sigma(B)\sigma(C)$ y $\rho_\theta(\tau_A(A))\rho_\theta(\tau_A(B))\rho_\theta(\tau_A(C))$ comparten dos vértices y como son congruentes, o bien

$$\rho_\theta(\tau_A(C)) = \sigma(C),$$

o bien $\rho_\theta(\tau_A(B))$ es simétrico de $\sigma(C)$ con respecto a la recta por $\sigma(A)$ y $\sigma(B)$. En el primer caso,

$$\sigma = \rho_\theta\tau_A$$

En el segundo,

$$\sigma = \mu_{\sigma(A)\sigma(B)}\rho_\theta\tau_A,$$

donde $\mu_{\sigma(A)\sigma(B)}$ es la reflexión con respecto al eje $\overline{\sigma(A)\sigma(B)}$. □

4.2.1 Ejercicios

1. Diga cuál es el resultado de componer:
   a) Dos traslaciones.
   b) Dos reflexiones.
   c) Dos rotaciones con el mismo centro. Con distinto centro.
2. Demuestre analíticamente los detalles de las afirmaciones hechas en los ejemplos.
3. Demuestre que las rotaciones dejan un único punto fijo, las reflexiones dejan todos los puntos de una recta fijos y las traslaciones no dejan puntos fijos, ¿puede usarse esto como método para clasificar las isometrías? Piense en isometrías más complejas que las tres básicas.
4. Hemos visto que si conocemos la imagen de tres puntos no colineales de una isometría ésta queda determinada. Si conocemos la imagen de dos puntos, ¿qué podemos decir? Analice distintas posibilidades.
5. Generalice el concepto de isometría del plano a isometría del espacio.

4.3 Simetrías

En esta sección estudiaremos conjuntos de funciones del plano en sí mismo que preservan una cierta figura, por ejemplo, un triángulo, es decir, conjuntos de biyecciones del plano tales que la imagen de la figura dada coincida con ésta. Estas funciones se denominan *simetrías* de la figura; también se las conoce como *movimientos rígidos* ya que envían la figura sobre ella misma sin deformarla ni romperla.

Es claro que toda simetría es una isometría y que ninguna traslación es una simetría. Por lo tanto, las simetrías de una figura están constituidas por rotaciones, reflexiones y sus compuestas.

Se puede estudiar las simetrías de cualquier figura, sin embargo, mientras más regular sea ésta, más simetrías tendrá. De hecho, los ejemplos más interesantes son los polígonos regulares.

4.3.1 Simetrías de un Triángulo Equilátero

Existen tres rotaciones, en 0°, 120° y 240°. La primera no es sino la identidad Id, la segunda la denotamos ρ y, como una rotación en 240° corresponde a efectuar dos veces la rotación en 120°, denotaremos ρ^2 a la tercera rotación. Observemos que

$$\rho\ \rho^2 = \rho^2\ \rho = Id,$$

ya que una rotación en 360° corresponde a una rotación en 0°.

Tenemos también tres reflexiones con respecto a las transversales de cada lado. En el cuadro siguiente se ilustran las seis simetrías del triángulo equilátero. Es bastante obvio que éstas son las únicas simetrías.

Si componemos, por ejemplo ρ con σ_1 obtendremos

$$\rho\ \sigma_1 = \sigma_0 \quad \text{y} \quad \sigma_1\ \rho = \sigma_2.$$

Podemos hacer una tabla en la que se resumen todas las posibles composiciones de las simetrías anteriores. Debe observarse que para obtener $\sigma\ \tau$ aplicamos primero τ y luego σ

$*$	Id	ρ	ρ^2	σ_0	σ_1	σ_2
Id	Id	ρ	ρ^2	σ_0	σ_1	σ_2
ρ	ρ	ρ^2	Id	σ_2	σ_0	σ_1
ρ^2	ρ^2	Id	ρ	σ_1	σ_2	σ_0
σ_0	σ_0	σ_1	σ_2	Id	ρ	ρ^2
σ_1	σ_1	σ_2	σ_0	ρ^2	Id	ρ
σ_2	σ_2	σ_0	σ_1	ρ	ρ^2	Id

4.3.2 Simetrías de un Cuadrado

Como se ilustra en la figura, en este caso tenemos cuatro rotaciones, en 0°, 90°, 180° y 270° las que, en forma análoga al caso del triángulo, denotaremos Id, ρ, ρ^2 y ρ^3, respectivamente. Es claro que no hay otras rotaciones.

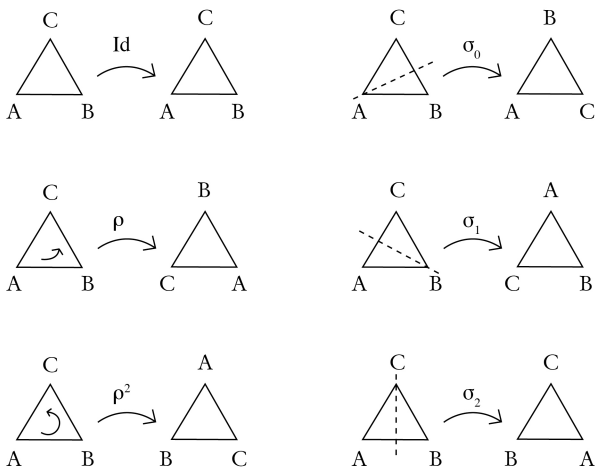


FIGURA 4.2. Simetrías del triángulo equilátero

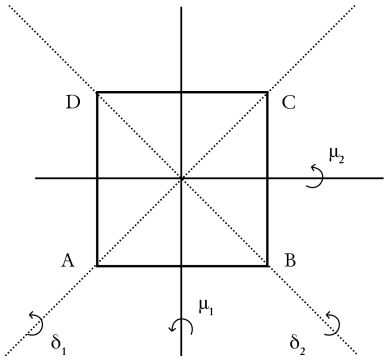


FIGURA 4.3. Simetrías de un cuadrado

También hay cuatro reflexiones, dos en torno a las diagonales, denotadas δ_1 y δ_2, y dos en torno a las simetrales de los lados opuestos, denotadas σ_1 y σ_2.

El siguiente cuadro ilustra todas las simetrías del cuadrado.

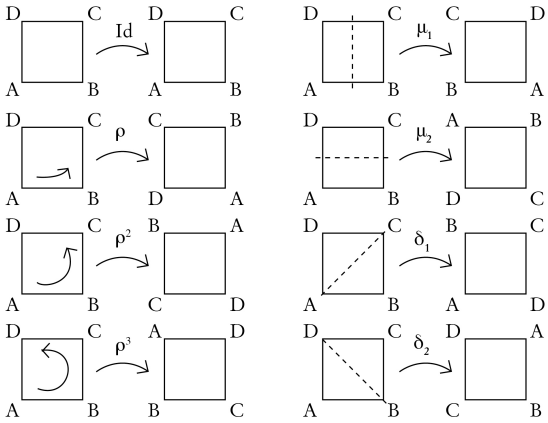


FIGURA 4.4. Todas las simetrías del cuadrado

También en este caso podemos hacer una tabla de todas las posibles composiciones.

$*$	Id	ρ	ρ^2	ρ^3	μ_1	μ_2	δ_1	δ_2
Id	Id	ρ	ρ^2	ρ^3	μ_1	μ_2	δ_1	δ_2
ρ	ρ	ρ^2	ρ^3	Id	δ_2	δ_1	μ_1	μ_2
ρ^2	ρ^2	ρ^3	Id	ρ	μ_2	μ_1	δ_2	δ_1
ρ^3	ρ^3	Id	ρ	ρ^2	δ_1	δ_2	μ_2	μ_1
μ_1	μ_1	δ_1	μ_2	δ_2	Id	ρ^2	ρ	ρ^3
μ_2	μ_2	δ_2	μ_1	δ_1	ρ^2	Id	ρ^3	ρ
δ_1	δ_1	μ_2	δ_2	μ_1	ρ^3	ρ	Id	ρ^2
δ_2	δ_2	μ_1	δ_1	μ_2	ρ	ρ^3	ρ^2	Id

4.3.3 Ejercicios

1. Encuentre las simetrías de las letras T, D, Z, O.
2. Encuentre las simetrías de un rectángulo, de un triángulo isósceles, de uno escaleno.
3. Encuentre las simetrías de una circunferencia.
4. Suponga que τ es una simetría de un hexágono regular cuyos vértices están numerados de 1 a 6.
   a) Si $\tau(1) = 3$, ¿cuáles son las posibilidades para $\tau(2)$?
   b) ¿Puede ser que $\tau(2) = 3$ y $\tau(4) = 2$?
   c) Si conocemos $\tau(1)$ y $\tau(4)$, ¿podemos saber de qué simetría se trata?
   d) Conjeture cuántos vértices debe conocer para determinar la simetría. Generalice su conjetura a simetrías de cualquier polígono regular.

5. Generalice el concepto de simetría de una figura plana a cuerpos en el espacio. Encuentre las simetrías de un cubo, de un tetraedro regular, de un paralelepípedo cualquiera, de una esfera.

Capítulo 5: Grupos

En este capítulo desarrollaremos los rudimentos de la teoría de grupos, una de las ideas más unificadoras de la matemática y que abarca entre otros a todos los ejemplos del capítulo anterior. La teoría de grupos es de la mayor importancia en el álgebra moderna y tiene gran cantidad de aplicaciones dentro y fuera de la matemática.

Su origen está en el centro del álgebra clásica, a saber, la búsqueda de una solución de las ecuaciones polinomiales por radicales. Esto quiere decir tratar de encontrar la solución de la ecuación

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

en términos de los coeficientes $a_0, a_1, \ldots, a_n$ usando operaciones algebraicas y raíces n–ésimas. El ejemplo conocido por todos es la solución por radicales de la ecuación de segundo grado $ax^2 + bx + c = 0$ mediante la fórmula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}\,.$$

Esta fórmula ya era conocida por el matemático indio Brahmagupta en el siglo VII.

En el siglo XVI se encontró la solución por radicales de las ecuaciones de tercer y cuarto grados. La solución con toda generalidad de la ecuación de tercer grado aparentemente fue hecha por N. Tartaglia. La historia de este descubrimiento es tragicómica e involucra a personajes pintorescos como el propio Tartaglia y G. Cardano, además de E. del Ferro, quien fue el primero en encontrar solución a algunos casos particulares y L. Ferrari, discípulo de Cardano y descubridor de la fórmula para la ecuación de cuarto grado. Para más detalles históricos y una buena presentación de las soluciones ver [**9**].

Por casi trescientos años se buscó la solución por radicales de la ecuación general de quinto grado sin ningún éxito. Fue en este proceso que matemáticos como Lagrange y Vandermonde a fines del siglo XVIII aplicaron la idea de permutar raíces de polinomios y en el proceso descubrieron las primeras leyes de los que más tarde daría origen al concepto de grupo.

La idea detrás de esto es simple aunque la teoría final es bastante compleja. Si consideramos la ecuación

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

y sus n raíces $x_1, x_2, \ldots, x_n$, entonces

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = (x - x_1)(x - x_2)\cdots(x - x_n)\,.$$

Luego de desarrollar el segundo término e igualar coeficientes se obtiene:

$$\begin{aligned} a_0 &= (-1)^n\, x_1 x_2 \cdots x_n \\ a_1 &= (-1)^{n-1}(x_1 x_2 \cdots x_{n-1} + x_1 x_2 \cdots x_{n-2} x_n + \cdots + x_2 x_3 \cdots x_n) \\ &\vdots \\ a_{n-2} &= x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n \\ a_{n-1} &= -(x_1 + x_2 + \cdots + x_n) \end{aligned}$$

Las funciones del lado derecho se dicen *simétricas* porque son invariantes bajo permutaciones, es decir, si permutamos todas o algunas de las raíces debemos obtener el mismo resultado, consecuentemente, si aplicamos cualquier función racional o radical a los coeficientes $a_0, a_1, \ldots, a_n$, el resultado debe ser simétrico respecto de las raíces $x_1, x_2, \ldots, x_n$.

Sin embargo lo que se busca es encontrar las funciones x_i a partir del sistema anterior de n ecuaciones con n incógnitas y esto se hace ejecutando operaciones racionales y radicales sobre los coeficientes. Observemos que las funciones x_i son altamente asimétricas, por lo que las simetrías de los términos que intervienen en el sistema de ecuaciones deben ser controladas, si se aceptan demasiadas simetrías no se podrá obtener las raíces a partir de los coeficientes.

En el caso $n = 2$, vemos que

$$\begin{aligned} c &= x_1 x_2 \\ b &= -(x_1 + x_2) \\ a &= 1 \end{aligned}$$

de modo que,

$$\begin{aligned} x_1, x_2 &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \\ &= \frac{(x_1 + x_2) \pm \sqrt{(x_1 + x_2)^2 - 4x_1 x_2}}{2} \\ &= \frac{(x_1 + x_2) \pm \sqrt{x_1^2 - 2x_1 x_2 + x_2^2}}{2} \end{aligned}$$

es decir, las raíces x_1 y x_2 se obtienen como combinación de las funciones simétricas $f(x_1, x_2) = x_1 + x_2$ y $g(x_1, x_2) = x_1^2 - 2\, x_1 x_2 + x_2^2$.

Si bien Lagrange y Vandermonde explicaron la solución de las ecuaciones de tercer y cuarto grados en términos de la limitación de las posibles simetrías en S_3 y S_4, no fueron capaces de entender la relación general para $n \geq 5$. A comienzos del siglo XIX, Ruffini y Abel avanzaron lo suficiente en el caso $n = 5$ como para establecer que no es posible encontrar soluciones por radicales de la ecuación general de quinto

grado. Ellos no estaban conscientes del concepto de grupo y sus resultados sólo se pueden interpretar retrospectivamente en la teoría, fue E. Galois quien invento el concepto y de hecho la palabra "grupo". Usando estas nuevas ideas, particularmente el de subgrupo normal, Galois demostró la imposibilidad de encontrar soluciones por radicales de la ecuación de grado $n \geq 5$. Con todo, para Galois un grupo era un grupo de permutaciones. Para conocer sobre la elegante teoría de Galois, el lector puede consultar [**2, 4, 5, 6**] o cualquier otro libro de nivel intermedio de álgebra abstracta.

Cauchy en 1844 sistematizó el concepto de grupo finito de permutaciones e introdujo la notación 1 para el neutro y f^{-1} para el inverso. El concepto de grupo abstracto fue concebido por Cayley, quien vio la necesidad de postular la asociatividad de la operación, que resulta dada para grupos de permutaciones. Paradojalmente, el mismo Cayley demostró que en esencia todo grupo es isomorfo a un grupo de permutaciones, por lo que en estricto rigor, el concepto abstracto es innecesario. Ver más adelante el Teorema 5.40.

5.1 Definiciones y Ejemplos

Definición 5.1. Un *grupo* es un conjunto no vacío G dotado de una operación $*$ que verifica las siguientes condiciones:

1. La operación $*$ es asociativa, es decir, para todo x,y,$z \in G$,
$$(x * y) * z = x * (y * z).$$
2. Existe un elemento $e \in G$ tal que para todo $x \in G$,
$$e * x = x * e = x.$$
Decimos que e es un *elemento neutro* de G.
3. Para todo $x \in G$, existe $y \in G$ tal que
$$x * y = y * x = e\,.$$
Decimos que y es un *inverso* de x.

Si además para todo x, $y \in G$,
$$x * y = y * x,$$
decimos que G es un grupo *conmutativo* o *abeliano*.

En rigor, un grupo está formado por un conjunto y una operación por lo que deberíamos hablar del par $\langle G, * \rangle$. Sin embargo, cuando la operación que estamos considerando se subentiende conocida, hablamos simplemente del grupo G. Debemos observar que sobre un mismo conjunto se puede definir distintas operaciones que lo convierten, por ende, en grupos distintos.

Los tres primeros ejemplos dados a continuación fueron desarrollados con detalle en el capítulo anterior.

Ejemplos 5.2.

1. El conjunto S_n de las permutaciones del conjunto $\{1, 2, \ldots, n\}$, con la composición de funciones como operación es un grupo. En efecto, la composición de funciones es asociativa, la función identidad es una biyección que actúa como elemento neutro y por último toda biyección tiene una inversa. En general, este no es un grupo conmutativo. De hecho es conmutativo sólo si $n \leq 2$.

2. El grupo S_3 tiene 6 elementos, a saber, $Id, (123), (132), (12), (23), (13)$. Si llamamos $\sigma_1 = (23)$, $\sigma_2 = (13)$, $\sigma_3 = (12)$ y $\rho = (123)$, entonces vemos que $\rho^2 = (132)$ y podemos hacer la tabla de la operación:

$*$	Id	ρ	ρ^2	σ_1	σ_2	σ_3
Id	Id	ρ	ρ^2	σ_1	σ_2	σ_3
ρ	ρ	ρ^2	Id	σ_3	σ_1	σ_2
ρ^2	ρ^2	Id	ρ	σ_2	σ_3	σ_1
σ_1	σ_1	σ_2	σ_3	Id	ρ	ρ^2
σ_2	σ_2	σ_3	σ_1	ρ	Id	ρ
σ_3	σ_3	σ_1	σ_2	ρ	ρ	Id

   El lector podrá notar la similitud entre esta tabla de operaciones y la que construimos en el capítulo anterior para las simetrías del triángulo equilátero. El hecho no es casual, las simetrías del triángulo equilátero corresponden a permutaciones de los vértices del triángulo, luego de numerarlos 1, 2, 3. Hemos usado las mismas letras para simbolizar la simetría con la correspondiente permutación de los vertices para poner de relieve este hecho y porque es la práctica habitual: identificamos dos grupos que difieren en su caracterización pero que son esencialmente el mismo. Esto ilustra un concepto importantísimo que estudiaremos en la siguiente sección, el de isomorfismo.

3. El conjunto de todas las isometrías del plano euclidiano, con la composición como operación es un grupo.

4. El conjunto de los movimientos rígidos del cuadrado, formado por todas aquellas transformaciones del plano que llevan los vértices y los lados del cuadrado ABCD de la figura sobre los vértices y lados, respectivamente, del cuadrado sin romper o deformar la figura.

   Este grupo se llama el *grupo diédrico* y lo denotaremos por D_4. Si $\sigma, \tau \in D_4$ la operación $\sigma * \tau$, o simplemente $\sigma\tau$, es el movimiento rígido que se obtiene al efectuar primero τ y en seguida σ.

   Entonces, D_4 es un grupo con la operación dada por la tabla que aparece en la página 76.

5. Más generalmente, podemos definir D_n, el grupo diédrico de grado n, como el grupo de todas las simetrías del polígono regular de n lados. Tal grupo tiene 2n elementos, n rotaciones en $0°$, $\frac{360}{n}°, \ldots, (n-1)\frac{360}{n}°$ y n reflexiones.

6. $\langle \mathbb{Z}, + \rangle$, o simplemente $\mathbb{Z}$, es un grupo. También lo son $\langle \mathbb{Q}, + \rangle$, $\langle \mathbb{R}, + \rangle$ y $\langle \mathbb{C}, + \rangle$.

7. Generalizando el ejemplo anterior, si A es un anillo y nos olvidamos del producto, entonces $\langle A, + \rangle$ es un grupo abeliano.
8. $\langle \mathbb{Z}, \cdot \rangle$, no es un grupo pues a pesar de cumplir con las dos primeras condiciones, no cumple la tercera, hay enteros, por ejemplo el 2, que no tienen inverso.
9. Ya vimos que cualquier anillo es, en particular, un grupo abeliano si consideramos sólo la suma. El ejemplo anterior muestra que esto no es así si consideramos sólo la multiplicación. El problema en muchos casos es que algunos elementos del anillo no tienen inverso multiplicativo. Sin embargo, hay un grupo asociado naturalmente a la parte multiplicativa de todo anillo unitario. Para esto sea A un anillo unitario y definamos

$$A^* = \{a \in A : a \text{ es una unidad de } A\}.$$

O sea, A^* es el subconjunto de A formado por todos los elementos que tienen un inverso multiplicativo. Entonces $\langle A^*, \cdot \rangle$ es un grupo.

Lo primero que debemos recordar es que el producto de dos unidades de un anillo es también una unidad, así, la operación está bien definida.

La demostración de que es un grupo sigue fácilmente. Basta notar que el producto heredado del anillo es asociativo, **1** es una unidad y actúa como neutro y finalmente, como nos hemos restringido precisamente al conjunto de los elementos invertibles, y el producto de dos elementos invertibles es invertible, A^* es un grupo.

Veremos a continuación tres ejemplos de este tipo de grupo.

10. Si K es un cuerpo, entonces $K^* = K - \{0\}$, luego $\langle K^*, \cdot \rangle$ es un grupo abeliano.
11. El anillo de las matrices reales de orden dos.

$$M_2(\mathbb{R})^* = \{ \text{ matrices invertibles de orden } 2\}.$$

Este grupo es muy importante y recibe el nombre de *grupo lineal de orden 2* y se le denota $GL_2(\mathbb{R})$.

Podemos generalizar este ejemplo para obtener $GL_n(\mathbb{R})$, el grupo de las matrices (con coeficientes reales) invertibles de orden n.

Todos estos son grupos no abelianos.

12. Consideremos ahora $\mathbb{Z}^* = \{1, -1\}$ dotado de la multiplicación. Este es un grupo de dos elementos cuyo neutro es el 1 y en el que cada elemento es su propio inverso.
13. Las clases residuales $\mathbb{Z}_n$ con la adición son también un ejemplo muy interesante y de él se pueden sacar muchas conclusiones en teoría de números.

Asociado con ellas está el grupo de sus unidades con el producto como operación

$$\mathbb{Z}_n^* = \{\overline{m} \in \mathbb{Z}_n : (m, n) = 1\}.$$

Teorema 5.3. *Sea G un grupo. Entonces*

1. *Existe un único elemento neutro.*

2. *Para todo $a \in G$, el inverso de a es único. Podemos por lo tanto denotarlo con un símbolo especial, a saber, a^{-1}.*
3. *Para todo $a \in G$,*
$$(a^{-1})^{-1} = a.$$
4. *Para todo $a, b \in G$,*
$$(a * b)^{-1} = b^{-1} * a^{-1}.$$
5. *La ley de cancelación es válida, es decir, si $a * b = a * c$, entonces $b = c$ y si $b * a = c * a$, entonces $b = c$.*
6. *Las ecuaciones*
$$a * x = b \quad y \quad x * a = b,$$
tienen solución única.

Demostración.

1. Supongamos que hay dos neutros e y e'. Entonces
$$e = e * e' = e'.$$
2. Si b y c son dos inversos de a, entonces
$$a * b = e = a * c,$$
luego
$$b = b * e = b * (a * c) = (b * a) * c = e * c = c.$$
3. Basta notar que por definición
$$a^{-1} * (a^{-1})^{-1} = (a^{-1})^{-1} * a^{-1} = e,$$
o sea, $(a^{-1})^{-1}$ es un inverso de a^{-1}. Pero obviamente a también es un inverso de a^{-1}, luego como el inverso de a^{-1} es único, $(a^{-1})^{-1} = a$.
4. Como
$$(a * b) * (b^{-1} * a^{-1}) = (b^{-1} * a^{-1}) * (a * b) = e,$$
por la unicidad del inverso,
$$(a * b)^{-1} = b^{-1} * a^{-1}.$$
5. Supongamos que
$$a * b = a * c$$
luego operando por a^{-1} por la izquierda, obtenemos
$$\begin{aligned} a^{-1} * (a * b) &= a^{-1} * (a * c) \\ (a^{-1} * a) * b &= (a^{-1} * a) * c \\ e * b &= e * c \\ b &= c. \end{aligned}$$
Para la otra cancelación se procede igual pero operando por la derecha.

6. Para la primera ecuación, operando por a^{-1} por la izquierda obtenemos

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

Para la otra ecuación se procede igual operando por la derecha. En ambos casos el resultado es obviamente único

□

En general se puede dar distintas estructuras de grupo a un mismo conjunto, basta para ello dotarlo de distintas operaciones. Por ejemplo, si definimos sobre $\mathbb{Q}$ la operación

$$a * b = \frac{ab}{2},$$

$\langle \mathbb{Q}^*, * \rangle$ es un grupo cuyo neutro es 2 y tal que $a^{-1} = \frac{2}{a}$, por lo tanto $\langle \mathbb{Q}^*, \cdot \rangle$ y $\langle \mathbb{Q}^*, * \rangle$ son dos grupos distintos definidos sobre el mismo conjunto.

Para conjuntos muy pequeños, se puede estudiar todas las posibles operaciones escribiendo todas las posibles tablas, tal como hicimos anteriormente las tablas de $\mathbb{Z}_2$, $\mathbb{Z}_3$ etc.

Por ejemplo veamos el caso de un conjunto de dos elementos. Como uno (y sólo uno) de ellos debe ser el neutro, lo designaremos con la letra e y llamaremos a al otro elemento. La tabla empieza así :

$*$	e	a
e	e	a
a	a	?

ya que e es el elemento neutro. Ahora es cosa de observar que puesto que a debe tener un inverso, debe haber algún elemento que operado con a sea el neutro, luego hay una sola forma de llenar el casillero marcado con ? , la única posibilidad es que a sea su propio inverso. Por lo tanto la única tabla sobre un conjunto de dos elementos que define una operación de grupo es

$*$	e	a
e	e	a
a	a	e

Debemos verificar que efectivamente la operación definida por la tabla anterior es asociativa. Esto es muy fácil de ver.

Observe que hemos demostrado que, esencialmente, hay un único grupo de dos elementos. Si cambiamos e por 0 y a por 1, tenemos que la tabla refleja al grupo $\mathbb{Z}_2$.

Veamos ahora el caso de un conjunto con tres elementos e, a y b y construyamos su tabla.

$*$	e	a	b
e	e	a	b
a	a	?	
b	b		

Debemos observar ahora que por el teorema 5.3,6, en cada línea (o columna) de la tabla debe aparecer cada elemento del conjunto. Por otra parte, por la ley de cancelación, en cada línea (o columna) cada elemento puede aparecer sólo una vez.

Por lo tanto en ? no puedo poner a, porque aparecería dos veces en la línea. Tampoco puedo poner e, porque en ese caso, b tendría que aparecer dos veces en la tercera columna, luego la única posibilidad es poner b en ?.

Por supuesto, esto obliga a que los otros tres lugares sean llenados como sigue

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

El lector puede como ejercicio intentar llenar las tablas para conjuntos con cuatro, cinco y seis elementos. Por ejemplo, hay sólo dos grupos con cuatro elementos, estos están dados por las tablas siguientes.

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Esencialmente, hay sólo dos grupos de cuatro elementos, uno de cinco elementos y dos de seis elementos.

Notación:

Si no hay confusión posible usaremos la notación

$$a * b = ab.$$

En este caso hablaremos del *producto* de a y b. En caso de que el grupo tenga un símbolo de operación conocido, por ejemplo $+$ o $\circ$, usaremos ese símbolo. También es habitual usar la convención de denotar la operación de los grupos abelianos con el símbolo $+$ de la adición, o sea,

$$\begin{aligned} a * b &= a + b, \\ a^{-1} &= -a. \end{aligned}$$

5.1.1 Grupos isomorfos

Usando tablas para las posibles operaciones sobre un conjunto hemos visto que hay sólo un grupo con dos elementos. Esto tiene que ser una forma de hablar porque ya conocemos varios grupos de dos elementos, a saber, $\mathbb{Z}_2$, S_2, $\langle\{1,-1\},\cdot\rangle$, $\langle\{Id,\mu\},\circ\rangle$, donde μ es una reflexión en el plano, o bien $\langle\{Id,\rho\},\cdot\rangle$, donde ρ es una rotación en 180° en torno a cualquier punto del plano, etc. Si examinamos las tablas de sus operaciones encontramos:

$+$	0	1
0	0	1
1	1	0

;

$\circ$	Id	(12)
Id	Id	(12)
(12)	(12)	Id

;

$\cdot$	1	-1
1	1	-1
-1	-1	1

$\circ$	Id	μ
Id	Id	μ
μ	μ	Id

;

$\circ$	Id	ρ
Id	Id	ρ
ρ	ρ	Id

vemos que ellas son iguales, salvo por el nombre que damos a la identidad y al segundo elemento. Estos grupos, si bien son distintos tienen la misma forma, decimos que son isomorfos. Más técnicamente, dos grupos son isomorfos si existe una biyección entre ellos que es compatible con las operaciones. Es decir, dos grupos G y H son *isomorfos* si existe una biyección $f : G \longrightarrow H$ tal que para todo x e $y \in G$

$$f(xy) = f(x)f(y).$$

La función f recibe el nombre de *isomorfismo de grupos*.

El concepto de isomorfismo es un caso particular de función que estudiaremos en una próxima sección, los homomorfismos, sin embargo, el concepto mismo de isomorfía es más elemental que aquél ya que la noción de ser iguales salvo por el nombre de los elementos es muy intuitiva, como lo ilustra el ejemplo de los grupos de dos elementos.

Ejemplos 5.4.

1. Dados cualesquiera dos de los grupos de dos elementos del ejemplo anterior, la función que manda el neutro de uno en el neutro del otro y el segundo elemento del primero en el segundo elemento del otro es obviamente una biyección. Para ver que las operaciones se comportan bien, basta verificar las tablas, por lo tanto dicha función es un isomorfismo.
2. La función $f : S_3 \longrightarrow D_3$ tal que para cada permutación $\mu \in S_3$ su imagen $f(\mu)$ es el movimiento rígido del triángulo equilátero que se obtiene al permutar los vértices del triángulo (numerados 1, 2 y 3) de la manera obvia es un isomorfismo.

   Es habitual en la literatura referirse a estos dos grupos como S_3. Rara vez se distingue entre éste y D_3, que tiene una connotación más geométrica.
3. Los grupos $\langle\mathbb{C}^*,\cdot\rangle$ y $\langle\mathbb{R}^*,\cdot\rangle$ de los números complejos y los números reales no nulos con la multiplicación como operación, respectivamente, no son isomorfos. Para ver esto, observemos primero que si f es un isomorfismo entre dos grupos entonces $f(e) = f(ee) = f(e)f(e)$, luego cancelando $f(e)$ tenemos $f(e) = e$. En nuestro caso si $f : \mathbb{C} \longrightarrow \mathbb{R}$ fuera un isomorfismo, tenemos que $f(1) = 1$.

Esto tiene consecuencias. En primer lugar, $(f(-1))^2 = f((-1)^2) = f(1) = 1$ y como $f(-1) \in \mathbb{R}$, $f(-1) = 1$ o bien $f(-1) = -1$. El primer caso es imposible pues tendríamos $f(-1) = 1 = f(1)$ y f es una biyección.

Por lo tanto $f(-1) = -1$. Este caso también tiene complicaciones porque ahora $(f(i))^2 = f(i^2) = f(-1) = -1$. Pero $f(i) \in \mathbb{R}$ y tendríamos un número real cuyo cuadrado es negativo, lo que es imposible. Por lo tanto no puede haber un isomorfismo entre estos grupos.

4. Los grupos $\langle \mathbb{Q}, + \rangle$ y $\langle \mathbb{R}, + \rangle$ no son isomorfos. Basta ver que $\mathbb{Q}$ y $\mathbb{R}$ no tienen la misma cardinalidad, luego no puede haber un isomorfismo entre ellos.

Los grupos isomorfos son "iguales" salvo en el nombre de sus elementos. En general es más fácil ver que dos grupos no son isomorfos. Para ello basta encontrar una propiedad que tenga uno de ellos pero no el otro. En cambio para demostrar que sí son isomorfos se debe construir el isomorfismo.

Ejercicios 5.5.

1. Diga cuáles de los siguientes conjuntos son grupos con respecto a las operaciones indicada.
   a) $\{\overline{2}, \overline{4}, \overline{6}, \overline{8}\}$ en $\mathbb{Z}_{10}$ con el producto como operación.
   b) $\{\frac{m}{n} \in \mathbb{Q} : (m, n) = 1 \text{ y } 3|n\}$ con la suma como operación.
   c) El conjunto de los racionales positivos con el producto como operación.
   d) El conjunto de los números irracionales con la suma como operación.
2. Definamos el conjunto $\mathbf{Q} = \{\mathbf{1}, -\mathbf{1}, \mathbf{i}, -\mathbf{i}, \mathbf{j}, -\mathbf{j}, \mathbf{k}, -\mathbf{k}\}$ de matrices complejas, donde
$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \ \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$
   Demuestre que Q con la multiplicación de matrices usual es un grupo. Este se llama el grupo de los *cuaterniones*. Lo descubrió W. R. Hamilton en 1843 y fue el primer ejemplo de un sistema algebraico no conmutativo. La representación matricial de los cuaterniones dada aquí no es la original de Hamilton.
3. Considere el conjunto G formado por las siguientes funciones de $\mathbb{R} - \{0, 1\}$ en sí mismo.
$$Id(x) = x \qquad f_1(x) = \tfrac{1}{1-x} \qquad f_2(x) = \tfrac{x-1}{x}$$
$$g_1(x) = \tfrac{1}{x} \qquad g_2(x) = 1 - x \qquad g_3(x) = \tfrac{x}{x-1}$$
   Demuestre que G con la composición de funciones como operación es un grupo. ¿A qué grupo que usted conoce es isomorfo este grupo?
4. Demuestre que si G_1 y G_2 son grupos, entonces $G_1 \times G_2$, con la operación definida por coordenadas, es decir, $(a_1, a_2) * (b_1, b_2) = (a_1\, b_1, a_2\, b_2)$ es un grupo.

   Extienda esta idea a productos de tres, cuatro o más grupos, ¿es esta la única manera de definir un grupo sobre el producto cartesiano de G_1 y G_2?
5. Demuestre que hay sólo dos grupos de cuatro elementos, uno de cinco elementos y dos de seis elementos.

6. Los grupos $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$ tienen cuatro elementos. Demuestre que no son isomorfos. Por lo tanto estos son, salvo isomorfismo, los dos únicos grupos de cuatro elementos mencionados en el problema anterior. El grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$ se llama el *grupo de Klein*.
7. Encuentre tres grupos isomorfos a $\mathbb{Z}_3$.
8. Diga por qué los siguientes pares de grupos no son isomorfos.
   a) $\mathbb{Z}_8$ y D_4
   b) $\mathbb{Z}_4 \times \mathbb{Z}_2$ y $\mathbb{Z}_8$
   c) $\mathbb{Z}$ y $\mathbb{R}$
9. El siguiente ejercicio es importante pero supone cierto manejo de la estructura de los números complejos. El lector que no la conozca puede descartarlo sin perder nada de los contenidos centrales del capítulo. Se llama *raíces n–ésimas de la unidad* a las soluciones complejas de la ecuación $x^n = 1$. Como vimos en el Capítulo 2, todo polinomio tiene tantas raíces complejas como su grado, de modo que hay n raíces n–ésimas de la unidad.
   a) Demuestre que el conjunto W_n de las raíces n–ésimas de la unidad son un subgrupo del grupo $\langle \mathbb{C}^*, \cdot \rangle$ de los números complejos bajo multiplicación.
   b) Demuestre que el conjunto $W = \bigcup_{n \in \mathbb{N}} W_n$ de todas las raíces de la unidad, para cualquier n, son un subgrupo de $\langle \mathbb{C}^*, \cdot \rangle$.
   c) Aprovechando que los números complejos se pueden visualizar en el plano, haga una representación geométrica de estos grupos.

5.2 Subgrupos, Subgrupo Generado, Grupos Cíclicos y el Teorema de Lagrange

Definición 5.6. Un subconjunto no vacío H de un grupo G es un *subgrupo* de G si H dotado de la misma operación es un grupo.

Si H es subgrupo de G escribimos $H \leq G$. Si $H \neq G$ decimos que H es un *subgrupo propio* de G.

Ejemplos 5.7.

1. $\mathbb{Z}$ es un subgrupo de $\mathbb{Q}$.
2. $2\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$.
3. Sea
$$H = \{\sigma \in S_n : \sigma(n) = n\}.$$
Entonces $H \leq S_n$.
4. Sean
$$\begin{aligned} H_1 &= \{A \in GL_2(\mathbb{R}) : A \text{ es triangular superior}\}, \\ H_2 &= \{A \in GL_2(\mathbb{R}) : det(A) = 1\}. \end{aligned}$$
Entonces H_1 y H_2 son subgrupos de $GL_2(\mathbb{R})$.
5. Consideremos $\mathcal{Z}(G) = \{g \in G : gx = xg \quad \text{para todo} \quad x \in G\}$, es decir el conjunto de aquellos elementos que conmutan con todos los elementos de G. Este es un subgrupo llamado el *centro* de G. Si G es abeliano entonces $\mathcal{Z}(G) = G$.

6. Todo grupo G tiene al menos dos subgrupos, a saber $\{e\}$ y G. Estos se llaman los *subgrupos triviales* de G.

Para verificar si un cierto subconjunto de un grupo es o no un subgrupo, conviene usar el siguiente teorema.

Teorema 5.8. *Sea G un grupo y sea $H \subseteq G$. Las siguientes proposiciones son equivalentes:*

1. *H es subgrupo de G.*
2.
   (i) *$H \neq \emptyset$.*
   (ii) *H es cerrado bajo productos, i.e., si $a, b \in H$, entonces $ab \in H$.*
   (iii) *H es cerrado bajo inversos, i.e., si $a \in H$, entonces $a^{-1} \in H$.*
3.
   (i') *$H \neq \emptyset$.*
   (ii') *Si $a, b \in H$, entonces $ab^{-1} \in H$.*

Demostración. Está claro que 1 implica 2 ya que la operación debe estar definida sobre H y todo elemento tiene que tener inverso en H.

También es inmediato que 2 implica 3.

Para ver que 3 implica 1, es claro que la operación de G restringida a H sigue siendo asociativa.

H contiene al elemento neutro, ya que sabemos por *(i')* que $H \neq \emptyset$, luego existe $a \in H$ y por *(ii')*, $e = a\,a^{-1} \in H$.

También por *(ii')* para todo $a \in H$,

$$a^{-1} = e\,a^{-1} \in H,$$

es decir todo elemento de H tiene su elemento inverso en H.

Por último, si a, $b \in H$, entonces, como $b^{-1} \in H$,

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

o sea, la operación de grupo está bien definida en H.

Todo lo anterior demuestra que si H verifica *(i')* y *(ii')*, $H \leq G$.

Esto completa la demostración del teorema. □

Ejercicio 5.9. Sea G un grupo. Si $H \subseteq G$ es no vacío, finito y cerrado bajo productos, entonces $H \leq G$.

Demostración. Por el teorema anterior, como H es no vacío y cerrado bajo productos, basta ver que también es cerrado bajo inversos.

Sea $a \in H$ y sea $n = |H|$ el número de elementos de H. Si definimos para todo j entero positivo

$$a^j = \underbrace{a a \cdots a}_{j},$$

entonces

$$a, a^2, a^3, \ldots, a^n, a^{n+1} \in H.$$

Pero tenemos sólo n elementos en H, luego por lo menos dos de ellos tienen que ser iguales, digamos

$$a^i = a^k$$

para ciertos números $1 \leq i < k \leq n+1$.

Pero entonces cancelando a i veces, obtenemos

$$e = a^{k-i} = aa^{k-i-1} = a^{k-i-1}a,$$

vale decir, si $k-i-1 > 0$,

$$a^{-1} = a^{k-i-1} \in H.$$

Si $k-i-1 = 0$, entonces $e = a^{k-i} = a$, por lo tanto $a^{-1} = e = a \in H$. □

Teorema 5.10. *Si para cada $i \in I$, H_i es un subgrupo del grupo G, entonces*

$$H = \bigcap_{i \in I} H_i \leq G.$$

Demostración. Es claro que $H \neq \emptyset$, ya que para todo $i \in I$, $e \in H_i$, luego $e \in H$.

Si x, $y \in H$, entonces para todo $i \in I$, x, $y \in H_i$, y por el teorema 5.8 (i"), $xy^{-1} \in H_i$, luego $xy^{-1} \in H$. Entonces por el mismo teorema, H es un subgrupo de G. □

Sean G un grupo y $X \subseteq G$, (X no necesariamente un subgrupo de G). Entonces

$$K = \bigcap \{H \leq G : X \subset H\},$$

es un subgrupo de G que obviamente contiene a X, es más, este es el subgrupo más pequeño de G que contiene a X, ya que si $X \subset H \leq G$, entonces $K \subset H$ porque la intersección está contenida en cada uno de sus elementos.

Esto nos permite la siguiente definición.

Definición 5.11. Sea X un subconjunto del grupo G, definimos el *subgrupo generado por X* como el menor subgrupo de G que contiene a X.

Si $X = \{a\}$, hablamos del subgrupo cíclico generado por a, estudiaremos estos grupos con más detalle en la próxima sección.

Notación:

$$a^n = \begin{cases} \underbrace{aa\cdots a}_{n} & \text{si } n > 0 \\ e & \text{si } n = 0 \\ \underbrace{a^{-1}a^{-1}\cdots a^{-1}}_{n} & \text{si } n < 0 \end{cases}$$

Como vimos en una demostración anterior, si tomamos potencias de un elemento a de un grupo puede existir un n tal que $a^n = e$, de hecho, si G es finito, tal n tiene que existir. Esto motiva la siguiente definición.

Definición 5.12. El *orden* de un elemento $a \in G$, denotado $|a|$, es el menor entero positivo k tal que $a^k = e$. Si ese entero no existe, decimos que a es de orden infinito.

Teorema 5.13. *Si G es un grupo y $X \subset G$, el subgrupo generado por X es*

$$H = \{x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} : n \in \mathbb{N}, k_i \in \mathbb{Z}, \text{ y } x_i \in X, \text{ para } 1 \leq i \leq n\}.$$

Demostración. Es claro que H es un subconjunto no vacío que contiene a X. También es claro que todo subgrupo que contiene a X, debe contener a H, ya que los subgrupos son cerrados bajo productos e inversos. Por lo tanto nos basta demostrar que H es un grupo.

Ya dijimos que H es no vacío. De la definición se obtiene en forma inmediata que H es cerrado bajo productos. Para ver que también es cerrado bajo inversos, si $h \in H$, digamos $h = x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$, entonces

$$h^{-1} = x_n^{-k_n} x_{n-1}^{-k_{n-1}} \cdots x_1^{-k_1},$$

que también está en H. □

No existe un resultado análogo al teorema 5.10 para la unión de una familia de subgrupos, en general, la unión de dos subgrupos no es un subgrupo como lo demuestra el ejemplo siguiente.

Ejemplo 5.14. Consideremos el grupo S_3 de todas las permutaciones de tres elementos según notaciones del capítulo anterior. Si

$$H_1 = \{Id, \sigma_1\} \text{ y } H_2 = \{Id, \sigma_2\},$$

vemos que su unión no es cerrada bajo productos ya que

$$\sigma_1 \sigma_2 = \rho,$$

luego la unión no es un subgrupo de S_3.

Sin embargo, si para cada $i \in I$, H_i es un subgrupo del grupo G, entonces existe el menor subgrupo que los contiene a todos, a saber, el subgrupo generado por

$$X = \bigcup_{i \in I} H_i.$$

Definición 5.15. Sea G un grupo y $H \leq G$. Definimos la siguiente relación sobre G:

$$x \sim y \text{ si y sólo si } xy^{-1} \in H.$$

Decimos que x e y son *congruentes módulo H*.

Observemos que si usamos notación aditiva, lo anterior se escribe

$$x \sim y \text{ si y sólo si } x - y \in H,$$

así, si el grupo es $\mathbb{Z}$ y el subgrupo H es $n\mathbb{Z}$, lo que obtenemos es el ya conocido concepto de congruencia módulo n de los enteros estudiada en el Capítulo 1.

Lema 5.16. *La relación definida arriba es una relación de equivalencia.*

Demostración. Si $x \in G$ entonces $xx^{-1} = e \in H$, luego $x \sim x$, o sea, $\sim$ es reflexiva.

Supongamos que $x \sim y$, es decir, $xy^{-1} \in H$, pero como H es subgrupo, es cerrado bajo inversos, luego

$$yx^{-1} = (y^{-1})^{-1}x^{-1} = (xy^{-1})^{-1} \in H.$$

Esto prueba la simetría de $\sim$.

Por último, si $x \sim y$ y $y \sim z$,

$$xy^{-1} \in H \text{ y } yz^{-1} \in H,$$

y como H es cerrado bajo productos,

$$xz^{-1} = (xy^{-1})(yz^{-1}) \in H.$$

Luego $\sim$ es transitiva. □

Observe que para demostrar que $\sim$ es relación de equivalencia, hemos usado todas las condiciones que definen un subgrupo.

Definición 5.17. Las clases de equivalencia de la relación de congruencia módulo H se denominan *clases laterales.*

La clase de a se denota Ha.

La notación anterior se justifica ya que la clase de a está dada por

$$\{x : xa^{-1} \in H\} = \{ha : h \in H\},$$

es decir, los elementos de la clase de a son de la forma "un elemento de H por a". Por ejemplo, la clase del elemento neutro e es

$$He = \{he : h \in H\} = H.$$

Observemos que en notación aditiva la clase sería $H + a$ y como la operación se supone conmutativa, esto es lo mismo que $a + H$, que fue la notación empleada en el Capítulo 3 para la relación análoga, es decir, esta notación es consistente con la anterior.

Lema 5.18. *Si $H \leq G$, $a \in G$, entonces*

$$|Ha| = |H|.$$

Demostración. Definimos

$$\begin{aligned} f : H &\longrightarrow Ha \\ h &\longmapsto ha. \end{aligned}$$

f es inyectiva ya que por la ley de cancelación, Si $ha = h'a$, entonces $h = h'$.

f es sobreyectiva ya que si $x \in Ha$, existe $h \in H$ tal que

$$x = ha = f(h).$$

□

Observación 5.1. Las clases laterales que hemos definido en esta sección habitualmente se llaman *clases laterales derechas* ya que la clase de a se obtiene operando por la derecha todos los elementos de H por a.

Esto resultó de la relación de equivalencia usada. Si definimos

$$x \sim y \text{ si y sólo si } x^{-1}y \in H,$$

ésta también es una relación de equivalencia, la única diferencia es que la clase de equivalencia de a ahora es

$$\{x : a^{-1}x \in H\} = \{ah : h \in H\} = aH\,.$$

Estas se denominan *clases laterales izquierdas.*

Resulta claro que el teorema 5.18 es también válido para clases izquierdas, es decir, toda clase lateral, izquierda o derecha, tiene la misma cardinalidad que H.

Debemos hacer notar que en general, las clases laterales izquierdas y derechas no coinciden. Por ejemplo, si consideramos el subgrupo $H = \{Id, \sigma_1\}$ de S_3, entonces las clases laterales derechas son

$$\{Id, \sigma_1\},\ \{\rho, \sigma_2\},\ \{\rho^2, \sigma_3\},$$

y las clases laterales izquierdas son

$$\{Id, \sigma_1\},\ \{\rho, \sigma_3\},\ \{\rho^2, \sigma_2\}.$$

Definición 5.19. Sea G un grupo.

1. El número de elementos de G, denotado $|G|$, se llama el *orden* de G.
2. Si $H \leq G$, el *índice de* H *en* G, denotado $(G : H)$, es el número de clases laterales (izquierdas o derechas) módulo H.

Teorema 5.20. Teorema de Lagrange.
Si G es un grupo finito y $H \leq G$, entonces $|H| \mid |G|$.

Demostración. Como $\sim$ es una relación de equivalencia, las clases laterales forman una partición de G. Además, como G es finito y cada clase es no vacía, hay un numero finito de clases, es decir,

$$G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_k,$$

para algún entero positivo k. Como las clases son disjuntas, esto implica que

$$|G| = |Ha_1| + |Ha_2| + \cdots + |Ha_k|,$$

luego

$$|G| = k|H|,$$

lo que termina la demostración. □

Corolario 5.21. *Si G es un grupo finito y $H \leq G$, entonces*

$$(G : H) = \frac{|G|}{|H|}.$$

El recíproco del teorema de Lagrange no es verdadero, es decir, si n divide al orden de un grupo, este no necesariamente tiene un subgrupo de orden n. El contraejemplo más pequeño es el grupo alternante A_4, cuyo orden es 12 pero que no tiene subgrupos de orden 6. Su demostración requiere de ciertos conceptos adicionales y la haremos en una sección más adelante.

Hay varios teoremas que dan respuesta parcial al recíproco del teorema de Lagrange. Mencionaremos algunos posponiendo para la última sección las demostraciones de las dos más importantes, a saber, el Teorema de Cauchy y una parte del teorema de Sylow.

Teorema 5.22. Teorema de Cauchy.
Si G es un grupo finito y $p \mid |G|$, p primo, entonces G tiene un elemento de orden p (y por lo tanto contiene un subgrupo de orden p).

Teorema 5.23. *Si G es un grupo finito conmutativo y $m \mid |G|$, entonces existe un subgrupo H de G tal que $|H| = m$.*

Teorema 5.24. Teorema de Sylow.
Si $|G| = p^n m$ donde p es primo y $(p, m) = 1$, entonces G tiene subgrupos de orden p, $p^2, \ldots, p^n$.

5.2.1 Grupos Cíclicos

Los grupos cíclicos tienen un papel muy destacado, sobre todo en la teoría de grupos abelianos finitos. Aunque no profundizaremos en ese aspecto, los estudiaremos con cierto detalle.

Definición 5.25. Un grupo G se dice *cíclico* si existe un elemento $a \in G$ tal que el subgrupo generado por a es todo G.

Observemos que como caso particular del teorema 5.13, el grupo cíclico generado por a está dado por

$$\{a^n : n \in \mathbb{Z}\}.$$

Teorema 5.26. *Si $a \in G$, entonces $|a|$ es el orden del grupo cíclico generado por a.*

Corolario 5.27. *Si G es finito y $a \in G$, entonces $|a| \mid |G|$.*

Corolario 5.28. *Si $|G| = n$ y $a \in G$, entonces $a^n = e$.*

Demostración. Como $|a| \mid |G|$, existe entero k tal que $n = |a|\, k$, luego

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

□

El siguiente corolario nos da una elegante demostración dentro de la teoría de conjuntos del teorema de Euler–Fermat que estudiamos en el Capítulo 1.

Corolario 5.29. Teorema de Euler-Fermat.
Si $(a, n) = 1$, *entonces*

$$a^{\varphi(n)} \equiv 1 \ (\textit{mód } n).$$

Demostración. Consideremos el grupo $\mathbb{Z}_n^*$ de las unidades del anillo $\mathbb{Z}_n$. Como vimos en el Capítulo 1, este grupo tiene $\varphi(n)$ elementos.

Ahora bien, como $(a, n) = 1$, $\overline{a} \in \mathbb{Z}_n^*$, por lo tanto

$$\overline{a}^{\,\varphi(n)} = \overline{1},$$

o lo que es lo mismo,

$$a^{\varphi(n)} \equiv 1 \ (\text{mód } n).$$

□

Teorema 5.30. *Si* G *es un grupo tal que* $|G| > 1$ *y no tiene subgrupos propios, entonces* G *es cíclico y de orden primo.*

Demostración. Como $|G| > 1$ podemos escoger un elemento $g \in G$ tal que $g \neq e$. Sea H el subgrupo de G generado por g. Entonces $g \in H \neq \{e\}$ luego por la hipótesis, $H = G$, es decir, G es cíclico.

Si el orden de H no fuera primo, digamos $|H| = m\,n$, entonces $a^m \neq e$, porque $m < |H| = |a|$, y $(a^m)^n = a^{mn} = a^{|H|} = e$, o sea, el orden de a^m es n y por lo tanto el subgrupo generado por a^m sería un subgrupo propio de G, contradiciendo nuestra hipótesis. □

Teorema 5.31. *Sea* G *un grupo cíclico.*

1. *Si* G *es infinito, entonces* G *es isomorfo con* $\mathbb{Z}$.
2. *Si* G *es finito de orden* n, *entonces* G *es isomorfo con* $\mathbb{Z}_n$.

Demostración. Sea a un generador de G. Si a es de orden infinito, entonces los elementos a^n son todos distintos y $G = \{a^n : n \in \mathbb{Z}\}$. Es inmediato que la función $f : \mathbb{Z} \longrightarrow G$ tal que $f(n) = a^n$ es un isomorfismo ya que es una biyección y $f(n+m) = a^{n+m} = a^n\,a^m = f(n)\,f(m)$.

Algo similar ocurre si $|G| = n$. En este caso $G = \{e, a, a^2, \ldots, a^{n-1}\}$ y la misma función es un isomorfismo. □

5.2.2 Ejercicios

1. En los ejercicios de la sección anterior definimos el conjunto W de todas las raíces de la unidad, ¿cuál es el orden de W? ¿cómo es el orden de cada uno de los elementos de W?
2. Diga cuáles son los órdenes posibles para los subgrupos de $\mathbb{Z}_{18}$, S_4 y $D_4 \times \mathbb{Z}_{10}$.
3. Suponga que el grupo G tiene elementos de orden 1, 2 $\cdots$, 12, ¿se puede decir qué orden tiene G?

4. Demuestre que si G es un grupo abeliano de orden par, entonces G tiene exactamente un elemento de orden 2, ¿sigue siendo cierto si G no es abeliano?
5. Demuestre que si $H \leq G$ y $K \leq G$ y $|H| = m$ y $|K| = n$, donde $(m, n) = 1$, entonces $|H \cap K| = 1$.
6. Demuestre que si $H \leq G$, $K \leq G$, $H \neq K$ y $|H| = |K| = p$, donde p es primo, entonces $|H \cap K| = 1$.
7. Demuestre que todo grupo de orden 33 contiene un elemento de orden 3. Indicación: Use el problema anterior.
8. Diga cuáles de los siguientes grupos son cíclicos.

   $a)$ $\mathbb{Q}$ $\quad$ $b)$ $\mathbb{Z}_3 \times \mathbb{Z}_4$

   $c)$ $\mathbb{Z}_3 \times \mathbb{Z}_6$ $\quad$ $d)$ R

   $e)$ D_5 $\quad$ $f)$ W_n

   (R es el grupo de todas las rotaciones del plano en torno al origen. W_n es el grupo de las raíces n–ésimas de la unidad definido antes en los ejercicios.)
9. Diga por qué los siguientes pares de grupos no son isomorfos.

   a) $\mathbb{Z}_4 \times \mathbb{Z}_2$ y D_4

   b) $\mathbb{Z}_4 \times \mathbb{Z}_2$ y $\mathbb{Z}_8$

   c) $\mathbb{Z}$ y $\mathbb{Q}$

5.3 Subgrupos Normales

Si G es un grupo y $H \leq G$, queremos ver la posibilidad de dotar al conjunto de clases laterales módulo H de una operación tal que defina sobre ellas una estructura de grupo. Como en el caso de los anillos, o en el caso particular de las clases residuales estudiado en el Capítulo 1, el punto crucial es que la operación debe estar bien definida, es decir, no debe depender de los representantes de las clases que se está usando.

La definición intuitivamente más natural es:

$$Ha * Hb = Hab.$$

Lo que queremos entonces es que si

$$a_1 \sim a_2 \text{ y } b_1 \sim b_2,$$

entonces

$$Ha_1b_1 = Ha_2b_2.$$

Para que esto suceda, como

$$a_1 = ha_2 \text{ y } b_1 = kb_2,$$

para ciertos elementos h y k de H,

$$Ha_1b_1 = Hha_2kb_2 = Ha_2kb_2.$$

Si pudiéramos conmutar los elementos a_2 y k tendríamos el resultado requerido. De hecho, bastaría que

$$a_2k = k'a_2$$

para algún $k' \in H$. Como a_2 es arbitrario, lo que se requiere es que para todo $a \in G$

$$Ha = aH.$$

Definición 5.32. Un subgrupo H del grupo G se dice *normal* si y sólo si para todo $g \in G$,

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

Si H es un subgrupo normal de G, escribiremos $H \lhd G$.

En realidad, para ver si un subgrupo es normal, basta demostrar que para todo $g \in G$, $gHg^{-1} \subset H$, ya que, entonces también $g^{-1}Hg \subset H$ y obtenemos la otra inclusión, $H \subset gHg^{-1}$.

Otra manera de presentar los subgrupos normales es como aquellos subgrupos para los cuales las clases laterales izquierdas y derechas coinciden. Más precisamente

Teorema 5.33. *$H \lhd G$ si y sólo si para cada $g \in G$, $Hg = gH$.*

Su demostración es inmediata.

Debe notarse que esta es una igualdad entre conjuntos, no estamos afirmando que para cada $h \in H$, $hg = gh$, sino que

$$hg \in gH \quad \text{y} \quad gh \in Hg,$$

o bien, para cada $h \in H$, existen h', $h'' \in H$ tales que

$$hg = gh' \quad \text{y} \quad gh = h''g.$$

Ejemplo 5.34.
1. Si G es abeliano, entonces todo subgrupo de G es normal.
2. Si $H = \{Id, \rho, \rho^2, \rho^3\}$, entonces $H \lhd D_4$.
3. Si $H = \{Id, \mu_1\}$, entonces H no es un subgrupo normal de D_4 ya que

$$\rho\mu_1\rho^{-1} = \mu_2 \notin H.$$

4. $A_n \lhd S_n$.

Teorema 5.35. *Sean G un grupo y $H \leq G$ tales que $(G : H) = 2$. Entonces $H \lhd G$.*

Demostración. Como $(G : H) = 2$, hay sólo dos clases laterales derechas y también hay sólo dos clases laterales izquierdas. Como H es una de ellas en ambos casos la otra clase lateral, ya sea izquierda o derecha es el complemento de H. Por lo tanto las clases laterales son H y H'.

Si $a \in H$, entonces $Ha = H = aH$.

Si $a \notin H$, entonces $Ha = H' = aH$, en cualquier caso, $Ha = aH$, luego el subgrupo es normal. □

Este teorema tiene una bonita aplicación, que quedó pendiente de una sección anterior, a saber, que el recíproco del Teorema de Lagrange es falso.

Ejemplo 5.36. El grupo alternante A_4, cuyo orden es 12 no tiene subgrupos de orden 6.

Demostración. Observamos que los ciclos de largo 3 son permutaciones pares, o sea pertenecen a A_4. Hay 8 ciclos de largo 3, por lo tanto hay sólo 4 permutaciones pares que no son ciclos de largo 3, de modo que un subgrupo H de 6 elementos debe contener al menos un ciclo de largo 3 digamos $(a\,b\,c)$.

Por otra parte, como $(A_4 : H) = 2$, tenemos que $H \lhd A_4$, o sea, si $\sigma \in A_4$, entonces $\sigma(a\,b\,c)\sigma^{-1} \in H$.

Recordemos que en el capítulo anterior vimos que $\sigma(a\,b\,c)\sigma^{-1} = (\sigma(a)\,\sigma(b)\,\sigma(c))$.

Ahora es cosa de hacer unos pocos cálculos. Consideraremos el ciclo $(\sigma(a)\,\sigma(b)\,\sigma(c))$ para algunas permutaciones pares σ, más precisamente los ciclos de largo 3 $(b\,d\,c)$, $(a\,d\,b)$ y $(b\,d\,c)$. El resultado es respectivamente, $(b\,d\,c)$, $(d\,a\,c)$ y $(a\,d\,b)$, es decir todos estos ciclos pertenecen a H. Pero H es un subgrupo, luego los inversos de estos ciclos también pertenecen a H. Por lo tanto H contiene a los 8 ciclos de largo 3, lo que no es posible ya que $|H| = 6$. □

Teorema 5.37. *Si $H \lhd G$, entonces*

$$G \,/\, H = \{Ha : a \in G\},$$

dotado de la operación

$$HaHb = Hab,$$

es un grupo llamado el grupo cuociente *de G por H. El neutro de este grupo es*

$$He = H,$$

y el inverso es

$$(Ha)^{-1} = Ha^{-1}.$$

Si G es abeliano, $G \,/\, H$, también lo es.

Demostración. Lo más importante es hacer notar que la operación está bien definida, pero eso es precisamente lo que motivó nuestra definición de subgrupo normal así es que eso está demostrado.

El resto es trivial, por ejemplo, $Ha\,H = Ha\,He = Hae = Ha$ y similarmente $H\,Ha = Ha$, es decir, H es un neutro para esta operación.

Para el inverso,

$$Ha\,Ha^{-1} = Haa^{-1} = He = H$$

que es el neutro de $G \,/\, H$. Similarmente $Ha^{-1}\,Ha = H$, por lo tanto Ha^{-1} es el inverso de Ha.

Por último, si G es abeliano, entonces $Ha\,Hb = Hab = Hba = Hb\,Ha$, es decir, $G \,/\, H$ es abeliano. □

5.3.1 Ejercicios

1. Encuentre todos los subgrupos de S_3. Diga cuáles son normales. Haga lo mismo para D_4, D_5 y todos los grupos que conozca.
2. Encuentre ejemplos de grupos tales que $K \lhd H \lhd G$, pero K no es normal en G.
3. Para los siguientes grupos y su respectivo subgrupo normal demuestre lo siguiente:
   a) $\mathbb{Z}_{12} \,/\, N \cong \mathbb{Z}_4$, donde $N = \{0, 4, 8\}$.
   b) $\mathbb{Z}_4 \times \mathbb{Z}_4 \,/\, N \cong \mathbb{Z}_4$, donde N es el subgrupo cíclico de $\mathbb{Z}_4 \times \mathbb{Z}_4$ generado por $(1, 2)$.
   c) $\mathbb{Z}_6 \times \mathbb{Z}_4 \,/\, N \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, donde N es el subgrupo cíclico de $\mathbb{Z}_6 \times \mathbb{Z}_4$ generado por $(2, 2)$.
4. Sea $H = \{Id, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$. Demuestre que $H \lhd S_4$. Encuentre un grupo conocido que sea isomorfo con $S_4 \,/\, H$.
5. Describa los elementos de $\mathbb{Q} \,/\, \mathbb{Z}$. Demuestre que todos los elementos de $\mathbb{Q} \,/\, \mathbb{Z}$ tienen orden finito. Demuestre que en $\mathbb{Q} \,/\, \mathbb{Z}$ hay elementos de todos los órdenes finitos posibles.
6. Sean $H \leq G$ y $N \lhd G$. Definamos $H\,N = \{h\,n \,:\, h \in H\,,\, n \in N\}$. Demuestre:
   a) $H\,N = N\,H$
   b) $H\,N \leq G$.
   c) $H \cap N \lhd H$.
   d) Verifique que si ni H ni N es normal, entonces $H\,N$ no es necesariamente un subgrupo.
   e) Si también $H \lhd G$, entonces $H\,N \lhd G$.
   f) Aunque ninguno de los subgrupos sea normal, $|H\,N| = \frac{|H|\,|N|}{|H \cap N|}$.

5.4 Homomorfismos

Definición 5.38. Sean G y H dos grupos. Una función $f : G \longrightarrow H$ es un *homomorfismo* si y sólo si

$$f(xy) = f(x)f(y).$$

Observe que el concepto de isomorfismo introducido en la primera sección es un caso particular de homomorfismo. Al igual que en el caso de los anillos, suele usarse también los conceptos de monomorfismo y epimorfismo. Un tipo especial de isomorfismo es aquel en que va del grupo G en sí mismo. Estos se llaman automorfismos y tienen un papel destacado en la teoría.

Ejemplos 5.39.

1. $\begin{aligned} f \,:\, \mathbb{Z} &\longrightarrow \mathbb{Z}_n \\ k &\longmapsto \overline{k}. \end{aligned}$
2. $\begin{aligned} f \,:\, G &\longrightarrow G \\ g &\longmapsto g. \end{aligned}$
3. $\begin{aligned} f \,:\, G &\longrightarrow H \\ g &\longmapsto e. \end{aligned}$

donde H es un grupo cualquiera. Este se llama el *homomorfismo trivial*.

4. $f : \mathbb{Z} \longrightarrow \mathbb{Z}_2$
$$n \longmapsto \begin{cases} 0 & \text{si } n \text{ es par,} \\ 1 & \text{si } n \text{ es impar.} \end{cases}$$

5. $f : \mathbb{R} \longrightarrow \mathbb{C}^*$
$$x \longmapsto cos\, x + i sen\, x.$$

6. $f : \{-1, 1\} \longrightarrow \mathbb{Z}_2$
$$n \longmapsto \begin{cases} 0 & \text{si } n = 1\,, \\ 1 & \text{si } n = -1\,. \end{cases}$$

7. $f : \mathbb{R}^+ \longrightarrow \langle \mathbb{R}, + \rangle$
$$x \longmapsto log\, x.$$

8. $f : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$
$$A \longmapsto det\,(A).$$

9. $T_a : G \longrightarrow G$
$$g \longmapsto a\, g.$$

Este último ejemplo es particularmente interesante. Si definimos

$$L(G) = \{T_a : a \in G\},$$

y llamamos $S(G)$ al conjunto de todas las permutaciones de los elementos de G, entonces

$$L(G) \leq S(G).$$

En efecto, resulta obvio que para cualquier $a \in G$, T_a es inyectiva. Además, si $g \in G$, entonces

$$g = aa^{-1}g = T_a(a^{-1}g),$$

luego T_a es sobreyectiva, o sea, T_a es una permutación de los elementos de G, es decir, $L(G) \subset S(G)$. También es claro que $L(G) \neq \emptyset$.

Por último, si T_a, $T_b \in L(G)$, entonces

$$(T_b)^{-1} = T_{b^{-1}} \in S(L),$$

ya que para todo x

$$T_b \circ T_{b^{-1}}(x) = T_b(b^{-1}x) = bb^{-1}x = x,$$

$$T_{b^{-1}} \circ T_b(x) = T_{b^{-1}}(bx) = b^{-1}bx = x,$$

además, como

$$T_a \circ T_b(x) = T_a(bx) = (ab)x = T_{ab}(x),$$

o sea,

$$T_a \circ T_b = T_{ab} \in S(L),$$

y por el teorema 5.8, $L(G) \leq S(G)$.

Lo anterior nos permite demostrar un famoso teorema que nos dice que, esencialmente, todos los grupos se pueden pensar como grupos de permutaciones de ciertos objetos. En particular obtenemos que todo grupo de orden finito n es isomorfo a un subgrupo de S_n.

Teorema 5.40. Teorema de Cayley.
Todo grupo es isomorfo a un subgrupo de un grupo de permutaciones.

Demostración. Definimos el isomorfismo de la manera obvia:

$$\begin{aligned} \Phi : G &\longrightarrow L(G) \\ a &\longmapsto T_a. \end{aligned}$$

Φ es inyectiva ya que si

$$\begin{aligned} \Phi(a) &= \Phi(b), \\ T_a &= T_b, \end{aligned}$$

luego evaluando en e,

$$a = ae = T_a(e) = T_b(e) = be = b.$$

Φ es obviamente sobreyectiva, puesto que para cada $a \in G$,

$$T_a = \Phi(a).$$

Para verificar que Φ es un homomorfismo, como vimos en el párrafo anterior,

$$\Phi(ab) = T_{ab} = T_a \circ T_b.$$

Por lo tanto, G es isomorfo a $L(G)$ que es un subgrupo del grupo de permutaciones $S(G)$. □

Teorema 5.41. *Si $f : G \longrightarrow H$ es un homomorfismo,*

1. $f(e) = e$
2. $f(a^{-1}) = (f(a))^{-1}$

Demostración. Para demostrar 1,

$$f(e) = f(ee) = f(e)f(e).$$

Multiplicando por $(f(e))^{-1}$ a cada lado,

$$e = f(e).$$

Para demostrar 2,

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

y

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

o sea

$$f(a^{-1}) = (f(a))^{-1}.$$

□

Definición 5.42. Si G y H son dos grupos y $f : G \longrightarrow H$ es un homomorfismo,

1. Llamamos *núcleo* o *kernel* de f a $ker\ f = \{g \in G : f(g) = e\}$.
2. Llamamos *imagen* de G por f a $Im\ f = \{f(g) : g \in G\}$.

Teorema 5.43. *Si $f : G \longrightarrow H$ es homomorfismo, entonces*

1. $ker\ f \lhd G$.
2. $Im\ f \leq H$.

Demostración.

1. En primer lugar, como $e \in ker\ f$, éste no es vacío.
   Sean a y b dos elementos del kernel de f. Entonces

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

luego $ab^{-1} \in ker\ f$ y por el teorema 5.8, $ker\ f \leq G$.

Para ver que $ker\ f$ es normal, sea $a \in ker\ f$ y $g \in G$, entonces

$$f(gag^{-1}) = f(g)f(a)(f(g))^{-1} = f(g)e(f(g))^{-1} = f(g)(f(g))^{-1} = e,$$

luego $gag^{-1} \in ker\ f$, es decir,

$$g\ ker\ f\ g^{-1} \subseteq ker\ f,$$

y el subgrupo es normal.

2. Como $f(e) = e$, $Im\ f$ no es vacío.
   Sean h y k elementos de $Im\ f$. Luego existen $a, b \in G$ tales que $h = f(a)$ y $k = f(b)$. Por lo tanto

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

luego $Im\ f \leq H$. □

Luego de demostrar el teorema anterior, resulta natural preguntarse si $Im\ f$ es o no un subgrupo normal de H. El siguiente ejemplo responde esta pregunta.

Ejemplos 5.44.

1. Consideremos la función

$$\begin{array}{rcl} f : \mathbb{Z}_2 & \longrightarrow & S_3 \\ n & \longmapsto & \begin{cases} Id & \text{si } n = \overline{0}, \\ \mu_1 & \text{si } n = \overline{1}. \end{cases} \end{array}$$

   f es un homomorfismo sin embargo, como vimos en los ejemplos, $Im\ f$ no es un subgrupo normal de S_3.

2. La primera proposición del teorema anterior es un caso particular, el más usado, de algo más general.

   Sea $f : G \longrightarrow H$ un homomorfismo y sea $N \leq H$. Entonces $f^{-1}(N) \leq G$.

   Si $N \lhd H$, entonces $f^{-1}(N) \lhd G$.

   Demostración. Escribamos $M = f^{-1}(N)$ para simplificar la notación.

   Es claro que $M \neq \emptyset$. Sean $x, y \in M$. Entonces $f(x) = a \in N$ y $f(y) = b \in N$. Entonces $f(x\,y^{-1}) = f(x)f(y)^{-1} = a\,b^{-1} \in N$, porque N es grupo.

   Supongamos ahora que $N \lhd H$ y sea $g \in G$. Si $x \in gMg^{-1}$, entonces $x = gmg^{-1}$, para algún $m \in M$, o sea $f(m) = n \in N$. Entonces $f(x) = f(gmg^{-1}) = f(g)f(m)(f(g))^{-1} = f(g)n(f(g))^{-1} \in N$, porque N es normal en H. Por lo tanto $M \lhd G$. □

Teorema 5.45. *Sea G un grupo y $N \lhd G$. Entonces*

$$\begin{array}{rcl} \Phi : G & \longrightarrow & G \,/\, N \\ g & \longmapsto & Ng \end{array}$$

es un homomorfismo.

El núcleo de este homomorfismo es N.

Demostración. Es claro que Φ es un homomorfismo ya que

$$\Phi(ab) = Nab = Na\ Nb = \Phi(a)\Phi(b).$$

Para encontrar el núcleo de Φ, notemos que $x \in ker\ \Phi$ si y sólo si $\Phi(x) = Nx = N$ si y sólo si $x \in N$. □

Teorema 5.46. *Sea $f : G \longrightarrow H$ un homomorfismo, entonces*

$$f \text{ es inyectiva si y sólo si } ker\ f = \{e\}.$$

Demostración. Supongamos que f es inyectiva. Entonces si $a \in ker\ f$,

$$f(a) = e = f(e),$$

luego $a = e$, o sea,

$$ker\ f = \{e\}.$$

Supongamos ahora que $ker\ f = \{e\}$. Entonces Si $f(a) = f(b)$,

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

o sea,

$$ab^{-1} \in ker\ f = \{e\},$$

y entonces $a = b$, por lo tanto f es inyectiva. □

Teorema 5.47. Primer teorema del isomorfismo.
Sean G y H grupos, $f : G \longrightarrow H$ un homomorfismo. Entonces

$$G \,/\, ker\ f \cong Im\ f.$$

Demostración. Para abreviar escribamos $N = ker\ f$ y definamos la función

$$\begin{aligned} \varphi : G \,/\, N &\longrightarrow Im\ f \\ Na &\longmapsto f(a). \end{aligned}$$

Entonces

$$\begin{aligned} \varphi(Na) = \varphi(Nb) \quad &\text{si y sólo si} \quad f(a) = f(b) \\ &\text{si y sólo si} \quad f(a)(f(b))^{-1} = e \\ &\text{si y sólo si} \quad f(ab^{-1}) = e \\ &\text{si y sólo si} \quad ab^{-1} \in ker\ f \\ &\text{si y sólo si} \quad Na = Nb, \end{aligned}$$

es decir, φ está bien definida ($\Leftarrow$) y es inyectiva ($\Rightarrow$).

Si $b \in Im\ f$, entonces $b = f(a)$ para algún $a \in G$. Por lo tanto $b = \varphi(Na)$ y φ es sobreyectiva, por lo tanto es biyectiva. Falta verificar que φ es un homomorfismo, pero esto es inmediato dada la forma en la que se definió el producto de clases y que f es un homomorfismo:

$$\varphi(Na\,Nb) = \varphi(Nab) = f(ab) = f(a)\,f(b)\,.$$

□

Corolario 5.48. *Si G es un grupo finito y $f : G \longrightarrow H$ es un homomorfismo, entonces*

$$|G| = |Im\ f| \cdot |ker\ f|.$$

Demostración. Del teorema anterior obtenemos

$$|G \,/\, ker\ f| = |Im\ f|,$$

pero como sabemos

$$|G \,/\, ker\ f| = (G : ker\ f) = \frac{|G|}{|ker\ f|}.$$

□

5.4.1 Ejercicios

1. Sean G un grupo y $g \in G$. Demuestre que $f_g : G \longrightarrow H$ definido por $f_g(x) = g^{-1}\,x\,g$ es un automorfismo. Estos son muy importantes en la teoría de grupos y reciben el nombre de *automorfismos interiores.*
2. Demuestre que si G es cíclico y a es un generador, entonces un homomorfismo $f : G \longrightarrow H$ queda determinado por la imagen $f(a)$ del generador.

3. Encuentre todos los homomorfismos de $\mathbb{Z}_4$ en $\mathbb{Z}_{12}$. Haga lo mismo a la inversa, o sea, desde $\mathbb{Z}_{12}$ en $\mathbb{Z}_4$. Ahora desde $\mathbb{Z}_4$ en $\mathbb{Z}_9$. Repita este ejercicio con diversas combinaciones de grupos $\mathbb{Z}_n$. Conjeture un teorema general acerca de todos los homomorfismos de $\mathbb{Z}_n$ en $\mathbb{Z}_m$. Ahora demuéstrelo.
4. Encuentre todos los posibles grupos que pueden ser imagen homomorfa de $\mathbb{Z}_{12}$, $\mathbb{Z}_{15}$, S_3 y D_4.
5. Demuestre que si $f : G \longrightarrow H$ es un homomorfismo sobreyectivo entonces
   a) Si G es abeliano, entonces H es abeliano.
   b) Si G es cíclico, entonces H es cíclico.

   ¿Valen los teoremas recíprocos?
6. Sean $H \leq G$ y $N \lhd G$. En los ejercicios de la sección anterior se pidió demostrar que $H \cap N \lhd H$ además, es inmediato que $H \cap N \lhd H\,N$. Demuestre que

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

   Este resultado se conoce como el *Segundo teorema del isomorfismo* .

5.5 Acción de un Grupo sobre un Conjunto

Una de las facetas más interesantes de los grupos es que ellos aparecen en distintas áreas de la ciencia, no sólo de la matemática. Por ejemplo, en físico–química, donde la simetrías de las moléculas, descritas naturalmente por un grupo de simetrías, pueden usarse para determinar la energía potencial de la molécula. Los grupos son una herramienta importante en cristalografía. Los grupos aparecen también en la teoría de códigos correctores de errores, usados en la codificación de mensajes.

Todas estas aplicaciones tienen en común un concepto general, el de acción de un grupo sobre un conjunto.

Sea G un grupo y X un conjunto. Una función $\Phi : G \times X \longrightarrow X$ es una *acción de G sobre X* si para todo $g_1, g_2 \in G$ y para todo $x \in X$

1. $\Phi(e, x) = x$
2. $\Phi(g_1, \Phi(g_2, x)) = \Phi(g_1\, g_2, x)$

Es habitual escribir simplemente $\Phi(g, x) = g \cdot x$ de forma que nuestra definición se reduce a

1. $e \cdot x = x$
2. $g_1 \cdot (g_2 \cdot x) = (g_1\, g_2) \cdot x$

Naturalmente el punto " $\cdot$ " no es una operación, sólo abrevia la función. Esto hay que tenerlo en cuenta porque a menudo se hace actuar el grupo sobre sí mismo (considerado como conjunto) y puede haber confusiones.

Ejemplos 5.49.

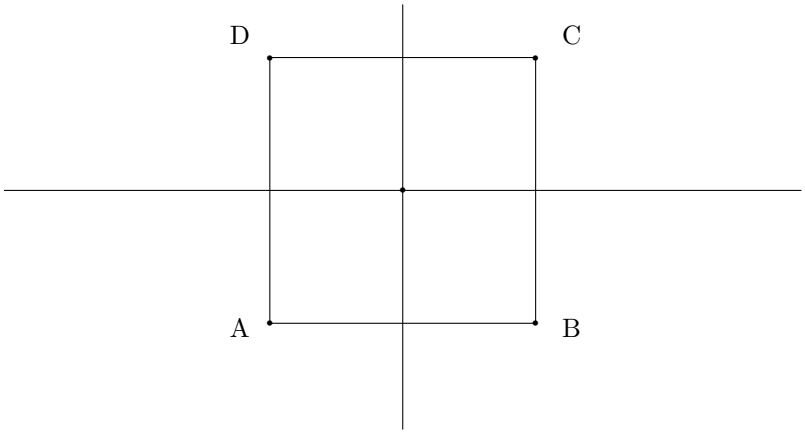
Casi todos los ejemplos del capítulo anterior han sido motivados por una acción natural de un grupo sobre algún conjunto.

1. Consideremos un conjunto de n objetos distintos $X = \{a_1, a_2, \ldots, a_n\}$.

   El grupo simétrico S_n actúa en forma natural sobre el conjunto X. La acción queda definida por

   $$\sigma \cdot a_k = a_{\sigma(k)} .$$

2. El grupo D_4 de las simetrías del cuadrado actúa en forma natural sobre el conjunto $X = \{A, B, C, D, \overline{AB}, \overline{BC}, \overline{CD}, \overline{DA}\}$



3. Podemos hacer actuar el grupo D_4 sobre otros conjuntos, por ejemplo, podemos agregar las diagonales $\overline{AC}$ y $\overline{BD}$, los puntos medios de los lados, etc.

   El grupo D_4 también actúa sobre todo el plano. Dado un punto P de coordenadas (x, y) la acción de los elementos de D_4 sobre P es:

	Id	ρ	ρ^2	ρ^3	μ_1	μ_2	δ_1	δ_2
(x, y)	(x, y)	$(y, -x)$	$(-x, -y)$	$(-y, x)$	$(-x, y)$	$(x, -y)$	(y, x)	$(-y, -x)$

4. Las isometrías pueden también entenderse como acciones de este grupo sobre todos los puntos del plano, o sobre todos los triángulos, o sobre distintos subconjuntos de puntos del plano.

   Una aplicación muy común en la teoría de grupos es hacer actuar un grupo G sobre sí mismo. Dos son las acciones más habituales.

5. Acción por traslación.

   $$\begin{array}{rcl} \cdot : G \times G & \longrightarrow & G \\ (g, x) & \longmapsto & g\,x \end{array}$$

   donde $g\,x$ es simplemente la operación del grupo, que en este caso tiene sentido. Es claro que esta es una acción.

6. Acción por conjugación. Queda definida por $g \cdot x = gxg^{-1}$. Vemos que $e \cdot x = x$ y que $(gh) \cdot x = (gh)x(gh)^{-1} = (gh)x(h^{-1}g^{-1}) = g(hxh^{-1})g^{-1} = g \cdot (h \cdot x)$.

5.5.1 Órbitas y estabilizadores

Vimos en el ejemplo 3 que si D_4 actúa sobre el plano, el punto P de coordenadas (x, y) es enviado a alguno de los puntos (x, y), $(y, -x)$, $(-x, -y)$, $(-y, x)$ y no a otros. El conjunto de puntos a los que $x \in X$ es enviado por la acción del grupo G se denomina la *órbita* de x. Más precisamente, si el grupo G actúa sobre el conjunto X, la órbita de $x \in X$ es

$$\mathcal{O}_x = \{y \in X \,:\, y = g \cdot x \quad \text{para algún} \quad g \in G\}\,.$$

Teorema 5.50. *El conjunto de las órbitas es una partición del conjunto X.*

Demostración. Como $e \cdot x = x$, $x \in \mathcal{O}_x \neq \emptyset$. Las órbitas son disjuntas porque si $z \in \mathcal{O}_x \cap \mathcal{O}_y$, entonces para ciertos $g, h \in G$, $z = g \cdot x = h \cdot y$, luego $y = e \cdot y = (h^{-1}h) \cdot y = h^{-1} \cdot (h \cdot y) = h^{-1} \cdot (g \cdot x) = (h^{-1}g) \cdot x$, o sea, $y \in \mathcal{O}_x$. Pero entonces dado cualquier $z = g \cdot y \in \mathcal{O}_y$, $z = g \cdot (h^{-1} \cdot x) = (gh^{-1}) \cdot x$, o sea, $z \in \mathcal{O}_x$, vale decir $\mathcal{O}_y \subseteq \mathcal{O}_x$. La inclusión en el otro sentido es análoga. □

Ejemplos 5.51.

1. En la acción del grupo simétrico S_n sobre el conjunto $X = \{a_1, a_2, \ldots, a_n\}$ hay una única órbita X.
2. En la acción del grupo D_4 de las simetrías del cuadrado sobre el conjunto $X = \{A, B, C, D, \overline{AB}, \overline{BC}, \overline{CD}, \overline{DA}\}$ de los ejercicios anteriores las órbitas son dos

$$\mathcal{O}_A = \{A, B, C, D\} \quad \text{y} \quad \mathcal{O}_{\overline{AB}}\{\overline{AB}, \overline{BC}, \overline{CD}, \overline{DA}\}\,.$$

3. Como dijimos anteriormente, en la acción del grupo D_4 sobre todo el plano, la órbita de un punto P de coordenadas (x, y) son los puntos

$$\mathcal{O}_P = \{(x, y), (y, -x), (-x, -y), (-y, x)\}\,.$$

   Observe que $\mathcal{O}_{(0,0)} = \{(0, 0)\}$, es decir el origen queda fijo. Este es el único punto que queda fijo bajo la acción de este grupo.
4. En la acción de un grupo sobre sí mismo por conjugación la órbita de x está constituida por todos los conjugados de x, o sea, $\mathcal{O}_x = \{gxg^{-1} \,:\, g \in G\}$. Estas se llaman clases de conjugación. Observe que si G es abeliano, entonces $gxg^{-1} = x$, para todo $g \in G$, de modo que toda órbita tiene un solo elemento, a saber, $\mathcal{O}_x = \{x\}$. De hecho, basta que $x \in \mathcal{Z}(G)$, es decir, que x pertenezca al centro de G, para que $\mathcal{O}_x = \{x\}$. Recíprocamente, si $\mathcal{O}_x = \{x\}$, entonces $x \in \mathcal{Z}(G)$.

Si G actúa sobre X, para cada $x \in X$ definimos el estabilizador de x como

$$G_x = \{g \in G \,:\, g \cdot x = x\}\,.$$

El estabilizador es a veces llamado grupo de isotropía de x.

Teorema 5.52. *El estabilizador de un elemento de X es un subgrupo de G.*

Demostración. Es claro que $e \in G_x$, debido a la primera condición que define las acciones. La segunda condición implica además que G_x es cerrado bajo productos. Para ver que es cerrado bajo inversos usamos ambas condiciones. Si $g \in G_x$, entonces

$$x = e \cdot x = (g^{-1}g) \cdot x = g^{-1}(g \cdot x) = g^{-1} \cdot x\,,$$

o sea, $g^{-1} \in G_x$. □

Ejemplos 5.53.

1. En la acción del grupo simétrico S_n sobre el conjunto $X = \{a_1, a_2, \ldots, a_n\}$ el estabilizador de a_i es $\{\sigma \in S_n : \sigma(i) = i\}$. Es fácil ver que este grupo es isomorfo a S_{n-1}.

2. En la acción del grupo D_4 de las simetrías del cuadrado sobre el conjunto $X = \{A, B, C, D, \overline{AB}, \overline{BC}, \overline{CD}, \overline{DA}\}$ de los ejercicios anteriores los estabilizadores son
   $D_{4\,A} = D_{4C} = \{Id, \delta_1\}$,
   $D_{4\,B} = D_{4D} = \{Id, \delta_2\}$,
   $D_{4\overline{AB}} = D_{4\overline{CD}} = \{Id, \mu_2\}$,
   $D_{4\overline{BC}} = D_{4\overline{DA}} = \{Id, \mu_1\}$.

3. En la acción del grupo D_4 sobre todo el plano, el estabilizador de un punto P de coordenadas (x, y) es

$$D_{4P} = \begin{cases} \{Id\}, & \text{si } x \neq \pm y\,, \\ \{Id, \delta_1\}, & \text{si } x = y \neq 0\,, \\ \{Id, \delta_2\}, & \text{si } x = -y \neq 0\,, \\ D_4, & \text{si } x = y = 0\,. \end{cases}$$

4. En la acción de un grupo sobre sí mismo por conjugación el estabilizador de x está constituida por todos los conjugados de x, o sea, $G_x = \{g : gxg^{-1} = x\} = \{g : gx = xg\}$. Este se llama el *centralizador* de x y es común denotarlo $C(x)$.

   Si $C(x) = G$ entonces x conmuta con todos los elementos de G, o sea, x pertenece al centro de G.

La órbita y el estabilizador de un elemento están relacionados de la siguiente manera.

Teorema 5.54. *Supongamos que un grupo finito G actúa sobre un conjunto X. Si $\mathcal{O}_{x_0}$ y G_{x_0} son respectivamente la órbita y el estabilizador de un elemento x_0 entonces*

$$|\mathcal{O}_{x_0}| = (G : G_{x_0})\,.$$

Demostración. Como el índice de G_{x_0} en G es la cardinalidad de las clases laterales (izquierdas o derechas), basta encontrar una biyección entre éstas y la órbita. Para ello definamos

$$\begin{array}{rcl} f \,:\, \mathcal{O}_{x_0} & \longrightarrow & G \mid G_{x_0} = \{g\, G_{x_0} \,:\, g \in G\} \\ h \cdot x_0 & \longmapsto & h\, G_{x_0} \end{array}$$

La función es inyectiva ya que si $h{\cdot}x_0 = h'{\cdot}x_0$, entonces $x_0 = h^{-1}{\cdot}(h{\cdot}x_0) = (h^{-1}h'){\cdot}x_0$, es decir, $h^{-1}h' \in G_{x_0}$, es decir $h\, G_{x_0} = h'\, G_{x_0}$.

Por otra parte, es claro que f es sobreyectiva, luego es una biyección. □

Corolario 5.55. *Supongamos que un grupo finito G actúa sobre un conjunto X. Si $\{x_1, \ldots, x_n\}$ es un conjunto de representantes de todas las órbitas de la acción, entonces*

$$|X| = \sum_{i=1}^{n} (G : G_{x_i})\,.$$

Demostración. Basta recordar que las órbitas son una partición de X y aplicar el teorema anterior. □

Teorema 5.56. Ecuación de Clase.
Si un grupo finito G actúa sobre sí mismo por conjugación entonces

$$|G| = |\mathcal{Z}(G)| + \sum (G : C(x_i))\,,$$

donde los x_i son los representantes de las órbitas (clases de conjugación) que no pertenecen al centro de G.

Demostración. Aplicaremos el corolario del Teorema 5.54. Separamos las órbitas en aquellas constituidas por un único elemento, a saber, x_i, y aquellas que tienen más de un elemento. Para la acción por conjugación vimos que la órbita de x tiene un único elemento si y sólo si $x \in \mathcal{Z}(G)$. Tenemos entonces tantas órbitas de un solo objeto como elementos tiene el centro de G, es decir,

$$|G| = |\mathcal{Z}(G)| + \sum (G : C(x_i))$$

como se quería. □

Una muy conocida aplicación de este teorema es la siguiente.

Ejemplo 5.57. Sea G un grupo de orden p^n, donde p es un número primo. Entonces $|\mathcal{Z}(G)| > 1$.
Demostración. Hacemos notar nuevamente que si $a \notin \mathcal{Z}(G)$, entonces $C(a) \neq G$, y por el teorema de Lagrange, $(G : C(a)) = p^m$, para algún $m < n$ (naturalmente m depende de a) en cualquier caso, lo importante es que p divide a $(G : C(a))$, y que

por lo tanto p divide a $\sum(G : C(x_i))$, cuando la suma se hace sobre aquellos x_i que no pertenecen al centro. Vemos ahora la ecuación de clase:

$$|G| = p^n = |\mathcal{Z}(G)| + \sum(G : C(x_i)) \,,$$

es decir,

$$|\mathcal{Z}(G)| = p^n - \sum(G : C(x_i))$$

es divisible por p. Como $e \in \mathcal{Z}(G))$, $|\mathcal{Z}(G)| > 1$ y el centro no es trivial. □

5.5.2 Dos aplicaciones importantes: Los teoremas de Cauchy y de Sylow

Demostraremos aquí dos teoremas más avanzados para ilustrar el poder de los conceptos y teoremas desarrollados en esta sección.

Lema 5.58. *Supongamos que G es un grupo de orden p^n, donde p es primo, que actúa sobre el conjunto X. Sea $X_0 = \{x \in X \,:\, g \cdot x = x \quad \text{para todo } g \in G\}$ el conjunto de los puntos de X que permanecen fijos bajo la acción. Entonces*

$$|X| \equiv |X_0| \pmod p \,.$$

Demostración. Debemos distinguir dos clases de órbitas. Para los puntos $x \in X_0$ sus órbitas son $\mathcal{O}_x = \{x\}$. Los puntos que no pertenecen a X_0, por el Teorema 5.54 tienen órbitas de cardinalidad $(G : G_x)$ y como la órbita de x tiene más de un punto, p divide a $(G : G_x)$, en particular p divide a $\sum(G : G_{x_i})$ si la suma se hace sobre todos los representantes que no pertenecen a X_0.

Recordando que las órbitas son una partición de X, tenemos $|X| = \sum|\mathcal{O}_i| = |X_0| + \sum(G : G_{x_i})$, o lo que es lo mismo

$$|X| - |X_0| = \sum(G : G_{x_i}) \,,$$

y como vimos esta última suma es divisible por p. □

Teorema 5.59. Teorema de Cauchy.
Sea G un grupo cuyo orden es divisible por un primo p. Entonces G contiene un elemento de orden p. Esto implica que G tiene un subgrupo de orden p.

Demostración. Consideremos el conjunto

$$X = \{(a_1, a_2, \ldots, a_p) \in G^p \,:\, a_1\, a_2 \cdots a_p = e\} \,.$$

Observe que los primeros $p-1$ elementos de cada p–tupla pueden elegirse arbitrariamente, pero el último queda determinado por las anteriores ya que $a_p = (a_1\, a_2 \cdots a_{p-1})^{-1}$, luego $|X| = |G|^{p-1}$ y por hipótesis es divisible por p.

Consideramos ahora el subgrupo G de S_p generado por el ciclo $\sigma = (12 \cdots p)$. Es claro que $|G| = p$. Hacemos actuar al grupo G iterando la acción de σ dada por

$$\sigma \cdot (a_1, a_2, \ldots, a_p) = (a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(p)}) = (a_2, a_3, \ldots, a_p, a_1) \,.$$

Ésta está bien definida porque como a_1 es el inverso de $a_2\, a_3\, \ldots\, a_p$, tenemos también que $(a_2\, a_3\, \ldots\, a_p)a_1 = e$, o sea $(a_2, a_3, \ldots, a_p, a_1) \in X$.

Como p divide a $|X|$, por el lema anterior, p divide a $|X_0|$. Observamos que $X_0 \neq \emptyset$ ya que la tupla $(e, e, \ldots, e) \in X_0$, por lo tanto $|X_0| > 0$ existe algún otro elemento en X_0.

Finalmente vemos que $(a_1, a_2, \ldots, a_p) \in X_0$ si y sólo si $a_1 = a_2 = \cdots = a_p$, por lo tanto debe existir $(a, a, \ldots, a) \in X_0$, luego $a^p = e$. □

El último teorema de este capítulo es el teorema de Sylow mencionado más arriba como un recíproco parcial del Teorema de Lagrange, ya que nos proporciona algunos divisores del orden de un grupo para los que necesariamente existen subgrupos. El teorema tiene numerosas aplicaciones que permiten estudiar la estructura de un grupo conociendo sólo su orden. Como verá el lector en su demostración usaremos todo lo que hemos aprendido en el capítulo.

Teorema 5.60. Teorema de Sylow.
Sea G un grupo finito de orden $p^n\, m$, donde p es primo y $p \nmid m$. Entonces G contiene un subgrupo de orden p^n.

Demostración. Lo demostraremos por inducción sobre el orden de G. Si $|G| = 1$, entonces el teorema es cierto trivialmente.

Supongamos ahora que $|G| > 1$ y que el resultado es cierto para todos los grupos que tienen orden menor que G, vale decir, tienen un subgrupo cuyo orden es la máxima potencia del primo p que divide a su orden.

Si G no tiene subgrupos propios, entonces por el Teorema 5.30, $|G| = p$ y G es cíclico, por lo que el teorema se cumple.

En el caso en que G sí tiene algún subgrupo propio H. Si $p^n \mid |H|$, por la hipótesis de inducción H tiene un subgrupo de orden p^n, el que a su vez es subgrupo de G.

Nos resta el caso en que $p^n \nmid |H|$. Esto es en particular cierto para el centralizador $C(a)$ de cualquier elemento $a \notin \mathcal{Z}(G)$. Observemos que este último requerimiento es necesario porque si $a \in \mathcal{Z}(G)$, entonces $C(a) = G$. Si miramos el conjunto de las clases laterales módulo $C(a)$, su cardinalidad $(G : C(a)) = \frac{|G|}{|C(a)|}$ es divisible por p, ya que los factores primos p en el numerador son más que los del denominador.

Apliquemos ahora la Ecuación de Clase, Teorema 5.56.

$$p^n\, m = |G| = |\mathcal{Z}(G)| + \sum (G : C(a_i))\,,$$

donde los a_i son los representantes de las clases de conjugación que no están en el centro de G. Por el argumento anterior p divide a esta suma y al término del lado izquierdo, por lo tanto $p \mid |\mathcal{Z}(G)|$.

Por el Teorema de Cauchy, 5.59, existe un elemento $a \in \mathcal{Z}(G)$ que tiene orden p. Si A es el subgrupo generado por a, entonces $|A| = p$. Además como $a \in \mathcal{Z}(G)$, entonces $A \lhd G$ (ver ejercicios).

Consideramos ahora el grupo cuociente $B = G \,/\, A$.

$$|B| = \frac{|G|}{|A|} = \frac{p^n\, m}{p} = p^{n-1}\, m < |G|\,,$$

por lo que le podemos aplicar la hipótesis de inducción, que en este caso significa que B tiene un subgrupo D cuyo orden es p^{n-1}.

Finalmente aplicamos el resultado probado en 5.44 al homomorfismo

$$\varphi : G \longrightarrow G \,/\, A$$

En este caso, como tenemos un subgrupo D de $G \,/\, A$, por lo tanto existe un subgrupo H de G tal que $H \,/\, A = \varphi(H) = D$ y por lo tanto $|H \,/\, A| = \frac{|H|}{p} = p^{n-1}$, por lo tanto $|H| = pn$, que es lo que queríamos demostrar. □

Hemos demostrado la versión más simple del llamado primer teorema de Sylow. Para conocer versiones más completas y las otras proposiciones de este teorema ver la bibliografía.

5.5.3 Ejercicios

1. Demuestre que S_n actúa sobre el conjunto $X = \mathcal{P}(\{1, 2, \ldots, n\})$ de todos los subconjuntos de $\{1, 2, \ldots, n\}$ de la manera obvia, es decir, para $\sigma \in S_n$ y $A \subseteq X$, $\sigma \cdot A = \{\sigma(1), \sigma(2), \ldots, \sigma(n)\}$.

   ¿Cuál es la órbita de $A = \{n-1, n\}$?, ¿cuál es su estabilizador?, ¿a qué grupo es isomorfo?

   Repita las preguntas anteriores para otros subconjuntos de $\{1, 2, \ldots, n\}$.

   Para $n = 2$ y $n = 3$, encuentre todas las órbitas y todos los estabilizadores.
2. Demuestre que S_3 actúa sobre $X = \{\langle x, y\rangle \,:\, 1 \leq x, y \leq 3\}$ de la siguiente manera. $\sigma \cdot \langle x, y\rangle = \langle \sigma(x), \sigma(y)\rangle$. Encuentre las órbitas y los estabilizadores.
3. Haga actuar el grupo D_4 de la manera natural sobre el conjunto X formado por: los cuatro vértices, los cuatro puntos medios de los lados, el centro, los cuatro lados, las dos diagonales y las dos medianas.

   Encuentre las órbitas y los estabilizadores.
4. Sea X el conjunto de todos los subgrupos de un grupo G y hagamos actuar G sobre X por conjugación, es decir, $g \cdot N = gNg^{-1}$. Demuestre que esta es efectivamente una acción.

   Aplíquelo al caso de D_4. Encuentre las órbitas, ¿qué puede decir de éstas?

Bibliografía

[1] Birkhoff, G., MacLane, S. *Álgebra Moderna.* Vicens-Vives, Barcelona, 1963.
[2] Fraleigh, J. B. *Álgebra Abstracta.* Addison-Wesley Iberoamericana, 1988.
[3] Jones, B. J. *Teoría de los Números.* Trillas, México, 1969.
[4] Herstein, I. N. *Álgebra Abstracta.* Grupo Editorial Iberoamérica, 1988.
[5] Herstein, I. N. *Topics in Algebra.* John Wiley & Sons, 1975.
[6] Hungerford, T.W. *Abstract Algebra. An Introduction.* Saunders College Publishing, 1990.
[7] Niven, I., Zuckerman, H. S. *Introducción a la Teoría de los Números.* Limusa-Wiley, 1969.
[8] Ore, O. *Number Theory and its History.* MacGraw-Hill, Nueva York, 1948.
[9] Stillwell, J. *Mathematics and its History.* Springer, Nueva York, 2002.
[10] Suazo, A., Labra, A. *Elementos de la Teoría de Cuerpos.* J.C. Sáez Editor, Santiago, 2011.
[11] Vinogradov, I. *Fundamentos de la Teoría de los Números.* Mir, Moscú, 1971.

Índice de figuras

Índice de Términos