ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE CIENCIAS

CARRERA MATEMÁTICA

UNA INTRODUCCIÓN AL ESTUDIO DE GRUPO, ANILLO Y CAMPO

Trabajo de Integración Curricular

Tipo: Proyecto de Investigación

Presentado para optar al grado académico de:

MATEMÁTICO

AUTOR: VICTOR PAÚL CONDEMAITA IZA

DIRECTOR: Dr. LEONIDAS ANTONIO CERDA ROMERO, PhD.

Riobamba – Ecuador

2022

Yo, VÍCTOR PAÚL CONDEMAITA IZA, declaro que el presente Trabajo de Integración Curricular es de mi autoría y los resultados del mismo son auténticos. Los textos en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Integración Curricular; El patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 19 de octubre de 2022

Víctor Paúl Condemaita Iza

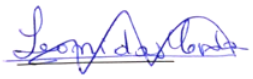
172425447-7

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE CIENCIAS

CARRERA MATEMÁTICA

El Tribunal del Trabajo de Integración Curricular certifica que: el Trabajo de Integración Curricular; Tipo: Proyecto de Investigación. **UNA INTRODUCCIÓN AL ESTUDIO DE GRUPO, ANILLO Y CAMPO**, realizado por: **VICTOR PAÚL CONDEMAITA IZA**, ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de Integración Curricular, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal Autoriza su presentación.

	FIRMA	**FECHA**
Ing. María de Lourdes Palacios Robalino Mgs. **PRESIDENTE DEL TRIBUNAL**		2022-10-19
Dr. Leonidas Antonido Cerda Romero PhD. **DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR**		2022-10-19
Ing. María José Mendoza Salazar Mgs. **MIEMBRO DEL TRIBUNAL**		2022-10-19

DEDICATORIA

Dedico mi investigación a mis padres, César Condemaita y María Iza que me han sabido inculcar los mejores valores y sobre todo ser un ejemplo de constancia y fortaleza diaria. A mis hermanos y hermanas por sus consejos y apoyo en todo momento.

Víctor

AGRADECIMIENTO

Quiero agradecer hoy, mañana y siempre a toda mi familia por su compresión y apoyo incondicional brindado durante mi formación profesional.

Mi eterna gratitud a mis asesores; Dr. Leonidas Cerda y Dra. Zenaida Castillo por su paciencia y orientación otorgada en el desarrollo de mi investigación.

Por último dar las gracias a mis amigos por su gran amistad y a mi novia quién me alentó día a día a cumplir mi meta personal.

Víctor

TABLA DE CONTENIDOS

ÍNDICE DE ANEXOS

RESUMEN

El objetivo del presente proyecto de investigación fue generar un documento guía sobre las estructuras algebraicas de grupos y anillos, para abordar con los temas planteados en las asignaturas de Álgebra Abstracta I y II de la carrera de Matemática de la Escuela Superior Politécnica de Chimborazo. Para ello se consideró una investigación de tipo documental, con enfoque cualitativo y nivel descriptivo, se utilizó el editor de texto Latex y se desarrolló mediante una lectura selectiva, reflexiva y crítica de la bibliografía existente sobre estas estructuras algebraicas. Como resultado se deja una guía de estudio titulada: "Una Introducción al Estudio de Grupo, Anillo y Campo", la cual describe en forma conveniente los tópicos de grupos, subgrupos y homomorfismos entre grupos, además de anillos, subanillos, dominios íntegros y campo de fracciones. Luego de finalizar esta investigación, se concluye que la asignatura Álgebra Abstracta, de la carrera de Matemática, requiere de un entendimiento riguroso de teoremas y demostraciones, y aquellos estudiantes que se inician en su estudio pueden presentar dificultades en el proceso de aprendizaje, sobre todo en los tópicos principales de la teoría de grupos y anillos. Se recomienda continuar el estudio sobre las estructuras algebraicas de grupos y anillos, abarcar sus aplicaciones, los campos de investigación, problemas actuales relacionados con éstas y posiblemente otras estructuras del Álgebra Abstracta.

Palabras clave: <MATEMÁTICA>, <ESTRUCTURAS ALGEBRAICAS>, <GRUPOS>, <ANILLOS>, <MONOGRAFÍA>.

Ing. Leonardo Fabio Medina Ñuste MSc.
1757773294

2083-DBRA-UTP-2022

SUMMARY/ABSTRACT

The aim of the current research work was to generate a guide on algebraic structures of groups and rings, in order to study the topics proposed in the Subjects of Abstract Algebra I and II Subjects, belonging to the Mathematics career of Escuela Superior Politécnica de Chimborazo. Thus, it was necessary to consider a documentary-type research with a qualitative approach and descriptive level, it was also necessary to use Latex text editor which was developed by means of a selective, reflexive and critical reading of the existing bibliography on these algebraic structures. The result is a study guide entitled: "An Introduction to the Study of Group, Ring and Field", which conveniently describes the topics of groups, subgroups and homomorphisms between groups, as well as rings, subrings, integral domains and fraction fields. Once the research finished, it was concluded that the subject of Abstract Algebra, belonging to the Mathematics career requires a rigorous understanding of theorems and demonstrations, and those students who are just starting to study may have difficulties in the learning process, especially on the main topics regarding the group and ring theory. It is recommended to carry on studies on algebraic structures of groups and rings, to consider their applications, research areas, current problems related and possibly other structures of Abstract Algebra.

Keywords: <MATHEMATICS>, <ALGEBRAIC STRUCTURES>, <GROUPS>, <RINGS>, <MONOGRAPH>.

Lic. Paul Rolando Armas Pasántes Mgs.

060328987-7

INTRODUCCIÓN

La asignatura Álgebra Abstracta, que se dicta en la carrera de Matemática de la Escuela Superior Politécnica de Chimborazo (ESPOCH) aborda las estructuras algebraicas de grupos y anillos. Esta teoría tiene mucha influencia debido a su aplicabilidad en problemas de otras disciplinas, tales como; la informática, la física y la química (Gallian, 2017, p.15).

La motivación para desarrollar esta guía de estudios surge de la experiencia personal y la de otros estudiantes al momento de cursar la asignatura Álgebra Abstracta, ya que su didáctica está basada en la comprensión rigurosa de teoremas y demostraciones; actividad que requiere del estudiante un nivel avanzado de abstracción y pensamiento crítico. Adicionalmente, la bibliografía especializada en los tópicos de grupos y anillos la encontramos en otros idiomas, dificultando aún más su entendimiento, y la Biblioteca Central de la ESPOCH no disponen de bibliografía suficiente sobre estas teorías.

La estructura algebraica de grupo permite modelar problemas con simetrías, funciones y el conjunto de los números reales. Cuatro fuentes principales influyeron en el desarrollo de esta teoría; el álgebra clásica estudiada por Lagrange en 1770, la teoría de números desarrollada por Gauss en 1801, la geometría estudiada por Klein en 1874 y el análisis explorado por Lie y Poincaré en 1874 - 1876. El término de anillos fue acuñado por David Hilbert en 1897, aunque una primera definición abstracta formal no se dio hasta que Abraham Fraenkel la presentó en 1914 (Gallian, 2017, p.227). En la teoría de anillos el interés se centra en los anillos conmutativos que han permitido desarrollar una aritmética en entornos más generales que los números enteros. Los antecedentes destacan que la teoría algebraica de números, la teoría invariante y la geometría algebraica fueron las fuentes principales que influyeron en el desarrollo de esta estructura.

Este proyecto de investigación deja como resultado una guía de estudios, pensada y diseñada para los estudiantes que se inician en el aprendizaje la asignatura de Álgebra Abstracta, ya que se escribió en forma sencilla, directa, y cada definición y concepto se ilustra con ejemplos. Ciertamente, no se estudian todos los tópicos de ambas estructuras ya que son teorías sumamente extensas, sin embargo, se espera facilitar la compresión y análisis de los elementos principales que componen estas teorías, e influir positivamente en el aprendizaje de estos tópicos por parte de las futuras generaciones de matemáticos de la ESPOCH.

La guía de estudios ofrece dos módulos, cada uno de los cuales consta de definiciones, proposiciones, teoremas y ejemplos, siempre considerando los aspectos más relevantes de cada estructura, planteados en forma simple y concisa. En el primer módulo se estudia la teoría de grupos, sus

propiedades y homomorfismos entre grupos, mientras que en el segundo módulo se presenta la estructura de anillo, sus propiedades y generalidades.

Es importante recalcar que esta investigación no expone las aplicaciones de las teorías mencionadas, sino que intenta cubrir los contenidos mínimos de los cursos de Álgebra Abstracta, contemplados en la malla curricular de la carrera de Matemática de la ESPOCH.

CAPÍTULO I

1. MARCO TEÓRICO REFERENCIAL

1.1. Antecedentes

En la Escuela Superior Politécnica de Chimborazo, específicamente en la carrera de Matemática, no hay evidencias de la existencia de una guía de estudios sobre las estructuras algebraicas de grupos y anillos, teorías que se trata en la asignatura de Álgebra Abstracta.

Elvis Cotrado (2017, p.40), encontró que la asignatura con menor índice de aprobación es el Álgebra Moderna con un 77,78 %, ya que de los nueve estudiantes del tercer año únicamente aprobaron dos.

De igual manera, la investigación presentada por Valentín Cruz (2001, p.25) refleja que la asignatura Álgebra Abstracta, impartida en el sexto semestre es una de las que presentó mayor dificultad de aprendizaje, según los alumnos de séptimo y noveno semestre de la carrera.

Esto no se debe a que el docente no esté capacitado para dictar la asignatura, sino más bien al hecho de que el Álgebra Abstracta es una de las materias que da inicio a la matemática teórica (pura).

Israel N, docente de la Universidad de Chicago, considera que el álgebra con frecuencia constituye el primer encuentro del estudiante con una disciplina matemática abstracta (Herstein, 1986, p.1).

Por otra parte, Thomas W, en su libro "Abstract Algebra Theory and Applications", señala que:

Uno de los mayores problemas en la enseñanza de un curso de álgebra abstracta es que para muchos estudiantes es su primer encuentro con un entorno que les exige hacer pruebas rigurosas. Tales estudiantes a menudo encuentran difícil ver el uso del aprendizaje para probar teoremas y proposiciones (Judson, 2012, p.3).

De igual manera, otros autores de textos sobre Álgebra Abstracta (Alcock, 2021; Beachy, 2019; Rotman, 2000) opinan que los estudiantes encuentran dificultades de aprendizaje cuando se enfrentan al estudio de dicha asignatura.

Estos antecedentes, sobre la asignatura Álgebra Abstracta, señalan un problema en el aprendizaje de estos tópicos en las carreras de matemática, que influye negativamente en el rendimiento académico de la asignatura, y motivan a realizar esta investigación documental, que dejó como resultado una guía de estudios: "Una Introducción al Estudio de Grupo, Anillo y Campo", enfocada principalmente en los contenidos mínimos requeridos para esta asignatura de Álgebra Abstracta de la carrera de Matemática de la ESPOCH.

1.2. Planteamiento del problema

1.2.1. *Enunciado del problema*

Una de las causas del bajo rendimiento en la asignatura de Álgebra Abstracta, en la carrera de Matemática de la Escuela Superior Politécnica de Chimborazo, es la falta de una guía de estudios que aborde los contenidos mínimos planteados en la malla curricular de la carrera.

1.3. Justificación

En la carrera de matemática de la ESPOCH el estudiante se enfrenta al estudio de las estructuras algebraicas de grupos y anillos, específicamente en el curso de Álgebra Abstracta que se contempla en la malla curricular de la carrera. Esta asignatura da inicio a la matemática teórica, por tal razón requiere de un documento de referencia, basado en un estudio crítico y enfocado en los temas que se dictan en la carrera, el cual influya positivamente en la comprensión de sus tópicos.

1.4. Objetivos

1.4.1. *Objetivo general*

Generar un documento que sirva de referencia para estudiantes de la carrera de matemática de la ESPOCH, mediante una lectura crítica de las referencias bibliográficas especializadas en los tópicos de las estructuras algebraicas de grupos y anillos, a fin de contribuir con la compresión y análisis del Álgebra Abstracta.

1.4.2. *Objetivos específicos*

- Determinar estrategias de búsqueda de información, identificando palabras claves del tema de investigación y las herramientas de búsqueda más útiles, para establecer aquellas fuentes más apropiadas que sustenten los temas planteados.
- Realizar una lectura reflexiva, selectiva y crítica sobre los tópicos de investigación, subrayando la información mas relevante de las referencias seleccionadas, para facilitar la comprensión del Álgebra Abstracta.
- Diseñar y escribir una la guía de estudios con los conceptos y definiciones fundamentales sobre las estructuras de grupos y anillos, mediante el uso del editor de texto LaTeX y basado en fuentes

confiables, para la posterior divulgación del documento.

CAPÍTULO II

2. MARCO METODOLÓGICO

2.1. Enfoque de investigación

Este trabajo de investigación se planificó con una metodología de enfoque cualitativo, debido a que se interpretó de manera subjetiva los contenidos de la bibliografía seleccionada, para describir los tópicos que se estudian en la asignatura de Álgebra Abstracta de la carrera de Matemática de la ESPOCH.

2.2. Nivel de investigación

Esta investigación corresponde a un estudio descriptivo, ya que el interés fue producir una guía de estudio, en la cual se describan los temas más importantes de cada estructura algebraica de acuerdo con los contenidos mínimos requeridos para esta asignatura.

2.3. Diseño de la investigación

La investigación es de tipo documental, con uso de fuentes secundarias debido a que se basó en la recolección de documentos digitales especializados en los temas de grupos y anillos, estos incluyeron: libros, revistas, tesis, monografías y otros. La bibliografía recabada para la redacción del documento guía constó de un 71.42 % de textos en el idioma inglés y poco accesibles para estudiantes que se inician en el estudio de estas estructuras algebraicas. Adicionalmente, se hizo un estudio teórico y crítico sobre estas estructuras para redactar la guía de estudio.

2.3.1. *Recolección y análisis de la información*

Una vez definido el tema de investigación, se procedió a recabar información en fuentes que incluyen libros, tesis y notas todas éstas digitales, las cuales contemplan el estudio de las estructuras algebraicas de grupos y anillos.

Posteriormente, mediante una lectura selectiva de las referencias seleccionadas, se procedió a la clasificación de la misma, eligiendo aquellos documentos que facilitaran el desarrollo y entendimiento de los tópicos que se tratan en la asignatura de Álgebra Abstracta.

2.3.2. *Redacción del trabajo de investigación*

Debido a que la guía de estudio sobre las estructuras de grupos y anillos, está dirigida a estudiantes que se inician en el estudio de la asignatura de Álgebra Abstracta, el documento se escribió de manera clara, concisa y sencilla, además cada definición se ilustra con ejemplos.

Para la escritura del documento guía, se consideraron tres fases; pre-escritura, redacción del escrito y revisión o post-escritura.

La **pre-escritura**, consistió en realizar una lectura reflexiva sobre la teoría de grupos y la teoría de anillos, entender definiciones, proposiciones, teoremas y ejemplos. Una vez entendido los tópicos se realizó un borrador a mano en el cual se especificaba el desarrollo completo de los teoremas, proposiciones y ejemplos en forma sistemática y detallada.

En la fase de **redacción del escrito** se realizó el proceso de escritura digital, para lo cual se utilizó el editor de textos Latex. Por último, la **revisión o post-escritura** consistió en una revisión y depuración final del documento guía.

De esta manera, se generó el documento guía "Una Introducción al Estudio de Grupo, Anillo y Campo", con los contenidos mínimos requeridos para la asignatura de Álgebra Abstracta de la carrera de Matemática de la ESPOCH y cuyo fin es facilitar el aprendizaje de estos tópicos a las futuras generaciones de matemáticos.

CAPÍTULO III

3. MARCO DE RESULTADOS Y DISCUSIÓN DE LOS RESULTADOS

3.1. Resultado

Esta investigación de diseño documental con carácter descriptivo y enfoque cualitativo, generó como resultado una guía de estudio titulado: "Una Introducción al Estudio de Grupo, Anillo y Campo", concebida con la idea de ser utilizada por los estudiantes de la carrera de matemática de la ESPOCH, y cuyo contenido contempla los tópicos mínimos requeridos en las asignaturas de Álgebra Abstracta I y II de la carrera de matemática de la ESPOCH. El propósito del documento es facilitarle al lector el entendimiento de los conceptos básicos sobre estas estructuras, y al mismo tiempo influir en el proceso de enseñanza-aprendizaje de los estudiantes de la carrera.

3.2. Estructura del documento guía

La guía de estudios que se deja como resultado, consta de dos módulos, cada uno de los cuales resalta definiciones, proposiciones, teoremas y ejemplos, siempre considerando los aspectos más relevantes de cada estructura. Adicionalmente, cada una de las secciones ofrece un preámbulo en el cual se identifican los temas a tratar y la estructura de la sección.

Módulo I: En este módulo se contempla el estudio elemental de los tópicos asociados a la Teoría de Grupos, los cuales fueron: grupos y sus propiedades, subgrupos, grupo de congruencia módulo m, grupo de permutaciones, grupos cíclicos, clases laterales, teorema de Lagrange, subgrupo normal, grupo cociente y se finalizó con el tema homomorfismos entre grupos y teorema de Cayley.

Módulo II: Este módulo abarcó el estudio básico relacionado con temas de la Teoría de Anillos, estos fueron: anillos y sus propiedades, subanillos, dominios de integridad, campos, ideales, anillo cociente y por último el tópico de campo de fracciones.

CONCLUSIONES

La asignatura Álgebra Abstracta, de la carrera de Matemática, requiere de un entendimiento riguroso de teoremas y demostraciones, y aquellos estudiantes que se inician en su estudio pueden presentar dificultades en el proceso de aprendizaje, sobre todo en los tópicos principales de la teoría de grupos y anillos.

Como producto del Trabajo de Integración Curricular desarrollado se deja una guía de estudio, que puede ser considerada como material de apoyo didáctico para el entendimiento de los temas de Teoría de Grupos y Teoría de Anillos.

Con respecto a la elaboración de la guía, el módulo que conllevó más tiempo de investigación y desarrollo fue el de la teoría de grupos; especialmente el subtópico de grupos de permutaciones. Esto se debe, en parte, a que fué el primer módulo que se diseñó, y también porque contiene la teoría básica en la cual se apoyan otras estructuras, incluyendo la teoría de anillos, lo cual lo hace más extenso.

La teoría de anillos no presentó mayores inconvenientes en cuanto su comprensión, y la estructura del documento hizo posible su inserción bajo las mismas consideraciones de redacción que el módulo anterior. El tópico de este módulo que requirió más lectura y dedicación fue el de los ideales de un anillo.

Se espera que la guía sea utilizada por las nuevas cohortes de estudiantes de la carrera de Matemática, y que su uso pueda influir positivamente en el proceso de aprendizaje de la asignatura Álgebra Abstracta.

RECOMENDACIONES

En vista de que la guía de estudio “Una Introducción al Estudio de Grupo, Anillo y Campo”, va dirigida a las futuras generaciones de matemáticos, se recomienda que la misma se ponga al alcance de los estudiantes de las próximas cohortes. También sería deseable hacer un estudio sobre su influencia en el aprendizaje y en el rendimiento académico de los estudiantes en la asignatura Álgebra Abstracta.

Son muchas las aplicaciones de las estructuras algebraicas de grupos y anillos, no solo en el campo de la matemática, sino también en otras especialidades, por tal razón se recomienda, a futuro, hacer un estudio detallado de estas aplicaciones, lo cual puede ser extendido a otras estructuras del Álgebra Abstracta.

Por último, se recomienda los lectores interesados en la teoría de anillos, revisar el contenido del primer módulo sobre teoría de grupos, antes de iniciarse en este segundo módulo.

BIBLIOGRAFÍA

ALCOCK, L. *How to Think About Abstract Algebra* [en línea]. New York-USA: Oxford University Press, 2021. [Consulta: 21 diciembre 2021]. Disponible en: https://books.google.com.ec/books?id=_7wcEAAAQBAJ&pg=PA4&dq=how+to+think+about+abstract+algebra&h1=es&sa=X&ved=2ahUKEwjEpdyIwY4_AhVZomoFHfisCaIQ6AF6BAgGEAI#v=onepage&q=how%20to%20think%20about%20abstract%20algebra&f=false

ARENAS, L. *Anillos y Cuerpos* [en línea]. 2008. [Consulta: 11 noviembre 2021]. Disponible en: https://repositorio.uchile.cl//bitstream/handle/2250/120334/Anillos_Cuerpos.pdf?sequence=1&isAllowed=y

AYRES, F. & JAISINGH, L. *Theory and Problems of Abstract Algebra* [en línea]. Second Edition. New York-USA: McGraw-Hill, 2003. [Consulta: 11 noviembre 2021]. Disponible en: http://elibrary.clce.ac.zm:8080/xmlui/handle/123456789/31

BEACHY, J. & BLAIR, W. *Abstract Algebra* [en línea]. Third Edition. Long Grove-USA: Waveland Press, 2019. [Consulta: 24 septiembre 2021]. Disponible en: https://books.google.com.ec/books?id=baEQAAAAQBAJ&printsec=frontcover&dq=ABSTRACT+ALGEBRA+THIRD+EDITION+John+A.+Beachy&hl=es&sa=X&redir_esc=y#v=onepage&q=ABSTRACT%20ALGEBRA%20THIRD%20EDITION%20John%20A.%20Beachy&f=false

BHATTACHARYA, P., JAIN, S., & NAGPAUL, S. *Basic Abstract Algebra* [en línea]. Second Edition. New York-USA: Cambridge University Press, 1994. [Consulta: 11 noviembre 2021]. Disponible en: https://books.google.es/books?hl=es&lr=&id=hiQ8e0b48swC&oi=fnd&pg=PR13&dq=Basic+abstract+algebra.+Bhattacharya&ots=skH6zk2XdD&sig=OqjLo-vgISVcMy5dvx3TiILPmro#v=onepage&q=Basic%20abstract%20algebra.%20Bhattacharya&f=false

BÓNA, M. *Combinatorics of permutations* [en línea]. Third Edition. Florida-USA: CRC Press, 2022. [Consulta: 15 diciembre 2021]. Disponible en: https://books.google.com.ec/books?id=vghsEAAAQBAJ&pg=RA1-PA56&dq=Combinatorics+of+Permutations.+B%C3%B3na,+M.&hl=es&sa=X&ved=2ahUKEwji6qL5zuX4AhXSTDABHSfp

D9IQ6AF6BAgFEAI#v=onepage&q=Combinatorics%20of%20Permutations.%20B%C3%B3na%2C%20M.&f=false

CLARK, A. *Elements of Abstract Algebra* [en línea]. New York-USA: Courier Corporation, 1984. [Consulta: 12 diciembre 2021]. Disponible en: https://books.google.es/books?hl=es&lr=&id=bj1kOY8gOfcC&oi=fnd&pg=PR9&dq=+Element+of+Abstract+Algebra.+Clark&ots=sQCShwpHI7&sig=g-D0CIE_ULNJ_oUuyTcC1uQA9ZI#v=onepage&q=Element%20of%20Abstract%20Algebra.%20Clark&f=false

COTRADO ELVIS. *Nivel de rendimiento académico, prolongación de estudios y deserción de los estudiantes ingresantes del 2009 de la especialidad de matemática, computación e informática de la escuela profesional de educación de la UNJBG* [en línea] (Trabajo de titulación)(Pregrado) Universidad Nacional Jorge Basadre Grohmann, Facultad de Educación, Comunicación y Humanidades, Tacna-Perú, 2017. p.40. [Consulta: 24 mayo 2022]. Disponible en: http://repositorio.unjbg.edu.pe/bitstream/handle/UNJBG/2791/1300_2017_cotrado_cotrado_ee_fech_educacion.pdf?sequence=1&isAllowed=y

CRUZ VALENTÍN. *Diagnóstico de factores e indicadores de deserción y reprobación* [en línea] (Trabajo de titulación)(Pregrado) Universidad Veracruzana, Facultad de Estadística e Informática, México, 2001. p.25. [Consulta: 24 mayo 2022]. Disponible en: https://cdigital.uv.mx/bitstream/handle/123456789/47476/CruzRojasValentin.pdf?sequence=1&isAllowed=y

DORRONSORO, J., & HERNÁNDEZ, E. *Números, Grupos y Anillos* [en línea]. Madrid-España: Addison-Wesley Iberoamericana España, 1996. [Consulta: 2 octubre 2021]. Disponible en: https://es.scribd.com/document/333205197/DORRONSORO-HERNANDEZ-Numeros-Grupos-y-Anillos-pdf

DUMMIT, D., & FOOTE, R. *Abstract Algebra* [en línea]. Third Edition. Vermont-USA: John Wiley & Sons, 2003. [Consulta: 15 noviembre 2021]. Disponible en: https://www.academia.edu/13527708/Abstract_algebra_Dummit_and_Foote

ELLIS, G. *Rings and Fields* [en línea]. New York-USA: Clarendon Press, 1992. [Consulta: 11 noviembre 2021]. Disponible en: https://es.b-ok.lat/book/2397081/85a834

GALLIAN, J. *Contemporany Abstract Algebra* [en línea]. Ninth Edition. USA: Cengage Learning, 2017. [Consulta: 24 septiembre 2021]. Disponible en: https://books.google.com.ec/books?id=JMUaCgAAQBAJ&printsec=frontcover&dq=Contemporary+Abstract+Algebra+-+Gallian,+Joseph+9th+edition&hl=es&sa=X&redir_esc=y#v=onepage&q=Contemporary%20Abstract%20Algebra%20-%20Gallian%2C%20Joseph%209th%20edition&f=false

HERSTEIN, I. *Abstract Algebra* [en línea]. Third Edition. Illinois-USA: Prentice Hall, 1996. [Consulta: 11 noviembre 2021]. Disponible en: https://kupdf.net/download/abstract-algebra-herstein-3rd-ed_59036ef7dc0d60c21e959f07_pdf

HUMPHREYS, J. *A Course in Group Theory* [en línea]. New York-USA: Oxford University Press, 1996. [Consulta: 11 noviembre 2021]. Disponible en: https://books.google.es/books?hl=es&lr=&id=2jBqvVb0Q-AC&oi=fnd&pg=PA1&dq=+A+course+in+group+theory.+Humphreys,+J.&ots=c0aw3bBdKK&sig=lbgA8ipSFIivcu-ntwutggon_rE#v=onepage&q=A%20course%20in%20group%20theory.%20Humphreys%2C%20J.&f=false

JUDSON, T. *Abstract Algebra Theory and Applications* [en línea]. Texas-USA: Orthogonal Publishing, 2012. [Consulta: 8 septiembre 2021]. Disponible en: http://debracollege.dspaces.org/bitstream/123456789/9/1/Thomas%20W.%20Judson.pdf

KLEINER, I. *A History of Abstract Algebra* [en línea]. Boston-Canadá: Springer, 2007. [Consulta: 26 octubre 2021]. Disponible en: https://books.google.es/books?hl=es&lr=&id=RTLRBK-wj6wC&oi=fnd&pg=PR11&dq=A+History+of+Abstract+Algebra&ots=p_QqRc9oHB&sig=5mPTJcBdnqY08o9UaYy6Jx1yw2k#v=onepage&q=A%20History%20of%20Abstract%20Algebra&f=false

LANG, S. *Algebra* [en línea]. Third Edition. New York-USA: Springer, 2005. [Consulta: 16 noviembre 2021]. Disponible en: https://math24.files.wordpress.com/2013/02/algebra-serge-lang.pdf

RIVERO, F. *Álgebra: Estructuras Algebraicas* [en línea]. Venezuela. 1996. [Consulta: 24 noviembre 2021]. Disponible en: https://fdocuments.mx/document/a-l-g-e-b-r-a-estructuras-algebraicas.html?page=7f

RIZO, J. *Técnicas de investigación documental* [en línea]. Manugua-Nicaragua: UNAN-FAREM Matagalpa, 2015. [Consulta: 16 mayo 2022]. Disponible en: https://farematagalpa.unan.edu.ni/pdf/TECNICAS%20DE%20INVESTIGACION%20DOCUMENTAL.pdf

ROTMAN, J. *A First Course in Abstract Algebra* [en línea]. Third Edition. Illinios-USA: Prentice Hall, 2000. [Consulta: 15 diciembre 2021]. Disponible en: https://github.com/carlosal1015/Books/blob/master/A%20first%20course%20in%20Abstract%20algebra%20by%20J.%20Rotman.pdf

TÁBARA, J. *Introducción a la teoría de anillos* [en línea]. 2001. [Consulta: 13 noviembre 2021]. Disponible en: http://mimosa.pntic.mec.es/jgomez53/matema/docums/tabara-anillos.pdf

ZALDÍVAR, F. *Introducción a la teoría de grupos* [en línea]. México: Reverte, 2007. [Consulta: 6 diciembre 2021]. Disponible en: https://books.google.com.ec/books?id=mNaJ1LC5WkUC&printsec=frontcover&dq=Barrera,+F.+(2004).+Introducci%C3%B3n+a+la+teor%C3%ADa+de+grupos.+La+Universidad+Aut%C3%B3noma+del+Estado+de+Hidalgo+(UAEH).&hl=es&sa=X&ved=2ahUKEwi7zKGExOX4AhXVmYQIHQnWDxYQ6AF6BAgLEAI#v=onepage&q&f=false

ZALDÍVAR, F. *Introducción a la teoría de números.* [en línea]. México: Fondo de Cultura Económica, 2014. [Consulta: 1 diciembre 2021]. Disponible en: https://books.google.es/books?hl=es&lr=&id=lPVsBgAAQBAJ&oi=fnd&pg=PP1&dq=Zald%C3%ADvar,+F.+(2014).+Introducci%C3%B3n+a+la+teor%C3%ADa+de+n%C3%BAmeros.+&ots=b3UlyIGxae&sig=57eTVEa0i0La1AATl-A35OjJUug#v=onepage&q=Zald%C3%ADvar%2C%20F.%20(2014).%20Introducci%C3%B3n%20a%20la%20teor%C3%ADa%20de%20n%C3%BAmeros.&f=false

ANEXOS

ANEXO A: GUÍA DE ESTUDIO "UNA INTRODUCCIÓN AL ESTUDIO DE GRUPO, ANILLO Y CAMPO"

Guía de estudio

Una introducción al estudio de Grupo, Anillo y Campo

Realizado por:

Víctor Condemaita

2022

Tabla de contenido

Prefacio

Se presenta una guía de estudio inicial sobre las estructuras algebraicas de Grupos y Anillos, la cual intenta cubrir estos temas, dictados en los cursos de Álgebra Abstracta, contemplados en la malla curricular de la carrera de Matemática de la Escuela Superior Politécnica de Chimborazo.

El propósito del documento es facilitarle al lector el entendimiento de los conceptos básicos sobre estas estructuras, y al mismo tiempo influir en el proceso de enseñanza-aprendizaje de los estudiantes de la carrera de matemática.

La guía ofrece dos módulos, cada uno de los cuales consta de definiciones, proposiciones, teoremas y ejemplos, siempre considerando los aspectos más relevantes de cada estructura.

En el primer módulo se estudia la teoría de grupos, propiedades de la estructura y sus derivaciones, considerando homomorfismos e isomorfismos entre grupos. En el segundo módulo presentamos la estructura de anillos, propiedades y aspectos relevantes para concluir con el tema de campo de fracciones.

En cada sección se presenta un preámbulo en el cual se identifican los temas a tratar y la estructura de la sección.

Módulo I

Teoría de Grupos

Grupos

La teoría de grupos es importante debido a sus múltiples aplicaciones en varias ramas del conocimiento. Un ejemplo que podemos entender gracias a esta teoría son las distintas combinaciones de movimientos que pueden realizarse para armar un cubo de Rubik.
Este módulo proporciona a los lectores nociones elementales sobre la teoría de grupos; se presenta definiciones, proposiciones, teoremas y ejemplos.

Propósito

Al finalizar este módulo el estudiante estará en capacidad de entender los conceptos asociados a la estructura de grupos y sus propiedades. Además, seguirá con rigor las proposiciones y teoremas que se estudian.

Contenido

1.1 Grupos y sus propiedades

Sea A un conjunto no vacío. Se llama operación $*$ definida en A, a toda función con dominio $A \times A$. Por ejemplo, si $A = \mathbb{N}$, la diferencia y la suma son operaciones definidas en $\mathbb{N}$.

El resultado de una operación definida en un conjunto A no siempre es un elemento de A. Por ejemplo, la diferencia de dos números naturales no siempre es un número natural. Cuando estudiamos la teoría de grupos nos interesa que las operaciones definidas en un conjunto cualquiera A, generen un elemento del conjunto A.

Definición 1.1 (Ley de composición interna)
Sea A un conjunto no vacío. Se llama ley de composición interna u operación cerrada definida en A, a toda función $*$ con dominio $A \times A$, cuyo rango es el conjunto A.

$$* : A \times A \to A$$

Ejemplos.

1. Si consideramos al conjunto A como el conjunto de los números enteros $\mathbb{Z}$, la suma $+$ es una ley de composición interna, ya que la suma de dos números enteros es un número entero.

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

2. Si consideramos al conjunto A como el conjunto de los números reales $\mathbb{R}$, el producto $*$ es una ley de composición interna, ya que el producto de dos números reales es un número real.

$$* : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$$

Notación. Sea A un conjunto no vacío. Una operación definida en A será denotada por $*$. En particular, escribimos $a * b$ para indicar el resultado de operar los elementos $a, b \in A$.

Definición 1.2

Sea A un conjunto no vacío, y sea $*$ una operación definida en A, se dice que la operación $*$ es:

1. cerrada en A, si $a * b \in A$ para todo $a, b \in A$,
2. conmutativa en A, si $a * b = b * a$ para todo $a, b \in A$,
3. asociativa en A, si $(a * b) * c = a * (b * c)$ para todo $a, b, c \in A$.

Además, se dice que:

4. el elemento $e \in A$ es un elemento neutro , si $a * e = a$, y $e * a = a$ para todo $a \in A$.
5. el elemento $a' \in A$ es un elemento inverso de $a \in A$, si $a' * a = e$, y $a * a' = e$, donde e es el elemento neutro.

Ejemplos.

1. Consideremos la operación suma $+$ definida en el conjunto de los números enteros $\mathbb{Z}$. Para todo $a, b, c \in \mathbb{Z}$ se cumple que la suma es cerrada, pues la suma de dos números enteros es un entero. La suma de números enteros es conmutativa y asociativa. Además $e = 0$ es el elemento neutro de la suma en $\mathbb{Z}$ ya que para todo a, $a + 0 = a$ y $0 + a = a$. Adicionalmente, para todo elemento $a \in \mathbb{Z}$ existe su inverso $a' = -a \in \mathbb{Z}$ ya que $a + a' = a + (-a) = 0$ y $a' + a = (-a) + a = 0$.

2. Sea X un conjunto arbitrario y $\mathscr{P}(X)$ el conjunto de todos los subconjuntos de X. Si tomamos la operación unión $\cup$ definida en $\mathscr{P}(X)$, tenemos que para todo $A, B, C \in \mathscr{P}(X)$ se cumple que la operación es cerrada pues la unión de elementos de $\mathscr{P}(X)$ es un elemento de $\mathscr{P}(X)$, y también la unión es conmutativa y asociativa en $\mathscr{P}(X)$. Además el elemento neutro de la unión es el conjunto vacío, pues $A \cup \emptyset = A$ y $\emptyset \cup A = A$, Por otra parte, no para todo $A \in \mathscr{P}(X)$, existe un elemento $A' \in \mathscr{P}(X)$ tal que $A \cup A' = \emptyset$ y $A' \cup A = \emptyset$, el único elemento que satisface esta propiedad es el conjunto vacío.

Una estructura matemática está compuesta por un conjunto no vacío junto con una, o varias operaciones (y/o relaciones) definidas en ese conjunto. El nombre de la estructura depende de las propiedades que cumplan las operaciones (y/o relaciones).

Si $*_1, *_2, \ldots, *_n$ son operaciones definidas en A, y $\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_m$ son m-relaciones en A, la $(n+m+1)$-upla $(A; *_1, *_2, \ldots, *_n, \mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_m)$ denotará una estructura matemática. A continuación definiremos el concepto de estructura algebraica, que son el tipo de estructura matemática que se estudia en el presente trabajo.

Definición 1.3 (Estructura algebraica)
Sea A un conjunto no vacío, y sea $*$ una operación cerrada en A. El par $(A; *)$ es una estructura algebraica.

En general, si $*_1, *_2, \cdots, *_n$ son operaciones cerradas en A, entonces $(A; *_1, *_2, \cdots, *_n)$, es una estructura algebraica. A continuación analizaremos algunas estructuras del tipo $(A; *)$.

Definición 1.4 (Semigrupo)
Sea G un conjunto no vacío, y sea $*$ una operación definida en G. Se dice que la estructura $(G; *)$ es un semigrupo si la operación $*$ es cerrada y asociativa en G.

Ejemplos.

1. Sea $\mathbb{Z}_{>0}$ el conjunto de los enteros no negativos y la operación $+$. La estructura $(\mathbb{Z}_{>0}; +)$ es un semigrupo. En efecto, la operación $+$ es cerrada en $\mathbb{Z}_{>0}$, pues la suma de dos enteros no negativos es un entero no negativo. Además, la suma de enteros no negativos es asociativa, esta propiedad se hereda de la estructura $(\mathbb{Z}; +)$.

2. Sea $M_2(\mathbb{R})$ el conjunto de matrices cuadradas de orden 2 con entradas reales. La estructura $(M_2(\mathbb{R}); +)$, donde $+$ es la suma usual de matrices, es un semigrupo. En efecto, si A, B, C son elementos de $M_2(\mathbb{R})$, se tiene que

La suma es cerrada, ya que

$$A + B = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}$$

La suma es asociativa, ya que

$$\begin{aligned}
(A + B) + C &= \left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \right) + \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \\
&= \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix} + \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \\
&= \begin{pmatrix} (a_{11} + b_{11}) + c_{11} & (a_{12} + b_{12}) + c_{12} \\ (a_{21} + b_{21}) + c_{21} & (a_{22} + b_{22}) + c_{22} \end{pmatrix} \\
&= \begin{pmatrix} a_{11} + (b_{11} + c_{11}) & a_{12} + (b_{12} + c_{12}) \\ a_{21} + (b_{21} + c_{21}) & a_{22} + (b_{22} + c_{22}) \end{pmatrix} \\
&= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} + c_{11} & b_{12} + c_{12} \\ b_{21} + c_{21} & b_{22} + c_{22} \end{pmatrix} \\
&= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \left(\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} + \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \right) \\
&= A + (B + C)
\end{aligned}$$

Por lo tanto, la estructura $(M_2(\mathbb{R}); +)$ es un semigrupo.

Definición 1.5 (Monoide)

Sea G un conjunto no vacío, y sea $*$ una operación definida en G. Decimos que la estructura $(G; *)$ es un monoide, si es semigrupo y además existe un elemento neutro en G.

Ejemplos.

1. La estructura $(\mathbb{Z}_{>0}; +)$ no es un monoide ya que no existe en $\mathbb{Z}_{>0}$ un elemento neutro para la suma.

2. La estructura $(M_2(\mathbb{R}); +)$ es un monoide.Ya que para todo $A \in M_2(\mathbb{R})$ existe el elemento neutro en $E \in M_2(\mathbb{R})$ tal que $A + E = E + A = A$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = A$$

3. La estructura $(\mathbb{Z}; *)$ con $*$ la operación definida por $a * b = a + b - 1$, es un monoide. En efecto, la operación $*$ es cerrada en $\mathbb{Z}$, ya que la suma dos números enteros es un entero y la diferencia con el entero -1 es entero. Además la operación $*$ es asociativa, ya que para todo $a, b, c, \in \mathbb{Z}$, se tiene que

$$\begin{aligned} (a * b) * c &= (a + b - 1) * c \\ &= a + b - 1 + c - 1 \\ &= a + (b + c - 1) - 1 \\ &= a * (b + c - 1) \\ &= a * (b * c) \end{aligned}$$

   Adicionalmente, para todo $a \in \mathbb{Z}$

$$a * e = a \Rightarrow a + e - 1 = a \Rightarrow e - 1 = a - a \Rightarrow e = 1$$

   entonces, $a * 1 = a + 1 - 1 = a$ y $1 * a = 1 + a - 1 = a$. En este caso $e = 1$ es el elemento neutro.

   Por lo tanto, la estructura $(\mathbb{Z}; *)$ es un monoide.

Definición 1.6 (Grupo)
Sea G un conjunto no vacío y sea $*$ una operación definida en G, diremos que la estructura $(G; *)$ es un grupo si la operación $*$ es:

1. cerrada en G, si $a * b \in G$ para todo $a, b \in G$,

2. asociativa en G, si $(a * b) * c = a * (b * c)$ para todo $a, b, c \in G$,

Además se dice que la operación tiene:

3. elemento neutro, si existe $e \in G$ tal que $a * e = a$ y $e * a = a$ para todo $a \in G$.

4. elemento inverso, si para cada $a \in G$, existe $a' \in G$ tal que $a' * a = e$ y $a * a' = e$.

Además si G es un conjunto finito, el grupo se denomina grupo finito.

Ejemplos.

1. Sea $\mathbb{I}$ el conjunto de los números impares y la suma usual $+$, la estructura $(\mathbb{I}; +)$ no es un grupo. En efecto, sean $a, b \in \mathbb{I}$, se tiene que

   i. La suma no es cerrada, ya que

   $$a + b = 2n_1 + 1 + 2n_2 + 1 = 2\underbrace{(n_1 + n_2)}_{n} + 2 = 2n + 2 \notin \mathbb{I}$$

   Por lo tanto, la estructura $(\mathbb{I}; +)$ no es un grupo.

2. Sea $\mathbb{R}^2$ el conjunto de los pares ordenados y la suma $+$, la estructura $(\mathbb{R}^2; +)$ es un grupo. En efecto, dados $g_1 = (x_1, y_1),\ g_2 = (x_2,\ y_2)$ y $g_3 = (x_3, y_3)$ en $\mathbb{R}^2$, se tiene que

   i. La suma es cerrada, pues $g_1 + g_2 = (x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$, tomando $(x_1 + x_2, y_1 + y_2) \in \mathbb{R}^2$.

   ii. La suma es asociativa, ya que

   $$\begin{aligned}(g_1 + g_2) + g_3 &= [(x_1, y_1) + (x_2, y_2)] + (x_3, y_3) \\ &= ((x_1 + x_2), (y_1 + y_2)) + (x_3, y_3) \\ &= ((x_1 + x_2) + x_3, (y_1 + y_2) + y_3) \\ &= (x_1 + (x_2 + x_3), y_1 + (y_2 + y_3)) \qquad \text{(asociatividad en } \mathbb{R})\end{aligned}$$

$$= (x_1, y_1) + [(x_2 + x_3), (y_2 + y_3)]$$
$$= (x_1, y_1) + [(x_2, y_2) + (x_3, y_3)]$$
$$= g_1 + (g_2 + g_3)$$

iii. Existencia del elemento neutro. Veamos cómo sería el elemento neutro en $(\mathbb{R}^2; +)$, sea $e = (e_1, e_2) \in \mathbb{R}^2$ se tiene que

$$g_1 + e = g_1 \Leftrightarrow (x_1, y_1) + (e_1, e_2) = (x_1, y_1) \Leftrightarrow \begin{cases} x_1 + e_1 = x_1 \Leftrightarrow e_1 = 0 \\ y_1 + e_2 = y_1 \Leftrightarrow e_2 = 0 \end{cases}$$

luego, $e = (0, 0)$ es el elemento neutro, ya que

$$g_1 + e = (x_1, y_1) + (0, 0) = (x_1 + 0, y_1 + 0) = (x_1, y_1)$$
$$e + g_1 = (0, 0) + (x_1, y_1) = (0 + x_1, 0 + y_1) = (x_1, y_1)$$

iv. Existencia del inverso. Veamos cómo sería el inverso de un elemento cualquiera de $(\mathbb{R}^2; +)$, sea $g'_1 = (x'_1, y'_1) \in \mathbb{R}^2$, se tiene que

$$g_1 + g'_1 = e \Leftrightarrow (x_1, y_1) + (x'_1, y'_1) = (0, 0) \Leftrightarrow \begin{cases} x_1 + x'_1 = 0 \Leftrightarrow x'_1 = -x_1 \\ y_1 + y'_1 = 0 \Leftrightarrow y'_1 = -y_1 \end{cases}$$

luego, $g'_1 = (-x_1, -y_1)$ es elemento inverso, ya que

$$g_1 + g'_1 = (x_1, y_1) + (-x_1, -y_1) = (x_1 + (-x_1), y_1 + (-y_1)) = (0, 0)$$
$$g'_1 + g_1 = (-x_1, -y_1) + (x_1, y_1) = ((-x_1) + x_1, (-y_1) + y_1) = (0, 0)$$

Por lo tanto, la estructura $(\mathbb{R}^2; +)$ es un grupo.

3. Sea $\mathbb{C}$ el conjunto de los números complejos y la suma en $\mathbb{C}$, la estructura $(\mathbb{C}; +)$ es un grupo. En efecto, sean $u = a + ib,\ w = a_1 + ib_1,\ z = a_2 + ib_2 \in \mathbb{C}$ con $a, b \in \mathbb{R}$, se tiene que

   i. La suma es cerrada, ya que la suma de dos números complejos es un número complejo.

   ii. La suma es asociativa, ya que

$$(u + w) + z = (a + ib + a_1 + ib_1) + a_2 + ib_2$$

$$
\begin{aligned}
&= (a + a_1 + i(b + b_1)) + a_2 + ib_2 \\
&= (a + a_1) + a_2 + i((b + b_1) + b_2) \\
&= a + (a_1 + a_2) + i(b + (b_1 + b_2)) && \text{(asociatividad en } \mathbb{R}) \\
&= a + ib + (a_1 + a_2 + i(b_1 + b_2)) \\
&= a + ib + (a_1 + ib_1 + a_2 + ib_2) \\
&= u + (w + z)
\end{aligned}
$$

iii. Existencia del elemento neutro en $\mathbb{C}$, dado por $e = 0 + i0$ tal que

$$u + e = a + ib + 0 + i0 = 0 + i0 + a + ib = a + ib = u$$

iv. Existencia del inverso. Veamos cómo sería el inverso de un elemento cualquiera de $\mathbb{C}$, sea $u' \in \mathbb{C}$ se tiene que

$$u + u' = e \Rightarrow u + u' = 0 + i0 \Rightarrow a + ib + u' = 0 + i0 \Rightarrow u' = -a - ib$$

luego, $u' = -a - ib$ es el elemento inverso, ya que

$$u + u' = a + ib + (-a - ib) = (-a - ib) + a + ib = 0 + i0 = e$$

Por lo tanto, la estructura $(\mathbb{C}; +)$ es un grupo.

Definición 1.7 (Grupo abeliano)
Sea G un conjunto no vacío, y sea $*$ una operación definida en G, diremos que la estructura $(G; *)$ es un grupo abeliano, si la operación $*$ cumple con la propiedad conmutativa.

Ejemplos.

1. Ya mostramos previamente $(\mathbb{R}^2; +)$ es un grupo, y además para todo par de elementos $g_1, g_2 \in \mathbb{R}^2$ se tiene que

$$
\begin{aligned}
g_1 + g_2 &= (x_1, y_1) + (x_2, y_2) \\
&= (x_1 + x_2, y_1 + y_2) \\
&= (x_2 + x_1, y_2 + y_1) \\
&= (x_2, y_2) + (x_1, y_1) \\
&= g_2 + g_1
\end{aligned}
$$

Por lo tanto, $(\mathbb{R}^2; +)$ es un grupo abeliano.

2. Ya mostramos previamente $(\mathbb{C}; +)$ es un grupo, y además para todo par de elementos $u = a + ib, v = a_1 + ib_1 \in \mathbb{C}$ se tiene que

$$\begin{aligned} u + v &= a + ib + a_1 + ib_1 \\ &= a + a_1 + i(b + b_1) \\ &= a_1 + a + i(b_1 + b) \\ &= a_1 + a + ib_1 + ib \\ &= a_1 + ib_1 + a + ib \\ &= v + u \end{aligned}$$

Por lo tanto, $(\mathbb{C}; +)$ es un grupo abeliano.

3. Sea $\mathbb{R}$ el conjunto de los números reales y sea $\oplus$ la operación definida por $a \oplus b = \sqrt[3]{a^3 + b^3}$, la estructura $(\mathbb{R}; \oplus)$ es un grupo abeliano. En efecto, sean $a, b, c \in \mathbb{R}$, se tiene que

   i. La operación es cerrada, ya que dados dos elementos en $\mathbb{R}$ por definición $a \oplus b = \sqrt[3]{a^3 + b^3} \in \mathbb{R}$.

   ii. La operación $\oplus$ es asociativa, ya que

$$\begin{aligned} (a \oplus b) \oplus c &= \left(\sqrt[3]{a^3 + b^3}\right) \oplus c \\ &= \sqrt[3]{\left(\sqrt[3]{a^3 + b^3}\right)^3 + c^3} \\ &= \sqrt[3]{a^3 + (b^3 + c^3)} && \text{(la suma es asociativa)} \\ &= \sqrt[3]{a^3 + \left(\sqrt[3]{b^3 + c^3}\right)^3} \\ &= a \oplus \left(\sqrt[3]{b^3 + c^3}\right) \\ &= a \oplus (b \oplus c) \end{aligned}$$

   iii. Existe un elemento neutro en $\mathbb{R}$, dado por $e = 0$ tal que

$$a \oplus e = a \oplus 0 = \sqrt[3]{a^3 + 0^3} = \sqrt[3]{0^3 + a^3} = \sqrt[3]{a^3} = a$$

iv. Para cada elemento de $\mathbb{R}$, existe un elemento inverso que está en $\mathbb{R}$, dado por $a' = -a$ tal que

$$a * a' = a * (-a) = \sqrt[3]{a^3 + (-a^3)} = \sqrt[3]{(-a^3) + a^3} = \sqrt[3]{0} = 0$$

v. La operación $\oplus$ es conmutativa, ya que a^3 y b^3 son números reales y la suma en $\mathbb{R}$ es conmutativa, entonces

$$a \oplus b = \sqrt[3]{a^3 + b^3} = \sqrt[3]{b^3 + a^3} = b \oplus a$$

Por lo tanto, la estructura $(\mathbb{R}; \oplus)$ es un grupo abeliano.

En la siguiente tabla se presenta un resumen de la clasificación de estructuras algebraicas del tipo $(G; *)$, de acuerdo a las propiedades que se cumplen en la misma.

Estructura $(G; *)$	Operación cerrada	Asociativa	Neutro	Inverso	Conmutativa
Semigrupo	$\surd$	$\surd$			
Monoide	$\surd$	$\surd$	$\surd$		
Grupo	$\surd$	$\surd$	$\surd$	$\surd$	
Grupo abeliano	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$

Tabla 1.1: Estructuras algebraicas del tipo $(G; *)$

A continuación, estudiaremos algunas de las propiedades más relevantes sobre los grupos.

Proposición 1.1

Sea la estructura $(G; *)$ un grupo.

1. Ley cancelación derecha: si $a * c = b * c$, entonces $a = b, \ \forall\, a, b, c \in G$.
2. Ley cancelación izquierda: si $c * a = c * b$, entonces $a = b, \ \forall\, a, b, c \in G$.
3. El elemento neutro del grupo es único.
4. El elemento inverso de $a \in G$ es único.

Demostración.

1. Si $a * c = b * c$, entonces

$$\begin{aligned} (a * c) * c' &= (b * c) * c' \\ a * (c * c') &= b * (c * c') && \text{(asociatividad en } G) \\ a * e &= b * e && (c * c' = e) \\ a &= b \end{aligned}$$

2. Si $c * a = c * b$, entonces

$$\begin{aligned} c' * (c * a) &= c' * (c * b) \\ (c' * c) * a &= (c' * c) * b && \text{(asociatividad en } G) \\ e * a &= e * b && (c' * c = e) \\ a &= b \end{aligned}$$

3. Para demostrar que el neutro del grupo es único, suponemos que e, e_1 son elementos neutros, entonces

$$\begin{aligned} e &= e * e_1 && (e_1 \text{ es neutro}) \\ &= e_1 && (e \text{ es neutro}) \end{aligned}$$

   luego, como $e = e_1$ llegamos a una contradicción, por lo tanto el neutro es único.

4. Para demostrar que el inverso es único, suponemos que a', a'' son inversos de $a \in (G; *)$, entonces

$$\begin{aligned} a' &= a' * e && (\text{ya que } e \text{ es neutro}) \\ &= a' * (a * a'') && (\text{ya que } a * a'' = e) \\ &= (a' * a) * a'' && (\text{asociatividad en } G) \\ &= e * a'' && (\text{ya que } a' * a = e) \\ &= a'' \end{aligned}$$

   luego, como $a' = a''$ llegamos a una contradicción, por lo tanto el inverso de a es único. □

Proposición 1.2

Sea la estructura $(G;*)$ un grupo, para todo $a,b \in G$ se satisfacen las siguientes propiedades.

1. $(a')' = a$
2. $(a*b)' = b'*a'$
3. $a^n * a^m = a^{n+m}$
4. $(a^n)^m = a^{nm}$

Demostración.

1. Ya que $(a')'$ es el inverso de a', entonces

$$\begin{aligned} a'*(a')' &= e \\ a*a'*(a')' &= a*e && (a*a' = e) \\ e*(a')' &= a*e && (e*a = a) \\ (a')' &= a \end{aligned}$$

2. Para probar la propiedad, basta mostrar que $(a*b)*(b'*a') = e$

$$\begin{aligned} (a*b)*(b'*a') &= a*(b*b')*a' && (\text{asociatividad en } G) \\ &= (a*e)*a' && (b*b' = e) \\ &= a*a' \\ &= e \end{aligned}$$

3. Veamos que,

$$\begin{aligned} a^n * a^m &= \underbrace{(a*a*a*\ldots*a)}_{n-veces} * \underbrace{(a*a*a*\ldots*a)}_{m-veces} \\ &= \underbrace{(a*a*a*\ldots*a)}_{n+m-veces} \\ &= a^{n+m} \end{aligned}$$

4. Veamos que,

$$\begin{aligned}(a^n)^m &= \underbrace{(a^n * a^n * a^n * \ldots * a^n)}_{m-veces} \\ &= a^{\underbrace{n+n+n+\ldots+n}_{m-veces}} \\ &= a^{nm}\end{aligned}$$

□

Es importante hacer mención a ciertas notaciones usadas en la teoría de grupos, las cuales son la notación aditiva y multiplicativa.

En algunas referencias bibliográficas, si la operación $*$ es la suma $+$, a la estructura $(G;+)$ se le llama grupo aditivo y en lugar de la notación $a * b$ se usa $a + b$ que se lee "la suma de a y b", el neutro es denotado por el símbolo 0 y el inverso de algún elemento se denota por $-a$.

Si la operación $*$ es el producto $\cdot$, a la estructura $(G;\cdot)$ se le llama grupo multiplicativo y en lugar de la notación $a * b$ se usa ab o $a \cdot b$ que se lee "el producto de a y b", el neutro es denotado por el símbolo 1 y el inverso de algún elemento se denota por a^{-1} ver ([Ga17], [Ju12], [Cl84], [La05], [Do96]).

A continuación, estudiaremos los subgrupos de un grupo dado, la caracterización de un subgrupo y ejemplos.

1.2 Subgrupos

En ocasiones es importante conocer si un determinado subconjunto de G goza de las mismas propiedades del grupo $(G;*)$. En esta sección estaremos analizando este tipo de subestructuras que fortalecen al grupo al brindar propiedades adicionales. Algunos subgrupos, como los subgrupos normales, que se estudiarán más adelante, han resultado de mucha utilidad inclusive para el estudio del grupo correspondiente.

Definición 1.8 (Subgrupo)

Sea $(G,*)$ un grupo, y sea H un subconjunto no vacío de G. Se dice que H es un subgrupo de G, si $(H;*)$ es un grupo con la operación definida en G.

Notación. Si $(H;*)$ es un subgrupo de $(G;*)$ escribiremos $H \leqslant G$ y si no lo es escribiremos $H \nleqslant G$.

Ejemplo. Sea la estructura $(\mathbb{Z},+)$ un grupo y sea $H = \{2n : n \in \mathbb{Z}\}$, entonces H es un subgrupo de $\mathbb{Z}$. En efecto, sean $a,\ b,\ c \in H$, se tiene que

i. La suma es cerrada, ya que la suma de números pares es par.

ii. La suma es asociativa, ya que esta propiedad se hereda de $(\mathbb{Z};+)$.

iii. Existe el elemento neutro en H dado por $e = 0 \in H$, tal que $a + e = a$.

iv. Para cada elemento de H, existe un elemento inverso que está en H, dado por $a' = -2n_1$ tal que $a + a' = 2n_1 + (-2n_1) = 0$

Por lo tanto, la estructura $(H;+)$ es un grupo y en consecuencia $H \leqslant \mathbb{Z}$.

Notación. De aquí en adelante siempre que estudiemos subgrupos escribiremos "la estructura G es un grupo", en lugar de "la estructura $(G,*)$ es un grupo". Además escribiremos a^{-1} en lugar de a' para denotar el inverso de un elemento.

Teorema 1.1 (Caracterización de subgrupos)
Sea la estructura G un grupo, decimos que H es un subgrupo de G, si y sólo si, para todo $x, y \in H$ se cumple que $xy^{-1} \in H$.

Demostración.

$\Rightarrow$) Suponemos que H es un subgrupo de G, entonces mostremos que $xy^{-1} \in H$. Si H es un subgrupo de G, entonces la estructura $(H;*)$ es un grupo, luego la $*$ operación es cerrada, y para todo elemento de H, existe su inverso en H, tomemos $x, y \in H$, entonces existe $y^{-1} \in H$, y en consecuencia $xy^{-1} \in H$.

$\Leftarrow$) Suponemos que $xy^{-1} \in H$, entonces mostremos que H es un subgrupo de G. Veamos que la estructura $(H;*)$ es un grupo. En efecto, ya que la operación $*$ es asociativa en G, entonces la operación $*$ es asociativa en H. Nos falta mostrar que en H existe el elemento neutro, inverso y que la operación $*$ es cerrada. Como H

es un subconjunto no vacío, tomemos un elemento $a \in H$, si consideramos $x = a$ e $y = a$, de la hipótesis sigue que $xy^{-1} = aa^{-1} = e \in H$. Para ver que $x^{-1} \in H$, consideremos $x = e$ e $y = a$, de la hipótesis sigue que $xy^{-1} = ea^{-1} = a^{-1} \in H$. Finalmente mostremos que la $*$ operación es cerrada en H, como ya mostramos que el inverso existe, tomemos $b^{-1} \in H$, y consideremos $x = a$ y $y = b^{-1}$, de la hipótesis sigue que, $xy^{-1} = a(b^{-1})^{-1} = ab \in H$. Por lo tanto, la estructura $(H; *)$ es un grupo, y en consecuencia $H \leqslant G$. □

Ejemplo. Sea la estructura $(\mathbb{Z}; +)$ es un grupo, y sea $H = \{2n : n \in \mathbb{Z}\}$, entonces H es un subgrupo de $\mathbb{Z}$. En efecto, sean $x, y \in H$, veamos que $x + y^{-1} \in H$, consideremos $x = 2n_1, y = 2n_2 \in H$, entonces

$$x + y^{-1} = 2n_1 + (-2n_2) = 2(n_1 - n_2) = 2n \in H \qquad (n = n_1 - n_2 \in \mathbb{Z})$$

Por lo tanto, $H \leqslant \mathbb{Z}$.

A continuación, estudiaremos algunos de los grupos y subgrupos de interés, dentro de los cuáles están los grupos de congruencia, los grupos de permutaciones, los grupos cíclicos, el subgrupo normal y el grupo cociente.

1.3 Grupo de congruencia módulo m

El concepto de congruencia es utilizado ampliamente en la Teoría de Números y permite caracterizar propiedades de números y de estructuras algebraicas en forma sencilla. Estudiaremos en esta sección, cómo una relación de congruencia determina una partición sobre el conjunto en donde está definida. Debido a su importancia, analizaremos la relación congruencia módulo m, que particiona al conjunto de números enteros $\mathbb{Z}$ en un conjunto finito de clases de equivalencia.

Definición 1.9 (Congruencia módulo m)
Sean a, b dos números enteros cualesquiera, y sea m un entero positivo fijo, decimos que a es congruente con b módulo m si $a - b = km$, para algún $k \in \mathbb{Z}$.

Si existe k entero tal que $a - b = km$, entonces se dice que $m \mid a - b$, y se lee m

divide a $(a-b)$. En este caso, decimos que a es congruente con b módulo m, lo cual denotaremos como $a \equiv b(\text{mód } m)$.

Ejemplos.

1. Si $m = 6$, se tiene que 25 es congruente a $7(\text{mód } 6)$, ya que 6 divide a $25 - 7 = 18$. Podemos escribir entonces $25 \equiv 7(\text{mód } 6)$.

2. Si $m = 8$, se tiene que 46 es congruente a $6(\text{mód } 8)$, ya que 8 divide a $46 - 6 = 40$. Podemos escribir entonces $46 \equiv 6(\text{mód } 8)$.

Proposición 1.3
La relación congruencia módulo m, es una relación de equivalencia en $\mathbb{Z}$.

Demostración. La relación congruencia módulo m, es reflexiva, simétrica y transitiva. En efecto, sean $a, b, c \in \mathbb{Z}$.

Reflexividad. Veamos que $a \equiv a(\text{mód } m)$, ya que $a - a = 0 = (0)m$, existe $k = 0$ tal que $a - a = km$, por lo tanto $a \equiv a(\text{mód } m)$.

Simetría. Si $a \equiv b(\text{mód } m)$, entonces $b \equiv a(\text{mód } m)$. Si $a \equiv b(\text{mód } m)$, se tiene que $a - b = km$ para algún $k \in \mathbb{Z}$. Y multiplicando esta última expresión por -1 se tiene que $b - a = -km$ donde $-k \in \mathbb{Z}$, por lo tanto $b \equiv a(\text{mód } m)$.

Transitividad. Si $a \equiv b(\text{mód } m)$ y $b \equiv c(\text{mód } m)$, entonces $a \equiv c(\text{mód } m)$.

Si $a \equiv b(\text{mód } m)$ y $b \equiv c(\text{mód } m)$, existen $k_1, k_2 \in \mathbb{Z}$, tales que $a - b = k_1 m$ y $b - c = k_2 m$. Sumando estas últimas expresiones se tiene que $a - c = (k_1 + k_2)m$. Tomando $k = k_1 + k_2 \in \mathbb{Z}$ se tiene que $a - c = km$. Por lo tanto, $a \equiv c(\text{mód } m)$.

□

Una vez que la relación congruencia módulo m es una relación de equivalencia, ésta define una partición del conjunto $\mathbb{Z}$ en subconjuntos llamados clases de equivalencia.

Definición 1.10 (Clase de equivalencia)
Sea m un entero positivo fijo, y sea $a \in \mathbb{Z}$. Se llama clase de equivalencia determinada por el elemento a al conjunto de enteros que son congruentes a $a(\text{mód } m)$ y se denota

$$[a] := \{x \in \mathbb{Z} : x \equiv a(\text{ mód } m)\}$$

Este conjunto $[a]$ se llama clase residual de a, ya que representa al conjunto de todos los números enteros que al dividirlos por m dejan un resto o residuo igual a a. Por lo tanto, habrá tantas clases de equivalencia como posibles restos de dividir por m. El conjunto cociente de $\mathbb{Z}$ determinado por la relación congruencia módulo m, se le conoce como conjunto cociente y se denota con $\mathbb{Z}/m$.

Definición 1.11 (Conjunto cociente)
Sea m un entero positivo arbitrario, pero fijo. Se define el conjunto cociente de la congruencia módulo m, al conjunto formado por todas las clases residuales, $\mathbb{Z}/m = \{[a] : [a] \text{ una clase residual}\}$

Para m entero positivo fijo, el conjunto cociente de los enteros módulo m es, $\mathbb{Z}/m = \{[0],\ [1], \ldots, [m-1]\}$, donde $[0],\ [1], \ldots, [m-a]$ son las clases residuales.

Ejemplo. Sea $m = 3$, el conjunto cociente es $\mathbb{Z}/3 = \{[0], [1], [2]\}$, donde

$$[0] = \{x \in \mathbb{Z} : x \equiv 0(\text{ mód } 3)\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$
$$[1] = \{x \in \mathbb{Z} : x \equiv 1(\text{ mód } 3)\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$$
$$[2] = \{x \in \mathbb{Z} : x \equiv 2(\text{ mód } 3)\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$$

En este ejemplo se puede observar que la clase residual del $[0]$, es el conjunto formado por todos los enteros que dejan residuo 0 al dividirse por 3, la clase residual del $[1]$ es el conjunto formado por todos los enteros que dejan residuo 1 al dividirse por 3 y la clase residual del $[2]$ es el conjunto formado por todos los enteros que dejan residuo 2 al dividirse por 3.

Es claro que $[0] \cup [1] \cup [2] = \mathbb{Z}$, y que $[0] \cap [1] = \varnothing,\ [0] \cap [2] = \varnothing,\ [1] \cap [2] = \varnothing$, lo que significa que $\mathbb{Z}/3$ representa una partición de $\mathbb{Z}$.

En general el conjunto $\mathbb{Z}/m$ contiene $[m-1]$ clases residuales, las cuales son conjuntos disjuntos cuya unión es $\mathbb{Z}$, es decir, el conjunto cociente $\mathbb{Z}/m$ es una partición de $\mathbb{Z}$.

Proposición 1.4

Sean $[a], [b] \in \mathbb{Z}/m$, si $[a] = [b]$ entonces $a \equiv b (\text{mód } m)$

Demostración. Si $[a] = [b]$, se tiene que $x \in [a]$ y $x \in [b]$ para todo $x \in \mathbb{Z}$, ya que $x \in [a]$ y $x \in [b]$ existen $k_1, k_2 \in \mathbb{Z}$ tal que $x - a = k_1 m$ y $x - b = k_2 m$, restando estas dos últimas expresiones se tiene que $x - b - x + a = (k_2 - k_1)m$. Tomando $k = k_2 - k_1 \in \mathbb{Z}$ se tiene que $a - b = km$, por lo tanto $a \equiv b (\text{mód } m)$. □

Definición 1.12 (Operaciones en $\mathbb{Z}/m$)

Sean $[a], [b]$ clases residuales de $\mathbb{Z}/m$ se define:

1. suma de clases: $[a] + [b] := [a + b]$
2. producto de clases: $[a] \cdot [b] := [ab]$

Proposición 1.5

Sean $[a], [b] \in \mathbb{Z}/m$, si $[a] = [a']$ y $[b] = [b']$. Se cumple que:

1. $[a + b] = [a' + b']$
2. $[ab] = [a'b']$

Demostración.

1. Si $[a] = [a']$ y $[b] = [b']$, entonces $a \equiv a' (\text{mód } m)$, implica $a - a' = k_1 m$ para algún $k_1 \in \mathbb{Z}$, análogamente se tiene que $b - b' = k_2 m$ para algún $k_2 \in \mathbb{Z}$, sumando estas últimas expresiones se tiene que $(a + b) - (a' + b') = (k_1 + k_2)m$. Tomando $k = k_1 + k_2 \in \mathbb{Z}$ se tiene que $(a + b) - (a' + b') = km$, de modo que $(a + b) \equiv (a' + b') (\text{mód } m)$, por lo tanto $[a + b] = [a' + b']$.

2. Si $[a] = [a']$ y $[b] = [b']$, entonces $a \equiv a' (\text{mód } m)$, implica $a - a' = k_1 m$ multiplicando por b' a ambos lados de la igualdad se tiene $b'a - b'a' = b'k_1 m$ para algún $k_1 \in \mathbb{Z}$, análogamente se tiene que $b - b' = k_2 m$ multiplicando por a a ambos lados de la igualdad se tiene $ab - ab' = ak_2 m$ para algún $k_2 \in \mathbb{Z}$. Sumando ambas expresiones se tiene, $b'a - b'a' + ab - ab' = b'k_1 m + ak_2 m$, luego $ab - a'b' = (b'k_1 + ak_2)m$. Tomando $k = b'k_1 + ak_2 \in \mathbb{Z}$ se tiene que $ab - a'b' = km$, de modo que $ab \equiv a'b' (\text{mód } m)$, por lo tanto $[ab] = [a'b']$. □

Definición 1.13

Sea m un entero positivo arbitrario, pero fijo. El conjunto $(\mathbb{Z}/m)^*$ se define como: $(\mathbb{Z}/m)^* = \{[a] : a \text{ y } m \text{ coprimos}\}$

Ejemplos.

1. Si $m = 8$, el conjunto $\mathbb{Z}/8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$, entonces el conjunto $(\mathbb{Z}/8)^* = \{[1], [3], [5], [7]\}$, ya que $\text{mcd}(1,8) = \text{mcd}(3,8) = \text{mcd}(5,8) = \text{mcd}(7,8) = 1$.

2. Si $m = 12$, el conjunto $\mathbb{Z}/12 = \{[0], [1], [2], [3], [4], \ldots, [11]\}$, entonces el conjunto $(\mathbb{Z}/12)^* = \{[1], [5], [7], [11]\}$, ya que $\text{mcd}(1,12) = \text{mcd}(5,12) = \text{mcd}(7,12) = \text{mcd}(11,12) = 1$.

Proposición 1.6

1. El par $(\mathbb{Z}/m; +)$, es un grupo con la operación $+$ suma de clases.

2. El par $((\mathbb{Z}/m)^*; \cdot)$, es un grupo con la operación $\cdot$ producto de clases.

Demostración.

1. La estructura $(\mathbb{Z}/m; +)$, es un grupo. En efecto, sean $[a], [b], [c] \in \mathbb{Z}/m$, se tiene que

   i. La suma es cerrada, ya que la suma de clases residuales es una clase residual.

ii. La suma es asociativa, ya que

$$\begin{aligned}([a]+[b])+[c] &= [a+b]+[c] \\ &= [(a+b)+c] \\ &= [a+(b+c)] && \text{(asociatividad en } \mathbb{Z}) \\ &= [a]+[b+c] \\ &= [a]+([b]+[c])\end{aligned}$$

iii. Existe un elemento neutro en $\mathbb{Z}/m$. En efecto, la clase $[0]$ es tal que $[a] + [0] = [a]$. Luego la clase $[0]$ es el elemento neutro de $\mathbb{Z}/m$.

iv. Para cada elemento de $\mathbb{Z}/m$ existe un elemento inverso que está en $\mathbb{Z}/m$, pues cada clase de $[a] \in \mathbb{Z}/m$ existe la clase $[m-a]$ tal que $[a]+[m-a] = [m] = [0]$.

Por lo tanto, la estructura $(\mathbb{Z}/m; +)$ es un grupo. Además $(\mathbb{Z}/m; +)$ es un grupo abeliano ya que $[a]+[b] = [a+b] = [b+a] = [b]+[a]$.

2. La estructura $((\mathbb{Z}/m)^*; \cdot)$, es un grupo. En efecto, sean $[a], [b], [c] \in (\mathbb{Z}/m)^*$, se tiene que

i. El producto es cerrado, ya que el producto de clases residuales es una clase residual.

ii. El producto es asociativo, ya que

$$([a][b])[c] = [ab][c] = [(ab)c] = [a(bc)] = [a][bc] = [a]([b][c])$$

iii. Existe un elemento neutro en $(\mathbb{Z}/m)^*$. En efecto, la clase $[1]$ es tal que $[a][1] = [a]$. Luego la clase $[1]$ es el elemento neutro de $(\mathbb{Z}/m)^*$.

iv. Para cada elemento de $(\mathbb{Z}/m)^*$ existe un elemento inverso que está en $(\mathbb{Z}/m)^*$. En efecto, cada clase de $[a] \in (\mathbb{Z}/m)^*$ tiene inverso multiplicativo si y sólo si $\text{mcd}(a, m) = 1$.

Por lo tanto, la estructura $((\mathbb{Z}/m)^*; \cdot)$ es un grupo. Además $((\mathbb{Z}/m)^*; \cdot)$ es un grupo abeliano. □

Considerando que $\mathbb{Z}/m$ y $(\mathbb{Z}/m)^*$ son conjuntos finitos, los grupos $(\mathbb{Z}/m;+)$ y $((\mathbb{Z}/m)^*;\cdot)$ son ejemplos de grupos finitos.

Nótese que la estructura $(\mathbb{Z}/m;\cdot)$ no es un grupo, ya que no para todo $[a] \in \mathbb{Z}/m$ existe su inverso en $\mathbb{Z}/m$. Por ejemplo en $(\mathbb{Z}/5;\cdot)$ no existe el elemento inverso de $[0] \in \mathbb{Z}/5$. También es claro que la estructura $((\mathbb{Z}/m)^*;+)$ no es un grupo, ya que $[0] \notin (\mathbb{Z}/m)^*$.

Notación. A partir de ahora el conjunto $\mathbb{Z}/m = \{[0],[1],\ldots,[m-1]\}$ lo denotaremos por $\mathbb{Z}/m = \{0,1,\ldots,m-1\}$, dando por entendido que $0,1,\ldots,m-1$ son clases residuales.

Definición 1.14 (Orden de un grupo)
Sea la estructura $(G;*)$ un grupo. Se llama orden del grupo $(G;*)$ a la cardinalidad del conjunto G, y se denota como $|G|$.

Ejemplos.

1. Sea $((\mathbb{Z}/12)^*;\cdot)$ un grupo, ya que el conjunto $(\mathbb{Z}/12)^* = \{1,5,7,11\}$ entonces la cardinalidad del conjunto $|(\mathbb{Z}/12)^*| = 4$, luego el orden del grupo $((\mathbb{Z}/12)^*;\cdot)$ es 4.

2. Sea $(\mathbb{Z}/6;+)$ un grupo, ya que el conjunto $\mathbb{Z}/6 = \{0,1,2,3,4,5\}$ entonces la cardinalidad del conjunto $|\mathbb{Z}/6| = 6$, luego el orden del grupo $(\mathbb{Z}/6;+)$ es 6.

Definición 1.15 (Orden de un elemento)
Sea la estructura $(G,*)$ un grupo, se llama orden de un elemento $a \in G$ al entero positivo más pequeño n tal que $a^n = e$. El orden del elemento a se denota como $|a|$.

Una primera idea para encontrar el orden de un elemento $a \in G$, es calcular $a, a^2, a^3, \cdots, a^n$, hasta obtener el elemento neutro del grupo por primera vez. Si no existe entero positivo n tal que $a^n = e$, decimos que el orden a es infinito.

Ejemplos.

1. Consideremos el conjunto, $\mathbb{Z}/8 = \{0,1,2,3,4,5,6,7\}$ y la $+$ operación suma definida en $\mathbb{Z}/8$, la estructura $(\mathbb{Z}/8;+)$ es un grupo. Por lo tanto, $|\mathbb{Z}/8| = 8$, lo cual nos dice que el orden del grupo $(\mathbb{Z}/8;+)$ es 8. Y si queremos saber el orden del elemento $6 \in \mathbb{Z}/8$, se procede de la siguiente manera:

$$6^1 = 6 \neq 0$$
$$6^2 = 6+6 = 12 \mid 8 = 4 \neq 0$$
$$6^3 = 6+6+6 = 18 \mid 8 = 2 \neq 0$$
$$6^4 = 6+6+6+6 = 24 \mid 8 = 0 = e$$

   Ya que $6^4 = e$, entonces el orden del elemento 6 en el grupo $(\mathbb{Z}/8;+)$ es 4, de manera análoga se puede encontrar el orden para los demás elementos del grupo.

2. Sea $\mathbb{R}$ el conjunto de los números reales y la operación producto, la estructura $(\mathbb{R};\cdot)$ es un grupo, como $|\mathbb{R}| = \infty$, entonces orden del grupo $(\mathbb{R};\cdot)$ es infinito y si quisiéramos encontrar el orden del elemento $5 \in \mathbb{R}$, no es posible, pues

$$5^1 = 5, \quad 5^2 = 25, \quad 5^3 = 125, \quad 5^4 = 625, \quad \ldots$$

   va a crecer hasta un valor cada vez más grande y nunca se va a llegar a encontrar el elemento neutro del grupo $(\mathbb{R};\cdot)$, por lo tanto el orden del elemento 5 en el grupo $(\mathbb{R};\cdot)$ es infinito.

1.4 Grupo de permutaciones

Uno de los grupos más importantes en el álgebra abstracta es el grupo de permutaciones, que estudiaremos en esta sección. Debido a su utilidad en el estudio de las simetrías de figuras geométricas, muchos autores se han abocado a analizar y describir todas las potencialidades de este grupo. Iniciamos el estudio de estos grupos con la noción de permutación, sus representaciones y las características de la operación composición que se define entre ellas.

Definición 1.16 (Permutación)
Se llama permutación del conjunto S a toda función biyectiva $\sigma : S \to S$.

Notación. Denotaremos como S_n al conjunto de todas las permutaciones de un conjunto finito S.

Una primera representación de una permutación $\sigma \in S_n$, está dada de forma matricial

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

Ejemplos.

1. Sea $S = \{1,2,3,4,5\}$, y sea la $\sigma : S \to S$, dada por $\sigma(1) = 3, \sigma(2) = 4$, $\sigma(3) = 1, \sigma(4) = 5, \sigma(5) = 2$, la forma matricial de la permutación es

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$$

2. Sea $S = \{1,2,3,4,5,6,7,8\}$, y sea la $\tau : S \to S$, dada por $\tau(1) = 7, \tau(2) = 4$, $\tau(3) = 5, \tau(4) = 6, \tau(5) = 3, \tau(6) = 2, \tau(7) = 1, \tau(8) = 8$, la forma matricial de la permutación es

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 4 & 5 & 6 & 3 & 2 & 1 & 8 \end{pmatrix}$$

3. Sea $S = \{1,2,3,4,5,6\}$, y sea la $\mu : S \to S$, dada por $\mu(1) = 5, \mu(2) = 4$, $\mu(3) = 2, \mu(4) = 1, \mu(5) = 6, \mu(6) = 3$, la forma matricial de la permutación es

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 2 & 1 & 6 & 3 \end{pmatrix}$$

Proposición 1.7

Sean $\sigma, \tau \in S_n$, entonces la composición $\sigma \circ \tau \in S_n$.

Demostración. Sean $\sigma, \tau \in S_n$, se tiene que σ y τ son funciones biyectivas de S_n en S_n, del análisis matemático se conoce que la composición de funciones biyectivas es biyectiva, por lo tanto $\sigma \circ \tau \in S_n$. □

De la proposición anterior, se concluye que la composición de permutaciones, es una permutación. Además denotaremos por $\sigma\tau$ en lugar de $\sigma \circ \tau$.

Ejemplo. Sean $\sigma, \tau \in S_5$, dadas por

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \qquad \text{y} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$$

entonces,

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \sigma(\tau(3)) & \sigma(\tau(4)) & \sigma(\tau(5)) \end{pmatrix}$$

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \sigma(3) & \sigma(4) & \sigma(5) & \sigma(1) & \sigma(2) \end{pmatrix}$$

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 2 & 3 \end{pmatrix}$$

La composición $\sigma\tau$, podemos interpretar como que; τ cambia 1 por 3 y σ cambia 3 por 1, por lo tanto en $\sigma\tau$, 1 es fijo; τ cambia 2 por 4 y σ cambia 4 por 5, por lo tanto $\sigma\tau$, cambia 2 por 5; τ cambia 3 por 5 y σ cambia 5 por 4, por lo tanto $\sigma\tau$, cambia 3 por 4, etc.

En general, la composición de permutaciones la podemos escribir como:

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

Si queremos hallar el inverso de una permutación $\sigma^{-1} \in S_n$, lo único que tenemos que hacer es voltear las dos filas de la permutación, y calcular $\sigma(1), \dots, \sigma(n)$.

Ejemplo. Sea $\sigma \in S_4$, dado por $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$

$$\sigma^{-1} = \begin{pmatrix} 4 & 3 & 1 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

La siguiente definición proporciona, una segunda representación de una permutación dada.

Definición 1.17 (Representación cíclica)
Sea S un conjunto no vacío, y sea $\sigma \in S_n$, dada la expresión de la forma $(a_1, a_2, \ldots, a_k) \in S$, tales que $\sigma(a_1) = a_2, \sigma(a_2) = a_3, \ldots, \sigma(a_k) = a_1$, se denomina ciclo.

En la definición anterior k representa la longitud del ciclo y es llamado k-ciclo. Además todo elemento fijo $a \in S$, escribimos $\sigma(a) = a$ que en la representación cíclica no hará falta escribirla, asumiendo que ese elemento es fijo en la permutación.

Ejemplos.

1. Sea $\sigma \in S_5$, dado por:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix} = (1,2,4,3,5) \qquad \text{(Representación cíclica)}$$

   es un ciclo de longitud 5.

2. Sea $\tau \in S_6$, dado por:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix} = (1,2)(3,4,6) \qquad \text{(Representación cíclica)}$$

   tenemos, $(1,2)$ ciclo de longitud 2, $(3,4,6)$ ciclo de longitud 3.

Cuando el contexto es claro siempre que $n < 10$, escribiremos los ciclos de S_n sin uso de las comas, ya que es la manera más común de representar los ciclos.

Ejemplo. Sea $\sigma \in S_5$, dado por:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix} = (12435) \qquad \text{(Representación cíclica)}$$

Cuando leemos una permutación en representación cíclica, lo que se hace es asignar cada elemento al de su derecha, excepto el elemento que está en el último, a éste se le asigna el primer elemento. El ejemplo anterior (12435) se interpreta como: 1 va al 2, 2 va al 4, 4 va al 3, 3 va al 5 y 5 va al 1.

Definición 1.18 (Orden de una permutación)
El orden de un ciclo con k movimientos es igual a k. En general el orden de una permutación σ es el mínimo común múltiplo (mcm) de las longitudes de los ciclos que componen a σ.

Ejemplos.

1. Sea $\sigma = (15)(247)(63)$. El orden de σ es 6. En efecto, ya que
   Tenemos (15), (63) que son ciclos de longitud 2 y (247) es un ciclo de longitud 3, de modo que $\text{mcm}(2,3) = 6$, por lo tanto $|\sigma| = 6$.

2. Sea $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 4 & 5 & 2 & 3 & 1 \end{pmatrix}$. El orden de τ es 10. En efecto, ya que $\tau = (17)(26345)$, se tiene que (17) es un ciclo de longitud 2 y (26345) es un ciclo de longitud 5, de modo que $\text{mcm}(2,5) = 10$, por lo tanto $|\tau| = 10$.

Ya que los ciclos son una manera particular de representar las permutaciones, entonces ahora veamos cómo se opera la composición de ciclos, recordando que operamos de derecha a izquierda.

Ejemplo. Sean $\sigma, \tau \in S_6$, dados por $\sigma = (12)(346)(5)$ y $\tau = (2315)(46)$, calculemos $\sigma\tau$.

$$\sigma\tau = \underbrace{(12)}_{\sigma_3}\underbrace{(346)}_{\sigma_2}\underbrace{(5)}_{\sigma_1}\underbrace{(2315)}_{\tau_2}\underbrace{(46)}_{\tau_1}$$

$$
\begin{aligned}
1 \xrightarrow{\tau_1} 1 \xrightarrow{\tau_2} 5 \xrightarrow{\sigma_1} 5 \xrightarrow{\sigma_2} 5 \xrightarrow{\sigma_3} 5 \qquad & \text{(inicia ciclo)} \\
5 \xrightarrow{\tau_1} 5 \xrightarrow{\tau_2} 2 \xrightarrow{\sigma_1} 2 \xrightarrow{\sigma_2} 2 \xrightarrow{\sigma_3} 1 \qquad & \text{(fin ciclo)} \\
2 \xrightarrow{\tau_1} 2 \xrightarrow{\tau_2} 3 \xrightarrow{\sigma_1} 3 \xrightarrow{\sigma_2} 4 \xrightarrow{\sigma_3} 4 \qquad & \text{(inicia ciclo)} \\
4 \xrightarrow{\tau_1} 6 \xrightarrow{\tau_2} 6 \xrightarrow{\sigma_1} 6 \xrightarrow{\sigma_2} 3 \xrightarrow{\sigma_3} 3 \qquad & \text{(continua ciclo)} \\
3 \xrightarrow{\tau_1} 3 \xrightarrow{\tau_2} 1 \xrightarrow{\sigma_1} 1 \xrightarrow{\sigma_2} 1 \xrightarrow{\sigma_3} 2 \qquad & \text{(fin ciclo)} \\
6 \xrightarrow{\tau_1} 4 \xrightarrow{\tau_2} 4 \xrightarrow{\sigma_1} 4 \xrightarrow{\sigma_2} 6 \xrightarrow{\sigma_3} 6 \qquad & \text{(6 es fijo)}
\end{aligned}
$$

Por lo tanto, la composición $\sigma\tau = (15)(243)(6)$.

Proposición 1.8

Sea $\mathrm{Sym}(S)$ el conjunto de todas permutación de S en S, y sea la operación composición $\circ$ definida en $\mathrm{Sym}(S)$. La estructura $(\mathrm{Sym}(S); \circ)$ es un grupo.

Demostración. Sean $\sigma, \tau, \mu \in \mathrm{Sym}(S)$, se tiene que

i. La operación $\circ$ es cerrada, ya que la composición funciones biyectivas es biyectiva.

ii. La operación $\circ$ es asociativa, ya que

$$(\sigma \circ \tau) \circ \mu(x) = (\sigma \circ \tau)\mu(x) = \sigma(\tau(\mu(x))) = \sigma(\tau \circ \mu(x)) = \sigma \circ (\tau \circ \mu)(x)$$

iii. Existe un elemento neutro, en este caso con la función identidad de $I = \sigma(I) \in \mathrm{Sym}(S)$, se satisface

$$\sigma \circ I(x) = \sigma(I(x)) = \sigma$$

iv. Para cada elemento de $\mathrm{Sym}(S)$, existe el inverso en $\mathrm{Sym}(S)$. En efecto, ya que sea $\sigma \in \mathrm{Sym}(S)$, se tiene que σ es una función biyectiva, ya que σ es biyectiva, existe su inverso σ^{-1} en $\mathrm{Sym}(S)$ tal que $\sigma \circ \sigma^{-1} = I$ y $\sigma^{-1} \circ \sigma = I$.

Por lo tanto, la estructura $(\mathrm{Sym}(S); \circ)$ es un grupo. □

El grupo $(\mathrm{Sym}(S); \circ)$ se llama **grupo de permutaciones**, además es un grupo no abeliano, ya que la composición de funciones es no conmutativa.

Cuando consideramos S_n el conjunto finito de todas las permutaciones del conjunto S de n elementos. La estructura $(S_n; \circ)$ se llama **grupo simétrico de n elementos**.

Proposición 1.9
La cardinalidad del conjunto de permutaciones S_n es igual a $n!$

Demostración. Por inducción

1. Para $n = 1$, el número de elementos de S_1 es igual a 1.
2. Para $n = k$, asumimos que el número de permutaciones de S_k elementos es $k!$.
3. Supongamos que $n = k + 1$ y mostremos que el número de elementos de S_{k+1} es justamente $(k + 1)!$.

   Como el elemento $k + 1$ puede ordenarse de $k + 1$ posiciones, existe aún k elementos que deben ser ordenados, por la hipótesis inductiva el número formas distintas de ordenar dichos elementos es $k!$. Por lo tanto, el número de formas de ordenar todos los $k + 1$ elementos es $(k + 1)k! = (k + 1)!$ □

Ejemplo. La estructura $(S_3; \circ)$ es un grupo. En efecto, ya que $|S_3| = 3! = 6$.

$$S_3 = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

i. La operación es cerrada.

ii. La composición de permutaciones es asociativa, ya que

$$(\sigma_i \circ \sigma_j) \circ \sigma_k = \sigma_i \circ (\sigma_j \circ \sigma_k)$$

iii. En este caso el elemento neutro en S_3, denotado por $I = \sigma_1$ satisface que: $\sigma_i \circ I = \sigma_i$ con $i = 1, \ldots, 6$, por ejemplo

$$\sigma_5\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

iv. Para cada $\sigma_i \in S_3$, existe su inverso en S_3, tal que: $\sigma_i \circ {\sigma_i}^{-1} = I$ y ${\sigma_i}^{-1} \circ \sigma_i = I$, por ejemplo

$$\sigma_5{\sigma_5}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Por lo tanto, la estructura $(S_3; \circ)$ es el grupo simétrico de 6 elementos.

1.5 Grupos cíclicos

En esta sección estudiaremos un tipo de grupos llamados grupos cíclicos y también sus subgrupos. Estos grupos juegan un papel importante en la clasificación de grupos abelianos y en la teoría de codificación o generación de códigos. Estableceremos el concepto de elemento generador de un grupo, y las propiedades de esta estructura.

Definición 1.19 (Grupo cíclico)
La estructura $(G; *)$ se dice que es un grupo cíclico, cuando existe $a \in G$ tal que $G = \{a^k : k \in \mathbb{Z}\}$.

Notación. Escribiremos $\langle a \rangle$ para denotar el conjunto $G = \{a^k : k \in \mathbb{Z}\}$.

La definición anterior nos dice que si $(G; *)$ es un grupo cíclico, entonces todo elemento de G puede ser expresado como una potencia de a y se dice entonces que a es generador de G, además en un grupo cíclico puede haber más de un elemento generador.

Definición 1.20 (Subgrupo cíclico)

Sea la estructura G un grupo y sea $a \in G$, el subconjunto $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ es un subgrupo de G y se llama subgrupo cíclico generado por a.

Ejemplos.

1. La estructura $(\mathbb{Z}; +)$ es un grupo cíclico. En efecto, ya que los elementos 1 y -1 son generadores del grupo.

2. En el grupo $(\mathbb{Z}/6; +)$, el elemento $2 \in \mathbb{Z}/6$ forma el subgrupo cíclico $\langle 2 \rangle = \{0, 2, 4\}$.

$$2^0 = 0$$
$$2^1 = 2 \mid 6 = 0(6) + 2$$
$$2^2 = 4 \mid 6 = 0(6) + 4$$

   Además $(\mathbb{Z}/6; +)$ es un grupo cíclico, ya que existe el elemento $5 \in \mathbb{Z}/6$ tal que $\langle 5 \rangle = \mathbb{Z}/6$.

$$5^0 = 0 \qquad 5^3 = 15 \mid 6 = 2(6) + 3$$
$$5^1 = 5 \mid 6 = 0(6) + 5 \qquad 5^4 = 20 \mid 6 = 3(6) + 2$$
$$5^2 = 10 \mid 6 = 1(6) + 4 \qquad 5^5 = 25 \mid 6 = 4(6) + 1$$

3. La estructura $((\mathbb{Z}/9)^*; \cdot)$ es un grupo cíclico. En efecto, ya que existe el elemento $2 \in (\mathbb{Z}/9)^*$, tal que $\langle 2 \rangle = (\mathbb{Z}/9)^*$.

$$2^0 = 1 \qquad 2^3 = 8 \mid 9 = 0(9) + 8$$
$$2^1 = 2 \mid 9 = 0(9) + 2 \qquad 2^4 = 16 \mid 9 = 1(9) + 7$$
$$2^2 = 4 \mid 9 = 0(9) + 4 \qquad 2^5 = 32 \mid 9 = 3(9) + 5$$

   Además en el grupo cíclico $((\mathbb{Z}/9)^*; \cdot)$, se tiene los subgrupos cíclicos

   i. Subgrupos triviales: $\langle 1 \rangle = \{1\}; \langle 2 \rangle = \langle 5 \rangle = (\mathbb{Z}/9)^*$

   ii. $H_1 = \langle 4 \rangle = \langle 7 \rangle = \{1, 4, 7\}$

   iii. $H_2 = \langle 8 \rangle = \{1, 8\}$

Teorema 1.2
Todo grupo cíclico es un grupo abeliano

Demostración. Si $(G;*)$ es cíclico, entonces existe $a \in G$ tal que $G = \langle a \rangle$. Ya que G es no vacío, tomemos $x, y \in G$ de modo que x, y pueden escribirse como potencias de a, de modo que $x = a^n$ e $y = a^m$ tales que

$$xy = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = yx$$

Por lo tanto, $(G;*)$ es un grupo abeliano. □

Definición 1.21 (Orden del grupo cíclico)
Sea la estructura $(G;*)$ un grupo. Para cualquier elemento $a \in G$ se cumple que $|a| = |\langle a \rangle|$.

Ejemplo. Sea $(\mathbb{Z}/4;+)$ un grupo cíclico el orden del elemento $3 \in \mathbb{Z}/4$ es $|\langle 3 \rangle| = 4$. En efecto, ya que el orden de $|3| = 4$.

$$3^1 = 3 = 3 \mid 4 = 3 \neq 0$$
$$3^2 = 3+3 = 6 \mid 4 = 2 \neq 0$$
$$3^3 = 3+3+3 = 9 \mid 4 = 1 \neq 0$$
$$3^4 = 3+3+3+3 = 12 \mid 4 = 0 = e$$

1.6 Clases laterales y Teorema de Lagrange

Otras clases de congruencias útiles son aquellas que se generan mediante la relación entre subgrupos de un grupo, las cuáles son llamadas clases laterales o cosets (por su denominación en inglés). Estas clases resultan útiles en el estudio combinatorio de grupos finitos, o en el conteo del número de subgrupos de un grupo finito. En esta sección desarrollamos este concepto para luego usarlo en la demostración del Teorema de Lagrange sobre la relación entre la cardinalidad de un grupo y la cardinalidad de alguno de sus subgrupos.

Definición 1.22 (Relación de congruencia módulo H)
Sea G un grupo y sea H un subgrupo de G, se define:

1. La relación de congruencia izquierda módulo H como: $a \equiv_i b (\text{mód } H)$ si y sólo si $a^{-1}b \in H$.
2. La relación de congruencia derecha módulo H como: $a \equiv_d b (\text{mód } H)$ si y sólo si $ab^{-1} \in H$.

Proposición 1.10

1. La relación $a \equiv_i b (\text{mód } H)$ es una relación de equivalencia.
2. La relación $a \equiv_d b (\text{mód } H)$ es una relación de equivalencia.

Demostración.

1. La relación $a \equiv_i b (\text{mód } H)$, es reflexiva, simétrica y transitiva. En efecto,

   Reflexividad. Para todo $a \in G$ se cumple que $a^{-1}a \in H$ ya que H es un subgrupo. Por lo tanto, $a \equiv_i a (\text{mód } H)$.

   Simetría. Sean $a, b \in G$, supongamos que $a \equiv_i b (\text{mód } H)$, entonces $a^{-1}b \in H$ por las propiedades de grupo se tiene que $(a^{-1}b)^{-1} = b^{-1}a \in H$. Por lo tanto, $b \equiv_i a (\text{mód } H)$.

Transitividad. Sean $a, b, c \in G$, supongamos que $a \equiv_i b (\text{mód } H)$ y que $b \equiv_i c (\text{mód } H)$, entonces $a^{-1}b \in H$ y $b^{-1}c \in H$. Y ya que H es un subgrupo, se tiene que $(a^{-1}b)(b^{-1}c) = a^{-1}(bb^{-1})c = a^{-1}c \in H$. Por lo tanto, $a \equiv_i c (\text{mód } H)$.

2. Análogamente se demuestra que la relación $a \equiv_d b (\text{mód } H)$ es una relación de equivalencia. □

Ya que que las relaciones de la proposición anterior son relaciones de equivalencia, éstas particionan al conjunto G en clases de equivalencia.

Veamos ahora como son las clases de equivalencia que generan estas relaciones.

Dado algún $a \in G$, la clase de equivalencia de a determinada por la relación de congruencia izquierda módulo H, es el siguiente conjunto

$$\begin{aligned}
[a] &= \{x \in G : a \equiv_i x (\text{ mód } H)\} \\
&= \{x \in G : a^{-1}x\} \\
&= \{x \in G : \text{ sea } h = a^{-1}x \text{ con } h \in H\} \\
&= \{x \in G : ah = (aa^{-1})x \text{ con } h \in H\} \\
&= \{x \in G : ah = x \text{ con } h \in H\} \\
&= aH
\end{aligned}$$

Es decir, el conjunto de las clases de equivalencia de a, es el conjunto de todos los elementos de la forma ah para algún $h \in H$.

Dado algún $a \in G$, la clase de equivalencia de a determinada por la relación de congruencia derecha módulo H, es el siguiente conjunto

$$\begin{aligned}
[a] &= \{x \in G : x \equiv_d a (\text{ mód } H)\} \\
&= \{x \in G : xa^{-1}\} \\
&= \{x \in G : \text{ sea } h = xa^{-1} \text{ con } h \in H\} \\
&= \{x \in G : ha = x(a^{-1}a) \text{ con } h \in H\} \\
&= \{x \in G : ha = x \text{ con } h \in H\} \\
&= Ha
\end{aligned}$$

Es decir, el conjunto de las clases de equivalencia de a, es el conjunto de todos los elementos de la forma ha para algún $h \in H$.

Definición 1.23 (Clases laterales)
Sea G un grupo, y sea H un subgrupo de G. Para todo $a \in G$, se tiene

1. Clase lateral izquierda de H con representante a al conjunto:
   $aH = \{ah : \text{ con } h \in H\}$

2. Clase lateral derecha de H con representante a al conjunto:
   $Ha = \{ha : \text{ con } h \in H\}$

Cuando tratamos con un grupo aditivo las clases laterales quedan dadas por:

1. Clase lateral izquierda de H: $a + H = \{a + h : \text{ con } h \in H\}$

2. Clase lateral derecha de H: $H + a = \{h + a : \text{ con } h \in H\}$

Proposición 1.11
Sea la estructura G un grupo y sea H un subgrupo de G, dado algún $a \in G$, se cumple que $aH = H$ sí y sólo si $a \in H$.

Demostración.

$\Rightarrow$) Supongamos que $aH = H$, entonces $a \in H$. Si $a, e \in aH$, entonces $a = ea \in aH$, por hipótesis $aH \subseteq H$ por lo tanto $a \in H$.

$\Leftarrow$) Supongamos que $a \in H$, entonces $aH = H$. Primero mostremos que $aH \subseteq H$, es decir, si $h \in aH$, entonces $h \in H$ como H es un subgrupo sigue que $ha^{-1} \in H$. Ahora mostremos que $H \subseteq aH$, es decir, si $h \in H$ entonces $h \in aH$, como H es un subgrupo existen $h \in H$ tal que $a^{-1}h \in H$, ya que que h puede escribirse como $h = eh = (aa^{-1})h = a(a^{-1}h)$, por lo tanto $h \in aH$. □

Ejemplos.

1. Sea $(\mathbb{Z}/6;+)$ un grupo y $H=\{0,3\}$ un subgrupo de $\mathbb{Z}/6$. Las clases laterales izquierdas son:

$$0+H=\begin{cases}0+0\\0+3\end{cases}=\{0,3\}, \qquad 3+H=\begin{cases}3+0\\3+3\end{cases}=\{3,0\}$$
$$1+H=\begin{cases}1+0\\1+3\end{cases}=\{1,4\}, \qquad 4+H=\begin{cases}4+0\\4+3\end{cases}=\{4,1\}$$
$$2+H=\begin{cases}2+0\\2+3\end{cases}=\{2,5\}, \qquad 5+H=\begin{cases}5+0\\5+3\end{cases}=\{5,2\}$$

   Por lo tanto, las clases laterales izquierdas son los conjuntos: $0+H, 1+H$ y $2+H$. Además, en este ejemplo las clases laterales izquierdas coinciden con las clases laterales derechas ya que el grupo es abeliano.

2. Sea el grupo simétrico $(S_3;\circ)$ y sea $H=\{\sigma_1,\sigma_2\}$ un subgrupo de S_3. Hallemos las clases laterales izquierdas

$$\sigma_1 H=\begin{cases}\sigma_1\sigma_1=\sigma_1\\\sigma_1\sigma_2=\sigma_2\end{cases}=\{\sigma_1,\sigma_2\}, \qquad \sigma_2 H=\begin{cases}\sigma_2\sigma_1=\sigma_2\\\sigma_2\sigma_2=\sigma_1\end{cases}=\{\sigma_2,\sigma_1\}$$
$$\sigma_3 H=\begin{cases}\sigma_3\sigma_1=\sigma_3\\\sigma_3\sigma_2=\sigma_6\end{cases}=\{\sigma_3,\sigma_6\}, \qquad \sigma_6 H=\begin{cases}\sigma_6\sigma_1=\sigma_6\\\sigma_6\sigma_2=\sigma_3\end{cases}=\{\sigma_6,\sigma_3\}$$
$$\sigma_4 H=\begin{cases}\sigma_4\sigma_1=\sigma_4\\\sigma_4\sigma_2=\sigma_5\end{cases}=\{\sigma_4,\sigma_5\}, \qquad \sigma_5 H=\begin{cases}\sigma_5\sigma_1=\sigma_5\\\sigma_5\sigma_2=\sigma_4\end{cases}=\{\sigma_5,\sigma_4\}$$

   Por lo tanto, las clases laterales izquierdas son: $\sigma_1 H, \sigma_3 H$ y $\sigma_4 H$.

Hallemos las clases laterales derechas

$$H\sigma_1 = \begin{cases} \sigma_1\sigma_1 = \sigma_1 \\ \sigma_2\sigma_1 = \sigma_2 \end{cases} = \{\sigma_1, \sigma_2\}, \qquad H\sigma_2 = \begin{cases} \sigma_1\sigma_2 = \sigma_2 \\ \sigma_2\sigma_2 = \sigma_1 \end{cases} = \{\sigma_1, \sigma_2\}$$

$$H\sigma_3 = \begin{cases} \sigma_1\sigma_3 = \sigma_3 \\ \sigma_2\sigma_3 = \sigma_5 \end{cases} = \{\sigma_3, \sigma_5\}, \qquad H\sigma_5 = \begin{cases} \sigma_1\sigma_5 = \sigma_5 \\ \sigma_2\sigma_5 = \sigma_3 \end{cases} = \{\sigma_5, \sigma_3\}$$

$$H\sigma_4 = \begin{cases} \sigma_1\sigma_4 = \sigma_4 \\ \sigma_2\sigma_4 = \sigma_6 \end{cases} = \{\sigma_4, \sigma_6\}, \qquad H\sigma_6 = \begin{cases} \sigma_1\sigma_6 = \sigma_6 \\ \sigma_2\sigma_6 = \sigma_4 \end{cases} = \{\sigma_6, \sigma_4\}$$

Por lo tanto, las clases laterales derechas son: $H\sigma_1, H\sigma_3$ y $H\sigma_4$.

En este ejemplo se evidencia que las clases laterales izquierdas y derechas son distintas. En general se tiene que $aH \neq Ha$.

Proposición 1.12

Sea la estructura G un grupo, H un subgrupo de G y sean las funciones

1. $\phi : H \to aH$ definida por $\phi(h) = ah$,
2. $\phi' : H \to Ha$ definida por $\phi'(h) = ha$.

   Entonces ϕ y ϕ' son biyectivas.

Demostración.

1. Veamos que ϕ es biyectiva.

   Inyectiva. Para todo $h_1, h_2 \in H$, suponemos que $\phi(h_1) = \phi(h_2)$, entonces $ah_1 = ah_2$, por la ley de cancelación izquierda se tiene que $h_1 = h_2$.

   Sobreyectiva. Todos los elementos de aH tienen la forma ah para $h \in H$, es decir, si $ah \in H$ existe $h \in H$ tal que $\phi(h) = ah$. Por lo tanto, ϕ es biyectiva, y en consecuencia $|H| = |aH|$.

2. Análogamente se demuestra que ϕ' es biyectiva. □

De la proposición anterior se concluye que el conjunto de las clases laterales izquierdas o derechas, tienen el mismo número de elementos (cardinalidad).

Teorema 1.3 (Teorema de Lagrange)
Sea la estructura G un grupo finito y sea H un subgrupo de G. Entonces el orden de H divide al orden de G, es decir, $|H| \mid |G|$.

Para la demostración de este teorema consideramos el conjunto de las clases laterales izquierdas aH.

Demostración.

Supongamos que $n = |H|$ es el orden de H y consideremos el conjunto aH. Por hipótesis, G es un grupo finito entonces el conjunto de las clases laterales de aH es finito, ahora suponemos que k es el número de clases laterales de aH, entonces $aH = \{a_1H, a_2H, \ldots, a_kH\}$, luego por la proposición 1.12 se tiene que $|H| = |a_kH|$.

Ya que que las clases laterales aH forman una partición de G, entonces los elementos de G son disjuntos dos a dos y la unión de todos los elementos es G, es decir, $G = a_1H \cup a_2H \cup, \ldots, \cup\, a_kH$, ahora suponemos que $m = |G|$ es el orden de G, entonces

$$m = |a_1H| + |a_2H| + \ldots + |a_kH| \quad = \sum_{i=1}^{k} |a_iH| = \sum_{i=1}^{k} |H| \quad = \sum_{i=1}^{k} n = kn$$

Por lo tanto, $m = kn$ de modo que $n \mid m$ y en consecuencia $|H| \mid |G|$. □

Definición 1.24 (Índice de H en G)
Sea la estructura G un grupo y sea H un subgrupo de G. Se llama índice de H en G al número de clases laterales izquierdas o derechas, y se denota como $[G : H]$.

Ejemplos.

1. Sea $(\mathbb{Z}/6; +)$ un grupo y $H = \{0, 3\}$ como $H \leqslant \mathbb{Z}/6$. Las clases laterales izquierdas son los conjuntos: $0 + H, 1 + H$ y $2 + H$, por lo tanto $[\mathbb{Z}/6 : H] = 3$.

2. Sea el grupo simétrico S_3 y sea $H = \{\sigma_1, \sigma_5, \sigma_6\}$ como $H \leqslant S_3$. Las clases laterales izquierdas son los conjuntos: $\sigma_1 H = \sigma_5 H = \sigma_6 H = \{\sigma_1, \sigma_5, \sigma_6\}$ y $\sigma_2 H = \sigma_3 H = \sigma_4 H = \{\sigma_2, \sigma_3, \sigma_4\}$, por lo tanto $[S_3 : H] = 2$.

1.7 Subgrupo normal y Grupo cociente

Cuando H es un subgrupo de G no podemos asegurar que las clases laterales aH y Ha sean iguales, pero si esto sucede H sería un subgrupo normal, lo cual resulta de interés ya que permite la construcción de una clase de grupos llamados grupos cociente. En esta sección estudiaremos estas dos estructuras y sus propiedades.

Definición 1.25 (Subgrupo normal)
Sea G un grupo y sea H un subgrupo de G. H se llama subgrupo normal de G si las clases laterales son iguales $aH = Ha$.

Notación. Escribiremos $H \triangleleft G$ para indicar que H es un subgrupo normal de G y si no lo es escribiremos $H \not\triangleleft G$.

Ejemplos.

1. Sea $(\mathbb{Z}/6; +)$ un grupo y $H = \{0, 3\}$ un subgrupo de $\mathbb{Z}/6$, entonces

   Las clases laterales izquierdas de H son: $a + H = \{0 + H, 1 + H, 2 + H\}$

$$0 + H = 3 + H = \{0, 3\}$$
$$1 + H = 4 + H = \{1, 4\}$$
$$2 + H = 5 + H = \{2, 5\}$$

   Las clases laterales derechas de H son: $H + a = \{H + 0, H + 1, H + 2\}$

$$H + 0 = H + 3 = \{0, 3\}$$
$$H + 1 = H + 4 = \{1, 4\}$$
$$H + 2 = H + 5 = \{2, 5\}$$

   Por lo tanto, $a + H = H + a$ y en consecuencia $H \triangleleft G$.

2. Sea el grupo simétrico $(S_3; \circ)$ y $H = \{\sigma_1, \sigma_2\}$ un subgrupo de S_3, entonces

   Las clases laterales izquierdas de H son los conjuntos: $aH = \{\sigma_1 H, \sigma_3 H, \sigma_4 H\}$.

$$\sigma_1 H = \sigma_2 H = \{\sigma_1, \sigma_2\}$$
$$\sigma_3 H = \sigma_6 H = \{\sigma_3, \sigma_6\}$$
$$\sigma_4 H = \sigma_5 H = \{\sigma_4, \sigma_5\}$$

   Las clases laterales derechas de H son los conjuntos: $Ha = \{H\sigma_1, H\sigma_3, H\sigma_4\}$.

$$H\sigma_1 = H\sigma_2 = \{\sigma_1, \sigma_2\}$$
$$H\sigma_3 = H\sigma_5 = \{\sigma_3, \sigma_5\}$$
$$H\sigma_4 = H\sigma_6 = \{\sigma_4, \sigma_6\}$$

   Por lo tanto, $aH \neq Ha$ y en consecuencia $H \not\lhd G$.

Proposición 1.13

Sea G un grupo y sea H un subgrupo de G, las siguientes afirmaciones son equivalentes:

a. para todo $a \in G$, $aH = Ha$,

b. para todo $a \in G$, $aHa^{-1} = H$

c. para todo $a \in G$, $aHa^{-1} \subseteq H$.

Demostración.

Veamos que: a $\rightarrow$ b

Suponemos que para todo $a \in G$, $aH = H$, entonces $aHa^{-1} = H$.

Se tiene que mostrar una doble contención, es decir, $aHa^{-1} \subseteq H$ y $H \subseteq aHa^{-1}$.

Sea $aha^{-1} \subseteq aHa^{-1}$ con $h \in H$, por hipótesis $aH = Ha$, entonces $ah \in aH = Ha$ luego $ah = h_1 a$ con $h_1 \in H$, multiplicando a la derecha por el inverso de a se tiene que $h_1 = aha^{-1} \in H$.

Sea $h \in H$, por hipótesis $aH = Ha$ entonces $ha \in Ha = aH$ luego $ha = ah_1$ con $h_1 \in H$, multiplicando a la derecha por el inverso de a se tiene que $h = aha^{-1} \in aHa^{-1}$.

Por lo tanto, $aHa^{-1} = H$.

Veamos que: b $\rightarrow$ c

Suponemos que para todo $a \in G$, $aHa^{-1} = H$, entonces $aHa^{-1} \subseteq H$.

Es inmediato, ya que por hipótesis $aHa^{-1} = H$, es decir, se cumple la doble contención en particular se cumple $aHa^{-1} \subseteq H$.

Veamos que: c $\rightarrow$ a

Suponemos que para todo $a \in G$, $aHa^{-1} \subseteq H$, entonces $aH = Ha$.

Se tiene que mostrar una doble contención, es decir, $aH \subseteq Ha$ y $Ha \subseteq aH$.

Sea $ah \in aH$ con $h \in H$, por hipótesis $aHa^{-1} \subseteq H$, entonces $aha^{-1} \in aHa^{-1}$, si $aha^{-1} = h_1$ multiplicando a la derecha por a se tiene que $ah = h_1a \in Ha$.
Sea $ha \in Ha$ con $h \in H$, por hipótesis $aHa^{-1} \subseteq H$, si $a = a^{-1}$ se tiene que $a^{-1}Ha \subseteq H$, entonces $a^{-1}ha \in H$ consideremos $a^{-1}ha = h_1$ multiplicando a la izquierda por a se tiene que $ha = ah_1 \in aH$.

Por lo tanto, $aH = Ha$. □

La proposición que acabamos de demostrar nos dice que tenemos 3 maneras distintas de argumentar que un subgrupo es normal en G. Siendo la afirmación **c** la más usual cuando se estudia los subgrupos normales. Es decir, un subgrupo H es normal en G si para todo $a \in G$ se cumple que $aHa^{-1} \subseteq H$.

Proposición 1.14

Si G es un grupo abeliano, entonces todos los subgrupos H de G son normales.

Demostración. Sea $H \leqslant G$, dado $a \in G$ veamos que $aHa^{-1} \subseteq H$.
Consideremos $aha^{-1} \in aHa^{-1}$ con $h \in H$, ya que G es un grupo abeliano, se tiene que $aha^{-1} = (aa^{-1})h = eh = h \in H$. □

Ejemplos.

1. Sea el grupo aditivo $\mathbb{Z}$ y sea $H = n\mathbb{Z}$ el subgrupo de los enteros múltiplos de $\mathbb{Z}$, entonces $H \triangleleft \mathbb{Z}$. En efecto, pues

   Sea $a \in \mathbb{Z}$, como $\mathbb{Z}$ es un grupo aditivo se tiene $a + H + a^{-1} \subseteq H$. Consideremos $a + h + a^{-1} \in a + H + a^{-1}$ con $h \in H$, ya que que el grupo aditivo $\mathbb{Z}$ es abeliano, se tiene que $a + h + a^{-1} = (a + a^{-1}) + h = h \in H$

2. Sea H y K dos subgrupos normales, entonces $H \cap K$ es un subgrupo normal en G. En efecto, pues

   Sea $a \in G$, entonces $a(H \cap K)a^{-1} \subseteq H \cap K$. Sea $h \in H \cap K$, entonces $h \in H$ y $h \in K$ puesto que H y K son subgrupos normales, entonces $aha^{-1} \in H$ y $aha^{-1} \in K$, por tanto $aha^{-1} \in H \cap K$.

Notación. Escribiremos G/H para denotar el conjunto cociente de todas las clases laterales izquierdas o derechas determinadas por un subgrupo normal H.

Definición 1.26
Sea G un grupo y sea H un subgrupo normal de G. Se define la operación $\otimes$ en las clases laterales izquierdas como: $aH \otimes bH := abH$.

Proposición 1.15
Sea G un grupo y H un subgrupo normal de G. Para todo $a, b, a', b' \in G$, si $aH = a'H$ y $bH = b'H$ entonces $abH = a'b'H$.

Demostración. Ya que estamos en el conjunto las clases laterales izquierdas, consideremos la relación de congruencia izquierda módulo H y veamos que la operación $\otimes$ está bien definida.

Ya que $aH = a'H$ y $bH = b'H$ se tiene que $a \equiv_i a' (\text{mód } H)$ y $b \equiv_i b' (\text{mód } H)$, entonces $ab \equiv_i a'b' (\text{mód } H)$.
Como $a \equiv_i a' (\text{mód } H)$ y $b \equiv_i b' (\text{mód } H)$, entonces $a^{-1}a' \in H$ y $b^{-1}b' \in H$, debemos demostrar que $(ab)^{-1}(a'b') \in H$.

Se sabe que $(ab)^{-1}(a'b') = b^{-1}(a^{-1}a')b'$ y por hipótesis $a^{-1}a' \in H$ entonces $(a^{-1}a')b' \in Ha$, pero $aH = Ha$ puesto que $H \triangleleft G$, $(a^{-1}a')b' = b'h$ con $h \in H$, luego $(ab)^{-1}(a'b') = b^{-1}(a^{-1}a')b' = b^{-1}b'h$ y como $b^{-1}b' \in H$ se tiene que $(ab)^{-1}(a'b') = b^{-1}b'h \in H$.
Por lo tanto, $ab \equiv_i a'b' (\text{mód } H)$. □

Proposición 1.16

Sea H un subgrupo normal de G y sea la operación $\otimes$ definida en G/H de la siguiente manera $aH \otimes bH := abH$. Entonces, $(G/H; \otimes)$ es un grupo.

Demostración. Sean $aH, bH, cH \in G/H$, se tiene que

i. La operación $\otimes$ es cerrada, ya que $aH \otimes bH = abH$

ii. La operación $\otimes$ es asociativa, ya que

$$\begin{aligned}(aH \otimes bH) \otimes cH &= (abH) \otimes cH \\ &= (ab)cH \\ &= a(bc)H \\ &= aH \otimes (bcH) \\ &= aH \otimes (bH \otimes cH)\end{aligned}$$

iii. Existe el elemento neutro dado por $H = eH \in G/H$ donde $e \in G$, tal que

$$aH \otimes eH = aeH = aH$$

iv. Existe el elemento inverso dado por $(aH)^{-1} = a^{-1}H \in G/H$, tal que

$$aH \otimes a^{-1}H = aa^{-1}H = eH = H$$

Por lo tanto, la estructura $(G/H; \otimes)$ es grupo. □

El grupo $(G/H; \otimes)$ que acabamos de probar, se llama **grupo cociente** o **grupo factor**.

Ejemplo. Sea $G = \mathbb{Z}/9$ un grupo y $H = \{0,3,6\}$ un subgrupo de G. La estructura $(G/H;\otimes)$ es un grupo cociente. En efecto,
Lo primero que debemos ver es que H es un subgrupo normal en G, pero esto se cumple puesto G es un grupo abeliano, por lo tanto $H \triangleleft G$.
Ahora determinemos los elementos de G/H, para ello encontramos las clases laterales izquierdas, las cuales son:

$$0+H=\{0,3,6\}, \quad 1+H=\{1,4,7\}, \quad \text{y} \quad 2+H=\{2,5,8\}$$

Luego $G/H=\{0+H,1+H,2+H\}$, ahora veamos que el conjunto G/H junto con la operación $\otimes$ es un grupo. En efecto, sean $0+H,1+H,2+H \in G/H$ se tiene que:

i. La operación $\otimes$ es cerrada, pues

$$0+H\otimes 1+H=0+1+H=1+H\in G/H$$

ii. La operación $\otimes$ es asociativa, ya que

$$\begin{aligned}(0+H\otimes 1+H)\otimes 2+H &= (0+1+H)\otimes 2+H\\ &= (0+1)+2+H\\ &= 0+(1+2)+H\\ &= 0+H\otimes(1+2+H)\\ &= 0+H\otimes(1+H\otimes 2+H)\end{aligned}$$

iii. Existe el elemento neutro dado por $H=0+H$, tal que

$$a+H\otimes 0+H=a+0+H=a+H$$

iv. Existe el elemento inverso dado por $(a+H)^{-1}=-a+H$, tal que

$$a+H\otimes -a+H=a+(-a)+H=0+H$$

Por lo tanto, $(G/H;\otimes)$ es un grupo cociente.

Proposición 1.17

Sea la estructura G un grupo y $H \triangleleft G$, si G es un grupo abeliano, entonces el grupo cociente es abeliano.

Demostración. Sean $aH, bH \in G/H$, entonces $aH \otimes bH = abH$, puesto que G es un grupo abeliano entonces $ab = ba$, se tiene que

$$aH \otimes bH = abH = baH = bH \otimes aH$$

□

1.8 Homomorfismos entre grupos y Teorema de Cayley

Dos grupos estarán relacionados estructuralmente si existe un homomorfismo entre ellos, y esta relación es más fuerte si existiera un isomorfismo; en ambos casos resultará de utilidad en el estudio de estos grupos, y en esencia brindará una forma alterna de operar los elementos de ambos grupos.

En particular, los isomorfismos señalan una identidad estructural entre los grupos, que puede ser usada en forma conveniente en muchas aplicaciones. Por ejemplo, el grupo simétrico S_n y el grupo $2\mathbb{Z}$ están relacionados ya que S_n puede ser dividido en permutaciones pares e impares exhibiendo una estructura similar a la de $2\mathbb{Z}$.

Un resultado interesante formulado por Arthur Cayley (1821-1895); establece que todo grupo es isomorfo a un grupo de permutaciones, lo cual es una forma alterna de estudiar a un grupo, sobre todo cuando este es finito.

En esta sección, presentaremos estos importantes conceptos y resultados.

Definición 1.27 (Homomorfismo de grupos)

Sean las estructuras $(G; *)$ y $(H; *')$ dos grupos. Un homomorfismo de $(G; *)$ en $(H; *')$ es una función $\phi : G \to H$ tal que para todo $a, b \in G$ se cumple $\phi(a * b) = \phi(a) *' \phi(b)$.

El comportamiento de los homomorfismos de grupos es conservar la operación de los grupos, es decir, al lado izquierdo se conserva la operación definida en el grupo G, mientras que al lado derecho se conserva la operación definida en el grupo H.

Grupo G	Grupo H	ϕ homomorfismo de G en H
$(G;*)$	$(H;+)$	$\phi(a*b)=\phi(a)+\phi(b)$
$(G;+)$	$(H;*)$	$\phi(a+b)=\phi(a)*\phi(b)$
$(G;*)$	$(H;*)$	$\phi(a*b)=\phi(a)*\phi(b)$

Tabla 1.2: Noción de ϕ un homomorfismo de grupos

Ejemplos.

1. Sea $(\mathbb{Z};+)$ un grupo y sea la función $\phi:\mathbb{Z}\to\mathbb{Z}$, definida por $\phi(a)=\pi a$ para todo $a\in\mathbb{Z}$, entonces ϕ es un homomorfismo. En efecto, sean $a,b\in\mathbb{Z}$ se tiene que $\phi(a+b)=\pi(a+b)=\pi a+\pi b=\phi(a)+\phi(b)$

2. Sea $(\mathbb{R}_{>0};\cdot)$ el grupo multiplicativo de los reales positivos y $(\mathbb{R};+)$ el grupo aditivo de los reales. La función $\phi:\mathbb{R}_{>0}\to\mathbb{R}$, definida por $\phi(a)=\log(a)$ para todo $a\in\mathbb{Z}$, entonces ϕ es un homomorfismo. En efecto, sean $a,b\in\mathbb{R}_{>0}$ se tiene que $\phi(ab)=\log(ab)=\log(a)+\log(b)=\phi(a)+\phi(b)$

3. Sean $(\mathbb{R}^2;+)$ y $(\mathbb{C};+)$ dos grupos y sea la función $\phi:\mathbb{R}^2\to\mathbb{C}$ definida por $\phi(a,b)=a+ib$, entonces ϕ es un homomorfismo. En efecto, sean $x=(a,b),\ y=(a_1,b_1)\in\mathbb{R}^2$ se tiene que

$$\begin{aligned}\phi(x+y)&=\phi((a,b)+(a_1,b_1))\\&=\phi(a+a_1,b+b_1)\\&=a+a_1+i(b+b_1)\\&=a+ib+a_1+ib_1\\&=\phi(a,b)+\phi(a_1,b_1)\\&=\phi(x)+\phi(y)\end{aligned}$$

Proposición 1.18

Sean las estructuras $(G;*)$ y $(H;*')$ dos grupos y ϕ un homomorfismo de grupos. Entonces se cumple que:

1. $\phi(e_G) = e_H$, donde e_G es el neutro de G y e_H el neutro de H.
2. $\phi(a^{-1}) = (\phi(a))^{-1}$, donde a^{-1} es el inverso de $a \in G$ y $(\phi(a))^{-1}$ es el inverso de $\phi(a) \in H$.

Demostración.

1. Sea $a \in G$, entonces $a = a * e_G$ aplicamos la función a ambos lados de la igualdad, entonces $\phi(a) = \phi(a * e_G)$ por hipótesis ϕ es homomorfismo se tiene que $\phi(a) = \phi(a) *' \phi(e_G)$, ahora multiplicamos por el inverso de $\phi(a)$ tal que $[(\phi(a))^{-1} *' \phi(a)] = [(\phi(a))^{-1} *' \phi(a)] *' \phi(e_G)$, entonces $e_H *' \phi(e_G) = e_H$, por lo tanto $\phi(e_G) = e_H$.
2. Sea $a \in G$, entonces $e_G = a * a^{-1}$ aplicamos la función ϕ a ambos lados de la igualdad $\phi(e_G) = \phi(a * a^{-1})$ como ϕ es homomorfismo se tiene que $\phi(e_G) = \phi(a) *' \phi(a^{-1})$ por la propiedad 1 se sigue que $e_H = \phi(a) *' \phi(a^{-1})$, de modo que $\phi(a^{-1})$ es el inversos de $\phi(a)$, por lo tanto $\phi(a^{-1}) = (\phi(a))^{-1}$. □

Proposición 1.19

Sean $\phi : G \to H$ y $\varphi : H \to K$ homomorfismos, donde G, H y K son todos grupos. La composición $\varphi \circ \phi : G \to K$ es homomorfismo.

Demostración. Sean $a, b \in G$, se tiene que:

$$\begin{aligned} \varphi \circ \phi(a * b) &= \varphi(\phi(a * b)) \\ &= \varphi(\phi(a) *' \phi(b)) \\ &= \varphi(\phi(a)) *'' \varphi(\phi(b)) \\ &= \varphi \circ \phi(a) *'' \varphi \circ \phi(b) \end{aligned}$$

□

Definición 1.28
Sea $\phi : G \to H$ un homomorfismo de grupos. Si ϕ es biyectiva, decimos que que ϕ es un isomorfismo de grupos.

Notación. Si ϕ es un isomorfismo de grupos, escribiremos $G \cong H$ para indicar que G es isomorfo a H y escribiremos $G \ncong H$ para indicar que ϕ no lo es.

Ejemplos.

1. Sea G un grupo multiplicativo y sea la función $\phi : G \to G$, definida por $\phi(a) = xax^{-1}$ para todo $a \in G$, entonces ϕ es un isomorfismo. En efecto, primero veamos que ϕ es un homomorfismo. Sean $a, b \in G$ se tiene que:

$$\phi(ab) = xabx^{-1} = xa(x^{-1}x)bx^{-1} = (xax^{-1})(xbx^{-1}) = \phi(a)\phi(b)$$

   Veamos que ϕ es inyectiva, suponemos $\phi(a) = \phi(b)$, entonces $xax^{-1} = xbx^{-1}$ aplicando la ley de cancelación por la derecha e izquierda se tiene que $a = b$.

   Veamos que ϕ es sobreyectiva, sea $b \in G$ consideremos $x = x^{-1}$ y $a = xbx^{-1}$, entonces $a = x^{-1}bx$ tal que

$$\phi(a) = \phi(x^{-1}bx) = x(x^{-1}bx)x^{-1} = (xx^{-1})b(xx^{-1}) = b$$

   Por lo tanto, ϕ es un isomorfismo de grupos y en consecuencia $G \cong G$.

2. Sea $\mathbb{R}$ el grupo aditivo y $\mathbb{R}_{>0}$ el grupo multiplicativo. La función $\phi : \mathbb{R} \to \mathbb{R}_{>0}$, definida por $\phi(a) = 2^a$ para todo $a \in \mathbb{R}$, es un isomorfismo. En efecto, primero veamos que ϕ es un homomorfismo. Sean $a, b \in \mathbb{R}$ se tiene que:

$$\phi(a + b) = 2^{(a+b)} = 2^a 2^b = \phi(a)\phi(b)$$

   Veamos que ϕ es inyectiva, suponemos $\phi(a) = \phi(b)$, entonces $2^a = 2^b$ multiplicando a ambos lados de la igualdad por el logaritmo en base dos se tiene que $\log_2(2^a) = \log_2(2^b)$, entonces $a = b$.

   Veamos que ϕ es sobreyectiva, sea $b \in \mathbb{R}_{>0}$ consideremos $a = \log_2(b) \in \mathbb{R}$, entonces $\phi(a) = \phi(\log_2(b)) = 2^{\log_2(b)} = b$.

   Por lo tanto, ϕ es un isomorfismo de grupos y en consecuencia $\mathbb{R} \cong \mathbb{R}_{>0}$.

Definición 1.29 (Núcleo e imagen)

Sea $\phi : G \to H$ un homomorfismo de grupos. Se define:

1. El núcleo o kernel de ϕ al conjunto: $\ker(\phi) = \{x \in G : \phi(x) = e_H\}$
2. La imagen de ϕ al conjunto: $\text{Im}(\phi) = \{y \in H : \phi(x) = y, \text{ dado } x \in G\}$

Ejemplos.

1. Sea $\phi : \mathbb{Z} \to \mathbb{Z}$ un homomorfismo grupos definido por $\phi(a) = 2a$. Entonces

$$\ker(\phi) = \{x \in \mathbb{Z} : \phi(x) = e_{\mathbb{Z}}\}$$
$$\phi(x) = 0 \Leftrightarrow 2x = 0 \Leftrightarrow x = 0 \Rightarrow \ker(\phi) = \{0\}$$

$$\text{Im}(\phi) = \{y \in \mathbb{Z} : \phi(x) = y, \text{ dado } x \in \mathbb{Z}\}$$
$$\phi(x) = y \Leftrightarrow 2x = y \Leftrightarrow x = y \Rightarrow \text{Im}(\phi) = 2\mathbb{Z}$$

2. Sea $\phi : \mathbb{R} \to \mathbb{R}_{>0}$ un homomorfismo grupos definido por $\phi(a) = 2^a$. Entonces

$$\ker(\phi) = \{x \in \mathbb{R} : \phi(x) = e_{\mathbb{R}_{>0}}\}$$
$$\phi(x) = 1 \Leftrightarrow 2^x = 1 \Leftrightarrow \log_2 2^x = \log_2(1) \Leftrightarrow x = 0 \Rightarrow \ker(\phi) = \{0\}$$

$$\text{Im}(\phi) = \{y \in \mathbb{R}_{>0} : \phi(x) = y, \text{ dado } x \in \mathbb{R}\}$$
$$\phi(x) = 2^x \Leftrightarrow 2^x = 2^x \Leftrightarrow \log_2 2^x = \log_2 2^x \Leftrightarrow x = x \Rightarrow \text{Im}(\phi) = \mathbb{R}_{>0}$$

3. Sea $\phi : \mathbb{R}^2 \to \mathbb{C}$ un homomorfismo de grupos definida por $\phi(a, b) = a + ib$. Entonces

$$\ker(\phi) = \{x \in \mathbb{R}^2 : \phi(x) = e_{\mathbb{C}}\}$$
$$\phi(a, b) = 0 + i0 \Leftrightarrow a + ib = 0 + i0 \Leftrightarrow a = 0 \text{ y } b = 0 \Rightarrow \ker(\phi) = \{(0, 0)\}$$

$$\text{Im}(\phi) = \{y \in \mathbb{C} : \phi(x) = y, \text{ dado } x \in \mathbb{R}^2\}$$
$$\phi(a, b) = a_1 + ib_1 \Leftrightarrow a + ib = a_1 + ib_1 \Leftrightarrow a = a_1 \text{ y } b = b_1 \Rightarrow \text{Im}(\phi) = \mathbb{R}^2$$

Proposición 1.20

Sean las estructuras $(G;*)$ y $(H;*')$ dos grupos y ϕ un homomorfismo de grupos, entonces $\ker(\phi)$ es subgrupo normal en G y $\mathrm{Im}(\phi)$ es un subgrupo de H.

Demostración.

Lo primero que tenemos que ver es que $\ker(\phi) \leqslant G$, sean $x, y \in \ker(\phi)$ veamos que $xy^{-1} \in \ker(\phi)$

$$\begin{aligned}\phi(x * y^{-1}) &= \phi(x) *' \phi(y^{-1}) \\ &= e_H *' (\phi(y))^{-1} \\ &= e_H *' (e_H)^{-1} \\ &= e_H *' e_H \\ &= e_H \in \ker(\phi)\end{aligned}$$

Por lo tanto, $\ker(\phi) \leqslant G$.

Ahora veamos que $\ker(\phi) \triangleleft G$, digamos que $\ker(\phi) = K$ entonces sea $x \in G$ veamos que $xKx^{-1} \subseteq K$

$$\begin{aligned}\phi(x * k * x^{-1}) &= \phi(x) *' \phi(k) *' \phi(x^{-1}) \\ &= \phi(x) *' e_H *' (\phi(x))^{-1} \\ &= \phi(x) *' (\phi(x))^{-1} \\ &= e_H \in K\end{aligned}$$

Por lo tanto, $\ker(\phi) \triangleleft G$.

por último veamos que $\mathrm{Im}(\phi) \leqslant H$, sean $y, y_1 \in \mathrm{Im}(\phi)$, entonces existen $x, x_1 \in G$ tal que $\phi(x) = y$ y $\phi(x_1) = y_1$, veamos que $yy_1^{-1} \in \mathrm{Im}(\phi)$

$$\begin{aligned}y *' y_1^{-1} &= \phi(x) *' (\phi(x_1))^{-1} \\ &= \phi(x) *' \phi(x_1^{-1}) \\ &= \phi(x * x_1^{-1}) \in \mathrm{Im}(\phi)\end{aligned}$$

Por lo tanto, $\mathrm{Im}(\phi) \leqslant H$. □

Teorema 1.4 (Teorema de Cayley)
Todo grupo es isomorfo a un grupo de permutaciones.

Demostración. Sea $(G;*)$ un grupo cualquiera, busquemos un grupo de permutaciones que denominaremos $(\overline{G};\circ)$ y mostremos que es isomorfo a $(G;*)$. Para $a \in G$, consideremos la función $\tau_a : G \to G$ definida por $\tau_a(x) = ax$ para todo $x \in G$, veamos que τ_a es biyectiva.
τ_a es **inyectiva**. En efecto, supongamos que $\tau_a(x) = \tau_a(y)$, por definición se tiene que $ax = ay$, luego por la ley de cancelación izquierda se tiene que $x = y$.
τ_a es **sobreyectiva**. En efecto, sea $y \in G$ y consideremos $x = a^{-1}y$ se tiene que $\tau_a(x) = \tau_a(a^{-1}y) = aa^{-1}y = y$, luego $\tau_a(x) = y$.
Por lo tanto, τ_a es una permutación de G.
Consideremos ahora la familia de permutaciones $\overline{G} = \{\tau_a : a \in G\}$ y mostremos que $(\overline{G};\circ)$ es un grupo. En efecto, sean $\tau_a, \tau_b, \tau_c \in \overline{G}$ y $a, b, c \in G$, se tiene que

1. La operación $\circ$ es cerrada, ya que
   $\tau_a \circ \tau_b(x) = \tau_a(\tau_b(x)) = \tau_a(bx) = (ab)x = \tau_{ab}(x)$

2. La operación $\circ$ es asociativa, ya que la composición de funciones es asociativa.

3. Existe el elemento neutro, ya que $\tau_e(x) = ex$ es la función identidad de $\overline{G}$, tal que $\tau_a \circ \tau_e(x) = \tau_a(\tau_e(x)) = \tau_a(ex) = (ae)x = ax = \tau_a$

4. Para cada elemento de $\overline{G}$, existe el elemento inverso $(\tau_a)^{-1} = \tau_{a^{-1}} = a^{-1}x \in \overline{G}$ tal que $\tau_a \circ \tau_{a^{-1}}(x) = \tau_a(\tau_{a^{-1}}(x)) = \tau_a(a^{-1}x) = (aa^{-1})x = ex = \tau_e$

   Por lo tanto, $(\overline{G};\circ)$ es un grupo de permutaciones.

Finalmente consideremos la función $\phi : G \to \overline{G}$ definida por $\phi(a) = \tau_a$ y mostremos que ϕ es un isomorfismo. En efecto, ya que
ϕ es un homomorfismo, sean $a, b \in G$ se tiene que

$$\phi(ab) = \tau_{ab} = \tau_a \circ \tau_b = \phi(a) \circ \phi(b)$$

ϕ es **inyectiva**, suponemos $\phi(a) = \phi(b)$, entonces $\tau_a = \tau_b$, si $x = e$ con $x \in G$ se tiene que $\tau_a(e) = \tau_b(e)$ luego $ae = be$, y se tiene que $a = b$.

ϕ es **sobreyectiva**, esto se cumple por como está definida ϕ, ya que si $\tau_y \in \overline{G}$ existe $y \in G$ tal que $\phi(y) = \tau_y$.
Por lo tanto, ϕ es un isomorfismo y en consecuencia $G \cong \overline{G}$. □

1.9 Clausura

La influencia de la teoría de grupos, en todas las áreas de la matemática, y también en muchas otras disciplinas, es abrumadora y al mismo tiempo extraordinaria. En este módulo hemos querido resaltar los conceptos, definiciones, proposiciones, teoremas y ejemplos más significativos de esta extensa teoría, con la esperanza de que estas nociones ayuden al lector, no solo a entenderla, sino que también le animen a profundizar sobre esta importante estructura algebraica y sus aplicaciones.

La estructura de grupo, adicionalmente, es el preámbulo para el estudio de otras estructuras más completas. En particular, el próximo módulo de esta monografía contempla el estudio de la estructura de Anillos, de mucha relevancia dentro de la matemática.

Módulo II

Teoría de Anillos

Anillos

La importancia de la teoría de anillos, puede evidenciarse no sólo en el trabajo de muchos matemáticos que la han usado para lograr avances en la especialidad, sino también en sus aplicaciones. Un ejemplo de aplicación lo constituye el funcionamiento de los sistemas de comunicación, específicamente de los codificadores y decodificadores.

Este módulo proporciona a los lectores nociones elementales sobre la teoría de anillos; se presenta definiciones, proposiciones, teoremas y ejemplos.

Adicionalmente, se recomienda al lector revisar el módulo I antes de iniciarse en el estudio de este módulo II, ya que esto facilitará su comprensión.

Propósito

Al finalizar este módulo el estudiante estará en capacidad entender los conceptos asociados a la teoría de anillos y sus propiedades. Además, seguirá con rigor las proposiciones y teoremas que se estudian.

Contenido

2.1 Anillos y sus propiedades

En esta sección se estudiará la estructura de anillo que tiene la forma $(A; *_1, *_2)$, donde A es un conjunto no vacío y $*_1$ y $*_2$ son operaciones cerradas en A. Adicionalmente, se discuten propiedades básicas de la estructura.

Definición 2.1 (Anillo)

Sea A un conjunto no vacío, y sean $\oplus, \odot$ operaciones definidas en A, diremos que la terna $(A; \oplus, \odot)$ es un anillo si se cumple las siguientes condiciones:

1. El par $(A; \oplus)$ es un grupo abeliano.
2. El par $(A; \odot)$ es un semigrupo.
3. La operación $\odot$ es distributiva respecto a la operación $\oplus$, es decir, para todo $a, b, c \in A$ se tiene que:

$$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c) \qquad \text{(ley distributiva izquierda)}$$
$$(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a) \qquad \text{(ley distributiva derecha)}$$

Ejemplos.

1. Sea $\mathbb{Z}$ el conjunto de los números enteros y sean las operaciones suma y producto usuales definidas en $\mathbb{Z}$. La terna $(\mathbb{Z}; +, \cdot)$ es un anillo, ya que

   i. El par $(\mathbb{Z}; +)$ es un grupo abeliano, ya que la suma de enteros devuelve enteros, además de ser asociativa y conmutativa, que el 0 es elemento neutro para la suma y que todo elemento tiene inverso es claro que $(\mathbb{Z}; +)$ es un grupo abeliano.

   ii. El par $(\mathbb{Z}; \cdot)$ es un semigrupo, ya que el producto de enteros devuelve enteros y que la multiplicación es asociativa, es claro que $(\mathbb{Z}; \cdot)$ es un semigrupo.

   iii. Por último, el producto de enteros es distributivo con respecto a la suma de enteros a la derecha y a la izquierda.

   Luego, podemos concluir que $(\mathbb{Z}; +, \cdot)$ es un anillo.

2. La estructura formada con el conjunto $\mathbb{Z}/m$, de las clases de congruencias módulo m, junto con las operaciones suma y producto usual entre clases. Veamos que la terna $(\mathbb{Z}/m; +, \cdot)$ es un anillo.

   i. De acuerdo con la proposición 1.6 del módulo I, el par $(\mathbb{Z}/m; +)$ es un grupo abeliano.

   ii. El par $(\mathbb{Z}/m; \cdot)$ es un semigrupo, ya que

   - El producto es cerrado, ya que el producto de clases residuales de $\mathbb{Z}/m$ da una clase residual de $\mathbb{Z}/m$.
   - El producto es asociativo, ya que para todo $[a], [b], [b] \in \mathbb{Z}/m$ se tiene que $([a][b])[c] = [ab][c] = [(ab)c] = [a(bc)] = [a][bc] = [a]([b][c])$.

   Por lo tanto, $(\mathbb{Z}/m; \cdot)$ es un semigrupo.

   iii. El producto es distributivo respecto a la suma, ya que

$$[a]([b] + [c]) = [a]([b + c]) = [a(b + c)] = [ab + ac] = [a][b] + [a][c]$$
$$([b] + [c])[a] = ([b + c])[a] = [(b + c)a] = [ba + ca] = [b][a] + [c][a]$$

   Por lo tanto, $(\mathbb{Z}/m; +, \cdot)$ es un anillo.

3. Sea $\mathbb{C}$ el conjunto de los números complejos y sean las operaciones suma y producto usuales. Veamos que la terna $(\mathbb{C}; +, \cdot)$ es un anillo.

   i. El par $(\mathbb{C}; +)$ es un grupo abeliano, ver el ejemplo 2 de grupos abelianos en la sección 1.1 del módulo I.

   ii. El par $(\mathbb{C}; \cdot)$ es un semigrupo. En efecto, sean $u = a + ib, v = a_1 + ib_1$, $z = a_2 + ib_2 \in \mathbb{C}$ se tiene que

   - El producto es cerrado, ya que
     $(a + ib)(a_1 + ib_1) = aa_1 + aib_1 + iba_1 + i^2bb_1 = aa_1 - bb_1 + i(ab_1 + ba_1)$

- El producto es asociativo, ya que

$$\begin{aligned}(uv)z &= [(a+ib)(a_1+ib_1)](a_2+ib_2)\\ &= (aa_1+aib_1+iba_1+ibib_1)(a_2+ib_2)\\ &= (aa_1)a_2+(aib_1)a_2+(iba_1)a_2+(ibib_1)a_2+(aa_1)ib_2+(aib_1)ib_2\\ &\quad +(iba_1)ib_2+(ibib_1)ib_2\\ &= a(a_1a_2)+a(a_1ib_2)+ib(ib_1a_2)+a(ib_1ib_2)+ib(a_1a_2)+ib(a_1ib_2)\\ &\quad +ib(ib_1a_2)+ib(ib_1ib_2)\\ &= (a+ib)[a_1a_2+a_1ib_2+ib_1a_2+ib_1ib_2]\\ &= (a+ib)[(a_1+ib_1)(a_2+ib_2)]\\ &= u(vz)\end{aligned}$$

Por lo tanto, $(\mathbb{C};\cdot)$ es un semigrupo.

iii. El producto es distributivo respecto a la suma, ya que

$$\begin{aligned}u(v+z) &= (a+ib)[(a_1+ib_1)+(a_2+ib_2)]\\ &= (a+ib)(a_1+a_2+ib_1+ib_2)\\ &= aa_1+aa_2+aib_1+aib_2+iba_1+iba_2+ibib_1+ibib_2\\ &= aa_1+aib_1+iba_1+ibib_1+aa_2+aib_2+iba_2+ibib_2\\ &= (a+ib)(a_1+ib_1)+(a+ib)(a_2+ib_2)\\ &= (uv)+(uz)\end{aligned}$$

$$\begin{aligned}(v+z)u &= [(a_1+ib_1)+(a_2+ib_2)](a+ib)\\ &= (a_1+a_2+ib_1+ib_2)(a+ib)\\ &= a_1a+a_2a+ib_1a+ib_2a+a_1ib+a_2ib+ib_1ib+ib_2ib\\ &= a_1a+ib_1a+a_1ib+ib_1ib+a_2a+ib_2a+a_2ib+ib_2ib\\ &= (a_1+ib_1)(a+ib)+(a_2+ib_2)(a+ib)\\ &= (vu)+(zu)\end{aligned}$$

Por lo tanto, $(\mathbb{C};+,\cdot)$ es un anillo.

Proposición 2.1

Sea $(A;+,\cdot)$ un anillo. Para todo $a,b,c \in A$ se satisfacen las siguientes propiedades:

1. $a0 = 0a = 0$
2. $a(-b) = (-a)b = -ab$
3. $(-a)(-b) = ab$
4. $a(b-c) = ab - ac$
5. $(b-c)a = ba - ca$

Demostración.

1. Nótese que $a0 = a(0+0) = a0 + a0$, por la ley de cancelación derecha se tiene que $a0 = 0$.
2. Como $b + (-b) = 0$, se tiene que $0 = a0 = a(b+(-b)) = ab + a(-b)$, recordemos que $-ab$ es el inverso de ab, entonces $-ab + 0 = -ab + ab + a(-b)$, por lo tanto $a(-b) = -ab$.
3. Como $0 = (-a)0 = -a(b+(-b)) = (-a)b + (-a)(-b) = -ab + (-a)(-b)$, sumando ab en la igualdad se tiene que $ab + 0 = ab + (-ab) + (-a)(-b)$, por lo tanto $(-a)(-b) = ab$.
4. $$a(b-c) = a(b+(-c)) = ab + a(-c) = ab - ac$$
5. $$(b-c)a = (b+(-c))a = ba + (-c)a = ba - ca$$ □

De aquí en adelante el grupo abeliano $(A;\oplus)$ lo representaremos en notación aditiva $(A;+)$ y al semigrupo $(A;\odot)$ lo representaremos en notación multiplicativa $(A;\cdot)$.

De este modo escribiremos $a+b$ en lugar de $a \oplus b$ y ab o $a \cdot b$ en lugar de $a \odot b$. Al neutro según la operación $\oplus$ lo llamaremos neutro aditivo y lo representaremos con 0; mientras que el neutro según la operación $\odot$ lo llamaremos neutro multiplicativo y lo representaremos con 1.

Definición 2.2 (Anillo unitario y Anillo conmutativo)
Sea $(A; +, \cdot)$ un anillo.

1. Si existe $1 \in A$ tal que $a \cdot 1 = a$ y $1 \cdot a = a$ para todo $a \in A$. Decimos que la terna $(A; +, \cdot)$ es un anillo unitario.
2. Si se cumple que $a \cdot b = b \cdot a$, para todo $a, b \in A$. Decimos que la terna $(A; +, \cdot)$ es un anillo conmutativo.

Ejemplos.

1. La terna $(\mathbb{Z}/m; +, \cdot)$ es un anillo unitario y conmutativo, ya que

   i. Existe $[e] = [1] \in \mathbb{Z}/m$, tal que

   $$\forall\, [a] \in \mathbb{Z}/m : \ [a][1] = [a1] = [a] \quad \text{y} \quad [1][a] = [1a] = [a]$$

   Por lo tanto, $(\mathbb{Z}/m; +, \cdot)$ es un anillo unitario.

   ii. Para todo $[a], [b] \in \mathbb{Z}/m$ se cumple que

   $$[a][b] = [ab] = [ba] = [b][a]$$

   Por lo tanto, $(\mathbb{Z}/m; +, \cdot)$ es un anillo conmutativo.

2. La terna $(\mathbb{C}; +, \cdot)$ es un anillo unitario y conmutativo, ya que

   i. Existe $e = 1 + 0i \in \mathbb{C}$, tal que

   $$ue = (a + ib)(1 + 0i) = a + a(0i) + ib + ib(0i) = a + ib$$
   $$eu = (1 + 0i)(a + ib) = a + ib + (0i)a + (0i)ib = a + ib$$

   Por lo tanto, $(\mathbb{C}; +, \cdot)$ es un anillo unitario.

ii. Para todo $u, v \in \mathbb{C}$ se cumple que

$$\begin{aligned} uv &= (a+ib)(a_1+ib_1) \\ &= aa_1 + aib_1 + iba_1 + ibib_1 \\ &= a_1a + a_1ib + ib_1a + ib_1ib \\ &= (a_1+ib_1)(a+ib) = vu \end{aligned}$$

Por lo tanto, $(\mathbb{C}; +, \cdot)$ es un anillo conmutativo.

Proposición 2.2

Para todo anillo unitario $(A; +, \cdot)$, se cumple:

1. El elemento neutro de la operación $\cdot$ es único.
2. $(-1)(a) = -a$
3. $(-1)(-a) = a$

Demostración.

1. La demostración es análoga al de la proposición 1.1 del módulo I.

2.
$$\begin{aligned} -a &= -a + 0 \\ &= -a + (0)a \\ &= -a + (1 + (-1))a \\ &= -a + a + (-1)a \\ &= (-1)a \end{aligned}$$

3.
$$\begin{aligned} 0(-a) &= 0 \\ (1 + (-1))(-a) &= 0 \\ 1(-a) + (-1)(-a) &= 0 \\ -a + (-1)(-a) &= 0 \end{aligned}$$

$$a + (-a) + (-1)(-a) = a + 0$$
$$(-1)(-a) = a$$

□

Definición 2.3
Sea $(A; +, \cdot)$ un anillo unitario. Se dice que a es una unidad del anillo A, si existe $b \in A$ tal que $ab = 1$ y $ba = 1$.

Si el elemento b existe, éste se denomina inverso. La definición de elemento inverso podemos encontrar en la sección 1.1 del módulo I. Además, si un elemento tiene inverso, éste es único. La demostración a la afirmación anterior es análoga al de la proposición 1.1.

Notación. Cuando el inverso del elemento a existe, lo denotaremos como a^{-1}.

Ejemplos.

1. En el anillo unitario $(\mathbb{R}; +, \cdot)$, todo elemento no nulo $a \in \mathbb{R}$ es una unidad de $\mathbb{R}$, ya que existe su inverso $a^{-1} = \frac{1}{a} \in \mathbb{R}$ tal que
$$aa^{-1} = a\left(\frac{1}{a}\right) = 1, \qquad a^{-1}a = \left(\frac{1}{a}\right)a = 1$$
2. En el anillo unitario $(\mathbb{Q}; +, \cdot)$, todo elemento $a = \frac{m}{n} \in \mathbb{Q}$ con $n \neq 0$ es una unidad de $\mathbb{Q}$, pues existe su inverso $a^{-1} = \frac{n}{m} \in \mathbb{Q}$ tal que
$$aa^{-1} = \frac{m}{n}\left(\frac{n}{m}\right) = 1, \qquad a^{-1}a = \left(\frac{n}{m}\right)\frac{m}{n} = 1$$
3. En el anillo unitario $(\mathbb{Z}; +, \cdot)$, las únicas unidades de $\mathbb{Z}$ son $\{1, -1\}$, ya que si $a \in \mathbb{Z}$, para que a sea unidad tiene que satisfacer $aa^{-1} = 1$ y $a^{-1}a = 1$, de modo que $a^{-1} = \frac{1}{a}$, pero esto no es verdad ya que $\frac{1}{a} \notin \mathbb{Z}$.

Definición 2.4 (Característica de un anillo)
Sea $(A; +, \cdot)$ un anillo. Se llama característica del anillo A y se escribe $\text{Char}(A)$, al entero positivo más pequeño n tal que $na = 0$ para todo $a \in A$.

Si no existe el entero positivo n tal que $na = 0$, decimos la característica de A es cero.

Ejemplos.

1. Considere el anillo $(\mathbb{Z}/7; +, \cdot)$, entonces $\text{Char}(\mathbb{Z}/7) = 7$, ya que para todo $a \in \mathbb{Z}/7$ existe $n = 7$ tal que

$$7(0) = 0 \qquad 7(4) = 28 = 0$$
$$7(1) = 7 = 0 \qquad 7(5) = 35 = 0$$
$$7(2) = 14 = 0 \qquad 7(6) = 42 = 0$$
$$7(3) = 21 = 0$$

2. Considere el anillo $(\mathbb{Z}/5; +, \cdot)$, entonces $\text{Char}(\mathbb{Z}/5) = 5$, ya que para todo $a \in \mathbb{Z}/5$ existe $n = 5$ tal que

$$5(0) = 0 \qquad 5(3) = 15 = 0$$
$$5(1) = 5 = 0 \qquad 5(4) = 20 = 0$$
$$5(2) = 10 = 0$$

   Note que para $n = 10$, $n = 15$ y en general los múltiplos de 5, también cumplen la definición de característica de un anillo; sin embargo $\text{Char}(\mathbb{Z}/5) = 5$ ya que $n = 5$ es el entero positivo más pequeño con esa propiedad.

3. Los anillos $(\mathbb{Z}; +, \cdot)$, $(\mathbb{R}; +, \cdot)$, $(\mathbb{Q}; +, \cdot)$ y $(\mathbb{C}; +, \cdot)$, tienen característica cero, ya que para todo a elemento de los anillos dados, se cumple que $0(a) = 0$.

Proposición 2.3

Sea $(A; +, \cdot)$ un anillo unitario.

1. Si 1 tiene orden n respecto a la suma, entonces $\text{Char}(A) = n$.

2. Si 1 tiene orden infinito respecto a la suma, entonces $\text{Char}(A) = 0$.

Recordemos que el orden de un elemento se define como n el entero positivo más pequeño tal que $a^n = e$, que en notación aditiva lo expresamos como $na = 0$.

Demostración.

1. Suponemos que 1 tiene orden aditivo n, entonces n es el entero positivo más pequeño tal que $n1 = 0$. Entonces, para todo $a \in A$, se tiene que

$$na = a + a + \ldots + a = a(1 + 1 + \ldots + 1) = a(n1) = a0 = 0$$

   Por lo tanto, $\text{Char}(A) = n$.

2. Suponemos que 1 tiene ordenen infinito, entonces no existe n entero positivo más pequeño tal que $n1 = 0$, de modo que $\text{Char}(A) = 0$. □

Ejemplos.

1. Para el anillo unitario $(\mathbb{Z}/7; +, \cdot)$, entonces $\text{Char}(\mathbb{Z}/7) = 7$, ya que 1 tiene orden n.

$$1 + 1 + 1 + 1 + 1 + 1 + 1 = 7 \mid 7 = 0$$

2. Para el anillo unitario $(\mathbb{Z}; +, \cdot)$, entonces $\text{Char}(\mathbb{Z}) = 0$, ya que 1 tiene orden infinito.

$$1 + 1 + \ldots + 1 + 1 + 1 + \ldots = \infty$$

   Otros anillos unitarios con característica cero son; $(\mathbb{R}; +, \cdot)$, $(\mathbb{Q}; +, \cdot)$.

2.2 Subanillos

En esta sección estudiaremos los subanillos de un anillo $(A; +, \cdot)$. Los subanillos son estructuras análogas a los subgrupos, donde un subconjunto de A goza de las mismas propiedades del anillo. Por ejemplo; dado que $\mathbb{Z}$ es un subconjunto de $\mathbb{R}$ se puede probar que $(\mathbb{Z}; +, \cdot)$ es un subanillo de $(\mathbb{R}; +, \cdot)$.

Definición 2.5 (Subanillo)
Sea la terna $(A; +, \cdot)$ un anillo y sea S un subconjunto no vacío de A. Se dice que S es un subanillo de A, si $(S; +, \cdot)$ es un anillo, donde $+$ y $\cdot$ son las operaciones definidas en A.

Notación. Si $(S; +, \cdot)$ es un subanillo de $(A; +, \cdot)$ escribiremos $S \leqslant A$ y si no lo es escribiremos $S \not\leqslant A$

Ejemplos.

1. Sea $(\mathbb{Z}; +, \cdot)$ el anillo de los enteros y sea $S = \{2n : n \in \mathbb{Z}\}$, entonces S es un subanillo de anillo $\mathbb{Z}$, ya que

   i. El par $(S; +)$ es un grupo abeliano.

   ii. El par $(S; \cdot)$ es un semigrupo.

   iii. El producto es distributivo respecto a la suma, ya que dados $a, b, c \in S$ se tiene que

   $$\begin{aligned} a(b+c) &= 2n_1(2n_2 + 2n_3) & (b+c)a &= (2n_2 + 2n_3)2n_1 \\ &= 2n_1(2(n_2 + n_3) & &= (2(n_2 + n_3)2n_1 \\ &= 2n_1 2(n_2 + 2n_1 2n_3 & &= 2(n_2 2n_1 + 2n_3 2n_1 \\ &= ab + ac & &= ba + ca \end{aligned}$$

   Por lo tanto, $(S, +, \cdot)$ es un anillo y en consecuencia $S \leqslant \mathbb{Z}$. En general el conjunto $n\mathbb{Z}$ con $n \in \mathbb{Z}$ fijo, es un subanillo del anillo $(\mathbb{Z}; +, \cdot)$.

2. Sea $(\mathbb{C}; +, \cdot)$ el anillo de los números complejos y consideremos el conjunto de los enteros gaussianos $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$, entonces $\mathbb{Z}[i]$ es un subanillo del anillo $\mathbb{C}$, ya que

   i. El par $(\mathbb{Z}[i]; +)$ es un grupo abeliano.

   ii. El par $(\mathbb{Z}[i]; \cdot)$ es un semigrupo.

   iii. El producto es distributivo respecto a la suma.

   Por lo tanto, $(\mathbb{Z}[i]; +, \cdot)$ es un anillo y en consecuencia $\mathbb{Z}[i] \leqslant \mathbb{C}$.

3. Sea $(\mathbb{R}; +, \cdot)$ un anillo y sea $S = \mathbb{Q}$, entonces S es un subanillo de $\mathbb{R}$, ya que

   i. El par $(S; +)$ es un grupo abeliano, ya que para todo $a = \frac{m}{n}$, $b = \frac{m_1}{n_1}$, $c = \frac{m_2}{n_2} \in S$, se tiene que

   - La suma es cerrada, ya que

   $$a + b = \frac{m}{n} + \frac{m_1}{n_1} = \frac{n_1 m + n m_1}{n n_1} \in S$$

- La suma es asociativa, esto se cumple ya que se hereda la asociatividad en $\mathbb{R}$.
- Existe el elemento neutro en S dado por $e = \frac{0}{n} \in S$, tal que

$$a + e = \frac{m}{n} + \frac{0}{n} = \frac{m+0}{n} = \frac{m}{n}$$

- Elemento inverso, para todo $a \in S$ existe $a^{-1} = -\frac{m}{n} \in S$, tal que

$$a + a^{-1} = \frac{m}{n} + \left(-\frac{m}{n}\right) = \frac{m-m}{n} = \frac{0}{n}$$

- La suma es conmutativa, esto se cumple ya que se hereda la conmutatividad de $\mathbb{R}$.

  Por lo tanto, $(S; +)$ es un grupo abeliano.

ii. El par $(S; \cdot)$ es un semigrupo, ya que para todo $a, b, c \in S$, se tiene que

- El producto es cerrado, ya que

$$ab = \frac{m}{n}\frac{m_1}{n_1} = \frac{mm_1}{nn_1} \in S$$

- El producto es asociativo, ya que se hereda la asociatividad de $\mathbb{R}$.

  Por lo tanto, $(S; \cdot)$ es un semigrupo.

iii. El producto es distributivo respecto a la suma, ya que

$$\begin{aligned} a(b+c) &= \frac{m}{n}\left(\frac{m_1}{n_1} + \frac{m_2}{n_2}\right) \\ &= \frac{m}{n}\left(\frac{n_2m_1 + n_1m_2}{n_1n_2}\right) \\ &= \frac{m(n_2m_1 + n_1m_2)}{nn_1n_2} \\ &= \frac{mn_2m_1 + mn_1m_2}{nn_1n_2} \\ &= \frac{mn_2m_1}{nn_1n_2} + \frac{mn_1m_2}{nn_1n_2} \\ &= \frac{mm_1}{nn_1} + \frac{mm_2}{nn_2} \\ &= ab + ac \end{aligned} \qquad \begin{aligned} (b+c)a &= \left(\frac{m_1}{n_1} + \frac{m_2}{n_2}\right)\frac{m}{n} \\ &= \left(\frac{n_2m_1 + n_1m_2}{n_1n_2}\right)\frac{m}{n} \\ &= \frac{(n_2m_1 + n_1m_2)m}{n_1n_2n} \\ &= \frac{n_2m_1m + n_1m_2m}{n_1n_2n} \\ &= \frac{n_2m_1m}{n_1n_2n} + \frac{n_1m_2m}{n_1n_2n} \\ &= \frac{m_1m}{n_1n} + \frac{m_2m}{n_2n} \\ &= ba + ca \end{aligned}$$

Por lo tanto, $(S; +, \cdot)$ es un anillo y en consecuencia $S \leqslant \mathbb{R}$.

Nota. Un subanillo S se dice que es propio cuando no coincide con todo el anillo A, es decir, si $S \neq A$.

Teorema 2.1 (Caracterización de subanillos)
Sea $(A;+,\cdot)$ un anillo y sea S un subconjunto de A. S es un subanillo de A si y sólo si,

1. para todo $a, b \in S$, se tiene que $a - b \in S$
2. para todo $a, b \in S$, se tiene que $ab \in S$

Demostración.

$\Rightarrow$) Suponemos que S es un subanillo de $(A;+,\cdot)$ veamos que $a - b \in S$ y $ab \in S$. Por hipótesis S es un subanillo, entonces $(S;+)$ es un grupo abeliano y $(S;\cdot)$ es un semigrupo, por lo tanto se cumplen las condiciones 1 y 2, ya que para todo $x, y \in S$ se tiene que $x - y \in S$ y $xy \in S$.

$\Leftarrow$) Suponemos que para todo $a, b \in S$ se cumple $a - b \in S$ y $ab \in S$, mostremos que $(S;+,\cdot)$ es un subanillo.

1. Por la condición que $a - b = a + (-b) \in S$ implica que $(S;+)$ sea un subgrupo del grupo abeliano $(A;+)$, luego $(S;+)$ es un grupo abeliano.
2. Por la condición que $ab \in S$ implica que $(S;\cdot)$ sea un semigrupo.
3. Que el producto sea distributivo respecto a la suma, se cumple pues estas leyes de distribución se cumplen en A, de modo que se cumple en S.

   Por lo tanto, $(S;+,\cdot)$ es un subanillo. □

Ejemplos.

1. Considere el anillo $(\mathbb{R};+,\cdot)$ y sea $S = \mathbb{Q}$, entonces S es un subanillo de $\mathbb{R}$, ya que

   i. para todo $a, b \in S$ se cumple que $a - b \in S$

$$a - b = \frac{m}{n} - \frac{m_1}{n_1} = \frac{n_1 m - n m_1}{n n_1} \in S$$

ii. para todo $a, b \in S$ se cumple que $ab \in S$

$$ab = \left(\frac{m}{n}\right)\left(\frac{m_1}{n_1}\right) = \frac{mm_1}{nn_1} \in S$$

Por lo tanto, $S \leqslant \mathbb{R}$.

2. Considere el anillo $(\mathbb{C}; +, \cdot)$ y sea $S = \mathbb{Z}[i]$, entonces S es un subanillo de $\mathbb{C}$, ya que

i. para todo $u, v \in S$ se cumple que $u - v \in S$

$$u - v = (a + ib) - (a_1 + ib_1) = a + ib - a_1 - ib_1 = a - a_1 + i(b - b_1)$$

ii. para todo $u, v \in S$ se cumple que $uv \in S$

$$uv = (a+ib)(a_1+ib_1) = aa_1 + ib_1a + iba_1 - bb_1 = aa_1 - bb_1 + i(b_1a + ba_1)$$

Por lo tanto, $S \leqslant \mathbb{C}$.

2.3 Dominios de Integridad (DI) y Campos

En esta sección estudiaremos algunos tipos especiales de anillos, tales como; los dominios de integridad y campos que son clases particulares de anillos con 3 propiedades que veremos más adelante. Los dominios de integridad, también conocidos como dominios enteros juegan un rol importante en la teoría de números y la geometría algebraica. Por otra parte los campos o cuerpos, son estructuras algebraicas indispensables de estudio en diversas ramas de las matemáticas puras, como: el análisis matemático, la geometría y la física.

Notación. En lo sucesivo escribiremos "sea A un anillo", en lugar de "sea $(A; +, \cdot)$ un anillo".

Definición 2.6 (Divisor de cero)
Sea A un anillo y sea $a \in A$ un elemento no nulo. Se dice que a es divisor de cero si existe $b \in A$ un elemento no nulo, tal que $ab = 0$.

Ejemplos.

1. En el anillo $(\mathbb{Z}/12; +, \cdot)$. Los elementos $4, 6, 8, 10$ son divisores de cero, ya que

$$4 \cdot 3 = 12 = 0 \qquad 8 \cdot 3 = 24 = 0$$
$$6 \cdot 2 = 12 = 0 \qquad 10 \cdot 6 = 60 = 0$$

2. El anillo de los enteros gaussianos $(\mathbb{Z}[i]; +, \cdot)$ no tiene divisores de cero. Ya que si suponemos lo contrario dados $u = a + ib, v = a_1 + ib_1 \in \mathbb{Z}[i]$, entonces $uv = 0 + i0$ teniendo en cuenta que u, v son imaginarios no nulos.

$$(a + ib)(a_1 + ib_1) = 0 + i0$$
$$(aa_1 - bb_1) + i(ab_1 + ba_1) = 0 + i0$$

   de modo que

$$\begin{cases} aa_1 - bb_1 = 0 \\ ab_1 + ba_1 = 0 \end{cases}$$

   Resolviendo este sistema de ecuaciones se obtiene que $a(a_1^2 + b_1^2) = 0$, de esto $a = 0$ o $a_1^2 + b_1^2 = 0$, entonces $a_1 = 0$ y $b_1 = 0$ de modo que $v = 0 + i0$, lo cual no es posible pues v no es nulo.

   Por lo tanto, el conjunto $\mathbb{Z}[i]$ no tiene divisores de cero.

3. El anillo $(\mathbb{Z}/7; +, \cdot)$, no tiene divisores de cero, ya que para todo $a \in \mathbb{Z}/7$ no existe $b \in \mathbb{Z}/7$, tal que $ab = 0$. En general $\mathbb{Z}/m$ no tiene divisores de cero cuando m es primo. En efecto

   Supongamos que $\mathbb{Z}/m$ si tiene divisores de cero, entonces dados $a, b \in \mathbb{Z}/m$ se tiene que cumplir que $ab = 0$ teniendo en cuenta que a y b son no nulos. Recordemos que estamos en el conjunto de las clases residuales y escribir a en lugar de $[a]$ es simple notación, para este caso utilicemos la notación habitual, sean $[a], [b] \in \mathbb{Z}/m$ se tiene que $[a][b] = [0]$ entonces $[ab] = [0]$, de modo que $ab \equiv 0(\text{mód } m)$, luego $m \mid ab - 0$, entonces $m \mid a$ o $m \mid b$ equivalente a $m \mid a - 0$ o $m \mid b - 0$ de este modo $a \equiv 0(\text{mód } m)$ o $b \equiv 0(\text{mód } m)$, esto implica que $[a] = [0]$ o $[b] = [0]$ lo cuál es una contradicción ya que $[a], [b]$ son no nulos.

Por lo tanto, si m es primo $\mathbb{Z}/m$ no tiene divisores de de cero. Normalmente, cuando m es primo, el conjunto $\mathbb{Z}/m$ se escribe como $\mathbb{Z}/p$.

Definición 2.7 (Dominio de integridad DI)
Un dominio de integridad A, es un anillo unitario, conmutativo que no tiene divisores de cero.

Ejemplos.

1. La terna $(\mathbb{Z}; +, \cdot)$ es un dominio de integridad, ya que $(\mathbb{Z}; +, \cdot)$ es un anillo unitario, conmutativo y además $\mathbb{Z}$ no tiene divisores de cero, pues dado $a \in \mathbb{Z}$ elemento no nulo, no existe $b \in \mathbb{Z}$ elemento no nulo, tal que $ab = 0$.

2. La terna $(\mathbb{Z}[i]; +, \cdot)$ es un dominio de integridad, ya que $(\mathbb{Z}[i]; +, \cdot)$ es un anillo unitario, conmutativo y además $\mathbb{Z}[i]$ no tiene divisores de cero, pues dado $u \in \mathbb{Z}[i]$ elemento no nulo, no existe $v \in \mathbb{Z}[i]$ elemento no nulo, tal que $uv = 0$.

3. La terna $(\mathbb{Z}/p; +, \cdot)$ es un dominio de integridad, ya que $(\mathbb{Z}/p; +, \cdot)$ es un anillo unitario, conmutativo y además $\mathbb{Z}/p$ no tiene divisores de cero, pues dado $a \in \mathbb{Z}/p$ elemento no nulo, no existe $b \in \mathbb{Z}/p$ elemento no nulo, tal que $ab = 0$.

4. La terna $(\mathbb{Z}/m; +, \cdot)$ no es un dominio de integridad, ya que $\mathbb{Z}/m$ tiene divisores de cero, pues dado $a \in \mathbb{Z}/m$ elemento no nulo, existe $b \in \mathbb{Z}/m$ elemento no nulo, tal que $ab = 0$.

Proposición 2.4
Sea A un dominio de integridad con $\text{Char}(A) = p$, entonces p es primo.

Demostración. Usando reducción al absurdo, suponemos que p no es primo, entonces $p = p_1 p_2$, por hipótesis $\text{Char}(A) = p$ entonces $pa = 0$ para todo $a \in A$. Como $p = p_1 p_2$, entonces $p_1 a \neq 0$ y $p_2 a \neq 0$ de modo que $(p_1 a)(p_2 a) \neq 0$, asociando tenemos $p_1(a p_2)a \neq 0$ ya que A es un dominio íntegro se tiene

que $p_1(p_2a)a \neq 0$, sigue que $(p_1p_2)(aa) \neq 0$, entonces $pa \neq 0$, lo cual es una contradicción ya que $pa = 0$, por lo tanto p es primo. □

Definición 2.8 (Dominio euclidiano DE)
Sea A un dominio de integridad. Decimos que A es un dominio euclidiano si existe una función $\delta : A \setminus \{0\} \to \mathbb{Z}$, tal que

1. para todo $a, b \in A \setminus \{0\}$, se tiene que $\delta(a) \leq \delta(ab)$.
2. para todo $a, b \in A$ con $b \neq 0$, existen $q, r \in A$ tales que $a = bq + r$ con $r = 0$ o $\delta(r) < \delta(b)$.

En el ítem 2 de la definición anterior, a es el dividendo, b es el divisor, q es el cociente y r es el resto.

Ejemplos.

1. El dominio de integridad $(\mathbb{Z}; +, \cdot)$ con la función $\delta(a) = |a|$ es un dominio euclidiano, ya que
   i. para todo $a, b \in \mathbb{Z} \setminus \{0\}$, se tiene que $\delta(ab) = |ab| = |a||b| = \delta(a)\delta(b)$, entonces $\delta(a) = |a| \leq |a||b| = \delta(ab) \Rightarrow \delta(a) \leq \delta(ab)$.
   ii. es precisamente el algoritmo de división para los enteros, que establece que para todo $a, b \in \mathbb{Z}$, existe $q, r \in \mathbb{Z}$ tal que $a = bq + r$ con $0 \leq r < b$. Por lo tanto, $(\mathbb{Z}; +, \cdot)$ es un dominio euclidiano.
2. El dominio de integridad $(\mathbb{Z}[i]; +, \cdot)$ con la función $\delta(u) = |u|^2$ es un dominio euclidiano, ya que
   i. para todo $u, v \in \mathbb{Z}[i] \setminus \{0\}$, se tiene que
   $$\delta(uv) = |uv|^2 = |u|^2|v|^2 = \delta(u)\delta(v)$$
   entonces $\delta(u) = |u|^2 \leq |u|^2|v|^2 = \delta(uv) \Rightarrow \delta(u) \leq \delta(uv)$.
   ii. Tomemos $u, v \in \mathbb{Z}[i]$ con $v \neq 0$, y consideremos $\frac{u}{v} \in \mathbb{C}$, entonces existe $q \in \mathbb{Z}[i]$, tal que $|\frac{u}{v} - q| \leq \frac{\sqrt{2}}{2} < 1$, de modo que $|\frac{u}{v} - q| < |v|$ elevamos

al cuadrado la desigualdad y tenemos que $|\frac{u}{v} - q|^2 < |v|^2$. Si definimos $r := u - qv \in \mathbb{Z}[i]$, vemos que $\delta(r) < \delta(v)$.

Por lo tanto, $(\mathbb{Z}[i]; +, \cdot)$ es un dominio euclidiano.

Definición 2.9 (Campo)

La estructura $K = (A; +, \cdot)$, es un campo si es un anillo unitario, conmutativo y en el que todo elemento distinto de cero es una unidad, es decir, existe $a^{-1} \in K$ tal que $aa^{-1} = 1$.

Ejemplos.

1. El anillo $(\mathbb{Q}; +, \cdot)$ es un campo, ya que $\mathbb{Q}$ es un anillo unitario, conmutativo y además todo elemento de $\mathbb{Q}$ distinto de cero es una unidad.

2. El anillo $(\mathbb{R}; +, \cdot)$ es un campo, ya que $\mathbb{R}$ es un anillo unitario, conmutativo y además todo elemento de $\mathbb{R}$ distinto de cero es una unidad.

3. El anillo $(\mathbb{C}; +, \cdot)$ es un campo, ya que $\mathbb{C}$ es un anillo unitario, conmutativo y además todo elemento de $\mathbb{C}$ distinto de cero es una unidad.

4. El anillo $(\mathbb{Z}; +, \cdot)$ es un unitario, conmutativo, sin embargo la terna $(\mathbb{Z}; +, \cdot)$ no es un campo ya que las únicas unidades de $\mathbb{Z}$ son 1 y -1.

Proposición 2.5

Si K es un campo, entonces K es un dominio de integridad.

Demostración. Por hipótesis K es un anillo unitario y conmutativo por ser un campo, sólo hace falta demostrar que K no tiene divisores de cero.
Suponemos por absurdo que K tiene divisores de cero, entonces $ab = 0$, con $a, b \neq 0$ para todo $a, b \in K$, ya que $ab = 0$, se tiene que $a^{-1}ab = (a^{-1})0 = 0$ pero entonces, $0 = a^{-1}ab = (a^{-1}a)b = 1b = b$.
Lo que implica que $b = 0$, lo cual no es posible, ya que $b \neq 0$. Por lo tanto, K no tiene divisores de cero y en consecuencia K es un dominio de integridad. □

Proposición 2.6
Si K es un dominio de integridad finito, entonces K es un campo.

Demostración. Suponemos que $K = \{0, 1, a_1, a_2, \ldots, a_n\}$ son todos los elementos del dominio de integridad finito, tenemos que mostrar que para todo $a \in K$, con $a \neq 0$ existe $b \in K$ tal que $ab = 1$.
Consideremos los elementos $a1, aa_1, aa_2, \ldots, aa_n$ todos elementos de K. Afirmamos que todos son elementos distintos, ya que si $aa_i = aa_j$ para $i \neq j$, entonces $a(a_i - a_j) = 0$ como $a \neq 0$, se tiene que $a_i = a_j$ en contradicción con $i \neq j$. Además K no tiene divisores de cero, esto implica que ninguno de estos elementos sea cero. De modo que $1, a_1, a_2, \ldots, a_n$, son los elementos $K \setminus \{0\}$, en cualquier orden de tal manera que o bien $a1 = 1$ lo que implica que $a = 1$ o bien $aa_i = 1$ para algún i.
Luego $a \in K$ tiene inverso y por tanto a es una unidad de K y ya que K es unitario y conmutativo, se concluye que K es un campo. □

Proposición 2.7
Si p es un número primo, entonces $\mathbb{Z}/p$ es un campo.

Demostración. Basta demostrar que $\mathbb{Z}/p$ es un dominio de integridad. Anteriormente ya vimos que la terna $(\mathbb{Z}/p; +, \cdot)$ es un dominio de integridad, ya que $\mathbb{Z}/p$ no tiene divisores de cero. Y por la proposición 2.6 se tiene que $\mathbb{Z}/p$ es un campo. □

Notación. Cuando p es primo, el campo $\mathbb{Z}/p$ lo denotaremos por $\mathbb{F}_p$.

2.4 Ideales y Anillo cociente

En el módulo I sección 1.7 estudiamos los subgrupos especiales de un grupo dado, conocidos como subgrupos normales, cuyas clases laterales forman el grupo cociente G/H. Nos preguntamos entonces si para la estructura de anillos existen conceptos análogos. El rol de los ideales es comparable al de los subgrupos

normales estudiados en la teoría de grupos, ya que mediante éstos podemos construir el anillo cociente.

Definición 2.10 (Ideal izquierdo e Ideal derecho)
Sea A un anillo y sea I un subconjunto de no vacío A.

Decimos que I es un ideal izquierdo de A si:

1. para todo $i, j \in I$, se tiene que $i - j \in I$
2. para todo $i \in I$ y $r \in A$, se tiene que $ri \in I$.

Decimos que I es un ideal derecho de A si:

1. para todo $i, j \in I$, se tiene que $i - j \in I$
2. para todo $i \in I$ y $r \in A$, se tiene que $ir \in I$.

Claramente, podemos observar que tanto el ideal izquierdo como el ideal derecho son subanillos del anillo A. Adicionalmente, si I es ideal izquierdo y derecho a la vez, I se llama ideal bilátero. En adelante, usaremos la palabra ideal en lugar de ideal bilátero.

Definición 2.11 (Ideal)
Sea A un anillo y sea I un subconjunto no vacío de A. Decimos que I es un ideal del anillo A si:

1. para todo $i, j \in I$, se tiene que $i - j \in I$
2. para todo $i \in I$ y $r \in A$, se tiene que $ri, ir \in I$.

Ejemplos.

1. Sea $(\mathbb{Z}; +, \cdot)$ un anillo y sea $I = 3\mathbb{Z}$. I es un ideal del anillo $\mathbb{Z}$, ya que

   i. Para todo $i = 3x, j = 3y \in 3\mathbb{Z}$ se tiene que

   $$i - j = 3x - 3y = 3(x - y) \in 3\mathbb{Z}$$

   ii. Para todo $i = 3x \in 3\mathbb{Z}$ y todo $r \in \mathbb{Z}$ se tiene que

$$ri = r(3x) = 3(rx) \in 3\mathbb{Z}$$
$$ir = (3x)r = 3(xr) \in 3\mathbb{Z}$$

Por lo tanto, $3\mathbb{Z}$ es un ideal del anillo $\mathbb{Z}$.

2. Sea $(\mathbb{Z}; +, \cdot)$ un anillo y sea $I = n\mathbb{Z} = \{nx : x \in \mathbb{Z}\}$. I es un ideal del anillo $\mathbb{Z}$, ya que

   i. Para todo $i = nx, j = ny \in n\mathbb{Z}$ se tiene que

   $$i - j = nx - ny = n(x - y) \in n\mathbb{Z}$$

   ii. Para todo $i = nx \in n\mathbb{Z}$ y todo $r \in \mathbb{Z}$ se tiene que

   $$ri = r(nx) = n(rx) \in n\mathbb{Z}$$
   $$ir = (nx)r = n(xr) \in n\mathbb{Z}$$

   Por lo tanto, $n\mathbb{Z}$ es un ideal del anillo $\mathbb{Z}$.

3. Sea $(\mathbb{Q}; +, \cdot)$ un anillo y sea $I = \mathbb{Z}$. I no es un ideal del anillo $\mathbb{Q}$, ya que

   i. Para todo $i, j \in \mathbb{Z}$ se tiene que $i - j \in \mathbb{Z}$ pues la diferencia de números enteros es otro entero.

   ii. Para todo $i \in \mathbb{Z}$ y todo $r = \frac{m}{n} \in \mathbb{Q}$ se tiene que

   $$ri = \tfrac{m}{n}(i) = \tfrac{mi}{n} \notin \mathbb{Z}$$

   $$ir = (i)\tfrac{m}{n} = \tfrac{im}{n} \notin \mathbb{Z}$$

   Por lo tanto, $\mathbb{Z}$ no es un ideal del anillo $\mathbb{Q}$.

4. Sea $(A; +, \cdot)$ un anillo unitario, conmutativo y sea $a \in A$. El conjunto $\langle a \rangle = \{ar : r \in A\}$ es un ideal del anillo A, ya que

   i. Para todo $i = ar_1, j = ar_2 \in \langle a \rangle$ se tiene que

   $$i - j = ar_1 - ar_2 = a(r_1 - r_2) \in \langle a \rangle$$

   ii. Para todo $i \in \langle a \rangle$ y todo $r \in A$ se tiene que $ir = (ar_1)r = a(r_1 r) \in \langle a \rangle$ no hace falta mostrar $ri \in \langle a \rangle$ pues el anillo es conmutativo.

Por lo tanto, $\langle a \rangle$ es un ideal del anillo A. El ideal de la forma $\langle a \rangle$ se llama ideal generado por a.

Proposición 2.8

Sea A un anillo y sean I, J ideales del anillo A. Entonces;

1. la suma: $I + J = \{i + j : i \in I \text{ y } j \in J\}$ es un ideal de A,
2. el producto: $IJ = \left\{ \sum_{k=1}^{n} i_k j_k : i_k \in I \text{ y } j_k \in J \right\}$ es un ideal de A.

Demostración.

1. $I + J$ es un ideal, ya que
   1. Para todo $x = i_1 + j_1, y = i_2 + j_2 \in I + J$ se tiene que
   $$x - y = (i_1 + j_1) - (i_2 + j_2) = (i_1 - i_2) + (j_1 - j_2) \in I + J$$
   2. Para todo $x = i_1 + j_1 \in I + J$ y todo $r \in A$ se tiene que
   $$rx = r(i_1 + j_1) = ri_1 + rj_1 \in I + J$$
   $$xr = (i_1 + j_1)r = i_1 r + j_1 r \in I + J$$

   Por lo tanto, $I + J$ es un ideal.
2. IJ es un ideal, ya que
   1. Para todo $x = \sum_{k=1}^{n} i_k j_k, y = \sum_{k=1}^{n} i'_k j'_k \in IJ$ se tiene que
   $$x - y = \sum_{k=1}^{n} i_k j_k - \sum_{k=1}^{n} i'_k j'_k = \sum_{k=1}^{n} (i_k j_k - i'_k j'_k) \in IJ$$
   2. Para todo $x = \sum_{k=1}^{n} i_k j_k \in IJ$ y todo $r \in A$ se tiene que
   $$rx = \sum_{k=1}^{n} r(i_k j_k) = r \sum_{k=1}^{n} i_k j_k \in IJ$$

$$xr = \sum_{k=1}^{n} (i_k j_k) r = r \sum_{k=1}^{n} i_k j_k \in IJ$$

Por lo tanto, IJ es un ideal. □

A continuación estudiaremos ciertos tipos de ideales especiales.

Definición 2.12 (Ideal primo)
Sea A un anillo conmutativo y sea I un ideal de A. Decimos que I es un ideal primo, si para todo $a, b \in A$ tal que $ab \in I$, entonces $a \in I$ o $b \in I$.

Ejemplos.

1. El ideal $3\mathbb{Z}$ del anillo conmutativo $(\mathbb{Z}; +, \cdot)$ es un ideal primo, ya que para todo $a, b \in \mathbb{Z}$, tal que $ab \in 3\mathbb{Z}$, entonces $a \in 3\mathbb{Z}$ o $b \in 3\mathbb{Z}$. Por ejemplo, consideremos $6, 8 \in \mathbb{Z}$ se tiene que $6 \cdot 8 = 48 \in 3\mathbb{Z}$ y $6 \in 3\mathbb{Z}$.

2. El ideal generado $I = \langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$ del anillo conmutativo $(\mathbb{Z}/12; +, \cdot)$ es un ideal primo, ya que para todo $a, b \in \mathbb{Z}/12$, tal que $ab \in I$, entonces $a \in I$ o $b \in I$. Por ejemplo, consideremos $9, 10 \in \mathbb{Z}/12$ se tiene que $9 \cdot 10 = 90 = 6 \in I$ y $10 \in I$.

Nota. Un ideal I se dice que es un ideal propio cuando no coincide con todo el anillo A, es decir, $I \neq A$.

Definición 2.13 (Ideal maximal)
Sea A un anillo conmutativo y sea I un ideal propio de A. Decimos que I es un ideal maximal, si existe un ideal J de A, tal que si $I \subseteq J \subseteq A$, entonces $J = I$ o $J = A$.

Ejemplos.

1. El ideal propio $I = 3\mathbb{Z}$ del anillo conmutativo $(\mathbb{Z}; +, \cdot)$ es un ideal maximal, ya que los ideales del anillo $\mathbb{Z}$ son de la forma $n\mathbb{Z}$ para algún $n \in \mathbb{Z}$. Si consideremos $J = n\mathbb{Z}$, entonces se cumple que $3\mathbb{Z} \subsetneq n\mathbb{Z} \subsetneq \mathbb{Z}$.

Si $3\mathbb{Z} \subsetneq J$, entonces $n \mid 3$ tal que $3 = nk$ con $k \in \mathbb{Z}$, como 3 es primo se tiene que 3 es divisible para sí mismo o para 1, entonces

Si $n = 1$, se tiene que $J = \mathbb{Z}$.

Si $n = 3$, se tiene que $J = I$.

Por lo tanto, $3\mathbb{Z}$ es un ideal maximal del anillo $\mathbb{Z}$.

2. Los ideales propios $\langle 2\rangle$ y $\langle 3\rangle$ son ideales maximales del anillo conmutativo $(\mathbb{Z}/12; +, \cdot)$.

   Supongamos que existe el ideal J de $\mathbb{Z}/12$, tal que $\langle 2\rangle \subsetneq J \subsetneq \mathbb{Z}/12$, como

   $$\langle 2\rangle = \{2r : r \in \mathbb{Z}/12\} = \{0, 2, 4, 6, 8, 10\} \subsetneq J$$

   Supongamos ahora que el elemento $a \in \mathbb{Z}/12$ es impar y está en J, entonces se tiene que $2, 1 \in J$, de donde $J = \mathbb{Z}/12$. Por lo tanto, $\langle 2\rangle$ es un ideal maximal.

   Ahora supongamos que existe el ideal J' de $\mathbb{Z}/12$, tal que $\langle 3\rangle \subsetneq J' \subsetneq \mathbb{Z}/12$, como $\langle 3\rangle = \{3r : r \in \mathbb{Z}/12\} = \{0, 3, 6, 9\} \subsetneq J'$.

   Consideremos que el elemento $a \in \mathbb{Z}/12$ es par y está en J', entonces se tiene que $3, 2 \in J'$, de donde $J' = \mathbb{Z}/12$. Por lo tanto, $\langle 3\rangle$ es un ideal maximal.

Tal como se definen las clases laterales izquierdas y derechas en la teoría de grupo, ver la sección 1.6 del módulo I, podemos definir las clases laterales de un anillo. Si A es un anillo e I un ideal de A se define las clases laterales izquierdas como: $x + I = \{x + i : i \in I\}$ para $x \in A$, análogamente se define las clases laterales derechas de un anillo.

Notación. Escribiremos A/I para denotar el conjunto cociente de todas las clases laterales izquierdas determinadas por un ideal I.

Definición 2.14

Sea A un anillo y sea I un ideal de A. Se definen las operaciones suma y producto en el conjunto de las clases laterales izquierdas.

1. $(x + I) + (y + I) = (x + y) + I$
2. $(x + I)(y + I) = (xy) + I$

Proposición 2.9

Sea A un anillo y sea I un ideal de A, para todo $x, x', y, y' \in A$ se tiene:

1. $(x+y)+I = (x'+y')+I$
2. $(xy)+I = (x'y')+I$

Demostración.

1. Suponemos que $x+I = x'+I$ e $y+I = y'+I$, entonces $x-x' \in I$ e $y-y' \in I$ por ser I ideal.

   Ya que I es ideal podemos sumar sus elementos, entonces

   $$(x-x')+(y-y') = x-x'+y-y' = (x+y)-(x'-y')$$

   de modo que $(x+y)-(x'-y') \in I$, luego $(x+y)+I = (x'+y')+I$.

2. Suponemos que $x = x'+i$ e $y = y'+i_1$ con $i, i_1 \in I$, entonces

   $$xy = (x'+i)(y'+i_1) = x'(y'+i_1)+i(y'+i_1) = x'y'+x'i_1+iy'+ii_1$$

   Como I es ideal, entonces $s = x'i_1+iy'+ii_1 \in I$,

   $$xy = x'y'+s \;\Rightarrow\; xy+I = x'y'+s+I \;\Rightarrow\; xy+I = x'y'+I$$

□

Proposición 2.10

Sea I un ideal del anillo A y sean las operaciones suma y producto definidas en A/I. Entonces la terna $(A/I;+,\cdot)$ es un anillo.

Demostración. Veamos que $(A/I;+,\cdot)$ es un anillo.

1. El par $(A/I;+)$ es un grupo abeliano, ya que para todo $x+I, y+I, z+I \in A/I$ se tiene que

   i. La suma es cerrada, ya que $(x+I)+(y+I) = (x+y)+I$

ii. La suma es asociativa, ya que

$$\begin{aligned}[(x+I)+(y+I)]+(z+I) &= [(x+y)+I]+(z+I)\\ &= ((x+y)+z)+I\\ &= (x+(y+z))+I\\ &= x+I+[(y+z)+I]\\ &= x+I+[(y+I)+(z+I)]\end{aligned}$$

iii. Elemento neutro, está dado por $0+I \in A/I$, tal que

$$(a+I)+(0+I) = (a+0)+I = a+I$$

iv. Elemento inverso, para todo $x+I \in A/I$ existe su inverso $(x+I)^{-1} = -x+I \in A/I$, tal que $(x+I)+(-x+I) = (x+(-x))+I = 0+I$

v. La suma es conmutativa, ya que

$$(x+I)+(y+I) = (x+y)+I = (y+x)+I = (y+I)+(x+I)$$

Por lo tanto, $(A/I;+)$ es grupo abeliano.

2. El par $(A/I;\cdot)$ es un semigrupo, ya que para todo $x+I, y+I, z+I \in A/I$ se tiene que

i. El producto es cerrado, ya que $(x+I)(y+I) = (xy)+I$

ii. El producto es asociativo, ya que

$$\begin{aligned}[(x+I)(y+I)](z+I) &= [(xy)+I](z+I)\\ &= [(xy)z]+I\\ &= [x(yz)]+I\\ &= (x+I)[(yz)+I]\\ &= (x+I)[(y+I)(z+I)]\end{aligned}$$

Por lo tanto, $(A/I;\cdot)$ es semigrupo.

3. El producto es distributivo respecto a la suma, pues

$$\begin{aligned}(x+I)[(y+I)+(z+I)] &= (x+I)[(y+z)+I] \\ &= [x(y+z)]+I \\ &= (xy+xz)+I \\ &= (xy)+I+(xz)+I \\ &= (x+I)(y+I)+(x+I)(z+I)\end{aligned}$$

$$\begin{aligned}[(y+I)+(z+I)](x+I) &= [(y+z)+I](x+I) \\ &= [(y+z)x]+I \\ &= (yx+zx)+I \\ &= (yx)+I+(zx)+I \\ &= (y+I)(x+I)+(z+I)(x+I)\end{aligned}$$

Por lo tanto, $(A/I;+,\cdot)$ es un anillo. □

El anillo $(A/I;+,\cdot)$ que acabamos de probar, se denomina **anillo cociente**. Además el anillo A/I es unitario y conmutativo, ya que $1+I$ es el elemento unidad de A/I y además se cumple que $(0+I)(1+I)=(1+I)(0+I)$.

Ejemplo. Consideremos el anillo $(\mathbb{Z};+,\cdot)$ y sea $3\mathbb{Z}$ un ideal del anillo $\mathbb{Z}$. La terna $(\mathbb{Z}/3\mathbb{Z};+,\cdot)$ es un anillo cociente.

Una vez que $3\mathbb{Z}$ es un ideal del anillo $\mathbb{Z}$, lo siguiente es determinar los elementos del conjunto cociente $\mathbb{Z}/3\mathbb{Z}$, de modo que calculamos las clases laterales izquierdas.

$$\begin{aligned}\mathbb{Z}/3\mathbb{Z} &= \{x+3\mathbb{Z} : x\in\mathbb{Z}\} \\ 0+3\mathbb{Z} &= \{\ldots,-3,0,3,\ldots\} \\ 1+3\mathbb{Z} &= \{\ldots,-2,1,4,\ldots\} \\ 2+3\mathbb{Z} &= \{\ldots,-1,2,5,\ldots\} \\ 3+3\mathbb{Z} &= \{\ldots,-3,0,3,\ldots\} \\ 4+3\mathbb{Z} &= 1+3+3\mathbb{Z} = 1+3\mathbb{Z} \\ 5+3\mathbb{Z} &= 2+3+3\mathbb{Z} = 2+3\mathbb{Z}\end{aligned}$$

luego, $\mathbb{Z}/3\mathbb{Z} = \{0+3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z}\}$. Veamos que $\mathbb{Z}/3\mathbb{Z}$ es un anillo cociente.

1. El par $(\mathbb{Z}/3\mathbb{Z}; +)$ es un grupo abeliano, ya que para todo $0+3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z} \in \mathbb{Z}/3\mathbb{Z}$ se tiene que

   i. La suma es cerrada, ya que $(0+3\mathbb{Z}) + (1+3\mathbb{Z}) = (0+1)+3\mathbb{Z} = 1+3\mathbb{Z}$

   ii. La suma es asociativa, ya que

$$\begin{aligned}[(0+3\mathbb{Z}) + (1+3\mathbb{Z})] + (2+3\mathbb{Z}) &= [(0+1)+3\mathbb{Z}] + (2+3\mathbb{Z}) \\ &= ((0+1)+2)+3\mathbb{Z} \\ &= (0+(1+2))+3\mathbb{Z} \\ &= 0+3\mathbb{Z} + [(1+2)+3\mathbb{Z}] \\ &= (0+3\mathbb{Z}) + [(1+3\mathbb{Z}) + (2+3\mathbb{Z})]\end{aligned}$$

   iii. Elemento neutro, está dado por $0+3\mathbb{Z} \in \mathbb{Z}/3\mathbb{Z}$, tal que

$$(1+3\mathbb{Z}) + (0+3\mathbb{Z}) = (1+0)+3\mathbb{Z} = 1+3\mathbb{Z}$$

   iv. Elemento inverso, para todo $1+3\mathbb{Z} \in \mathbb{Z}/3\mathbb{Z}$ existe su inverso $(1+3\mathbb{Z})^{-1} = -1+3\mathbb{Z} \in \mathbb{Z}/3\mathbb{Z}$, tal que

$$(1+3\mathbb{Z}) + (-1+3\mathbb{Z}) = (1+(-1))+3\mathbb{Z} = 0+3\mathbb{Z}$$

   v. La suma es conmutativa, ya que

$$(0+3\mathbb{Z}) + (1+3\mathbb{Z}) = (0+1)+3\mathbb{Z} = (1+0)+3\mathbb{Z} = (1+3\mathbb{Z}) + (0+3\mathbb{Z})$$

   Por lo tanto, $(\mathbb{Z}/3\mathbb{Z}; +)$ es grupo abeliano.

2. El par $(\mathbb{Z}/3\mathbb{Z}; \cdot)$ es un semigrupo, ya que para todo $0+3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z} \in \mathbb{Z}/3\mathbb{Z}$ se tiene que

   i. El producto es cerrado, ya que $(0+3\mathbb{Z})(1+3\mathbb{Z}) = (0\cdot 1)+3\mathbb{Z} = 0+3\mathbb{Z}$

ii. El producto es asociativo, ya que

$$\begin{aligned}[(0+3\mathbb{Z})(1+3\mathbb{Z})](2+3\mathbb{Z}) &= [(0\cdot 1)+3\mathbb{Z}](2+3\mathbb{Z}) \\ &= [(0\cdot 1)2]+3\mathbb{Z} \\ &= [0(1\cdot 2)]+3\mathbb{Z} \\ &= (0+3\mathbb{Z})[(1\cdot 2)+3\mathbb{Z}] \\ &= (0+3\mathbb{Z})[(1+3\mathbb{Z})(2+3\mathbb{Z})]\end{aligned}$$

Por lo tanto, $(\mathbb{Z}/3\mathbb{Z};\cdot)$ es semigrupo.

3. El producto es distributivo respecto a la suma, pues

$$\begin{aligned}(0+3\mathbb{Z})[(1+3\mathbb{Z})+(2+3\mathbb{Z})] &= (0+3\mathbb{Z})[(1+2)+3\mathbb{Z}] \\ &= [0(1+2)]+3\mathbb{Z} \\ &= (0\cdot 1+0\cdot 2)+3\mathbb{Z} \\ &= (0\cdot 1)+3\mathbb{Z}+(0\cdot 2)+3\mathbb{Z} \\ &= (0+3\mathbb{Z})(1+3\mathbb{Z})+(0+3\mathbb{Z})(2+3\mathbb{Z})\end{aligned}$$

$$\begin{aligned}[(1+3\mathbb{Z})+(2+3\mathbb{Z})](0+3\mathbb{Z}) &= [(1+2)+3\mathbb{Z}](0+3\mathbb{Z}) \\ &= [(1+2)0]+3\mathbb{Z} \\ &= (1\cdot 0+2\cdot 0)+3\mathbb{Z} \\ &= (1\cdot 0)+3\mathbb{Z}+(2\cdot 0)+3\mathbb{Z} \\ &= (1+3\mathbb{Z})(0+3\mathbb{Z})+(2+3\mathbb{Z})(0+3\mathbb{Z})\end{aligned}$$

Por lo tanto, $(\mathbb{Z}/3\mathbb{Z};+,\cdot)$ es un anillo cociente.

Teorema 2.2

Sea A un anillo unitario y conmutativo, y sea I un ideal de A. I es ideal primo si y sólo si A/I es un dominio de integridad.

Demostración.

$\Rightarrow$) Si I es ideal primo, entonces A/I es un dominio de integridad.

Sean $a+I, b+I$ elementos de A/I, suponemos que

$$(a+I)(b+I) = ab+I = 0+I$$

entonces $ab \in I$, como I es ideal primo entonces $a \in I$ o $b \in I$, lo que implica que $a + I = 0 + I$ o $b + I = 0 + I$, por lo tanto A/I no tiene divisores de cero y en consecuencia A/I es un dominio integridad.

$\Leftarrow$) Si A/I es un dominio de integridad, entonces I es ideal primo.
Sean $a + I, b + I$ elementos de A/I, suponemos que $(a + I)(b + I) = 0 + I$ entonces $a + I = 0 + I$ o $b + I = 0 + I$, lo que implica que o bien $a \in I$ o $b \in I$, por lo tanto I es ideal primo. □

Teorema 2.3

Sea A un anillo unitario y conmutativo, y sea I un ideal de A. I es ideal maximal si y sólo si A/I es un campo.

Demostración.

$\Rightarrow$) Si I es ideal maximal, entonces A/I es un campo.
Supongamos que $b \in A$ pero $b \notin I$, entonces probemos que $b + I \neq 0 + I$ tiene inverso.
Consideremos el conjunto $B = \{br + a : r \in A, a \in I\}$, de modo que B es un ideal de A que contiene propiamente a I, en efecto ya que dados $x, y \in B$ y para todo $r \in A$ se cumple que $x - y \in B$ y $xr \in B$ por tanto B es ideal de A, además $I \subsetneq B$ ya que dado $a \in I$, se tiene que $a = b \cdot 0 + a \in B$.
Por hipótesis, I es ideal maximal entonces $B = A$ y como A es anillo unitario se tiene que $1 \in B$, de tal manera que $1 = bc + a'$ con $a' \in I$, luego

$$1 + I = bc + a' + I = bc + I = (b + I)(c + I)$$

esto muestra que el elemento $b + I$ tiene inverso y por lo tanto A/I es un campo.

$\Leftarrow$) Si A/I es un campo, entonces I es ideal maximal.
Suponemos que J es un ideal de A que contiene propiamente a I, y sea $b \in J$ pero $b \notin I$. Ya que A/I es un campo, dado $b + I \in A/I$ existe su inverso tal que $1 + I = (b + I)(c + I)$. Como $b \in J$, entonces $bc \in J$, ya que

$$1 + I = (b + I)(c + I) = bc + I$$

Ya que $1 + I = bc + I$, se tiene que $1 - bc + I = 0 + I$ de aquí $1 - bc \in I$ y como $I \subsetneq J$ se sigue que $1 - bc \in J$, luego $1 = (1 - bc) + bc \in J$, de modo que $1 \in J$, por lo tanto $J = A$, ya que para todo $r \in A$ se tiene que $r = r \cdot 1 \in J$ se sigue que $A \subseteq J$, la contención inversa es trivial. Se concluye que I es ideal maximal. □

2.5 Campo de fracciones

Recordemos que un dominio de integridad es un anillo unitario, conmutativo sin divisores de cero, por otra parte, un campo se define como un anillo unitario, conmutativo en el cual todo elemento distinto de cero tiene inverso. Estas definiciones semejantes entre ambas estructuras, motiva a preguntarse si es posible que dado un dominio de integridad, se pueda generar un campo a partir de elementos del DI dado.

Se sabe que $\mathbb{Z}$ es un DI, pero $\mathbb{Z}$ no es un campo. Por otro lado $\mathbb{Q}$ es campo y los elementos del conjunto $\mathbb{Q}$, lo podemos expresar como cocientes (fracciones) de números enteros, pero $\mathbb{Z}$ es un DI, esto da una idea que si es posible construir un campo, a partir de un dominio integridad.

Definición 2.15
Sea A un dominio de integridad, se define el producto cartesiano A como:

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

Asumimos que el par (a, b) representa un cociente de la forma $\frac{a}{b}$. Por ejemplo, sabemos que los enteros $\mathbb{Z}$ son un dominio de integridad, entonces el producto cartesiano $\mathbb{Z} \times \mathbb{Z} = \{(a, b) : a, b \in \mathbb{Z}\}$, de modo que dado el par $(9, 2)$ representa el cociente $\frac{9}{2} \in \mathbb{Q}$. Nótese, que el par $(a, 0)$ no representa ningún cociente en $\mathbb{Q}$, ya que no existe la división entre 0.

Notación. Dado que la segunda coordenada del par (a, b), nunca será cero. Denotaremos por S al subconjunto de $A \times A \setminus \{0\}$ de modo que:

$$S = \{(a, b) : a, b \in A,\ b \neq 0\}$$

Definición 2.16

Sea A un dominio de integridad y sean $(a,b),(c,d) \in S$, se define en S la siguiente relación: $(a,b) \sim (c,d)$ si y sólo si $ad = bc$

Si $A = \mathbb{Z}$, dados $(6,7),(18,21) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$, se tiene que $(6,7) \sim (18,21)$, ya que $(6)(21) = (7)(18)$ por lo cuál la definición es aceptable.

Proposición 2.11

La relación "$\sim$" es una relación de equivalencia.

Demostración. La relación "$\sim$" es reflexiva, simétrica y transitiva.

Reflexividad. Para todo $(a,b) \in S$, se cumple que $(a,b) \sim (a,b)$, ya que $ab = ab$ esto último por le hecho de que A es DI.

Simetría. Sea $(a,b),(c,d) \in S$, suponemos que $(a,b) \sim (c,d)$, entonces $ad = bc$ y ya que A es un DI, se tiene que $cb = da$, por lo tanto $(c,d) \sim (a,b)$.

Transitividad. Sean $(a,b),(c,d),(e,f) \in S$, suponemos que $(a,b) \sim (c,d)$ y $(c,d) \sim (e,f)$, entonces $ad = bc$ y $cf = de$, de estas igualdades y del hecho que A es un DI, se tiene que $bcf = bde \Rightarrow adf = bde \Rightarrow afd = bed$, luego aplicando la ley de cancelación por la derecha se tiene que $af = be$, por lo tanto $(a,b) \sim (e,f)$. □

Dado que $\sim$ es una relación de equivalencia, ésta particiona a S en clases de equivalencia. Escribiremos $[a,b]$ para representar la clase de equivalencia de $(a,b) \in S$.

Notación. El conjunto cociente $S/\sim$ lo denotaremos por A_S.

Ya que A_S es el conjunto cociente formado por todas las clases de equivalencia, se tiene que

$$A_S = \{[a,b] : (a,b) \in S\}$$

Una vez que hemos definido el conjunto cociente de las clases de equivalencia, si queremos mostrar que A_S es un campo, es preciso definir operaciones entre elementos de A_S.

Definición 2.17
Sean $[a,b],[c,d]$ clases de A_S, se definen:

1. suma: $[a,b]+[c,d]=[ad+bc,bd]$
2. producto: $[a,b][c,d]=[ac,bd]$

Proposición 2.12
San $a,b,c,d,a',b',c',d' \in A$. Si $[a,b]=[a',b']$ y $[c,d]=[c',d']$, entonces

1. $[a,b]+[c,d]=[a',b']+[c',d']$
2. $[a,b][c,d]=[a',b'][c',d']$

Demostración.

1. De nuestra hipótesis se deduce que $[ad+bc,bd]=[a'd'+b'c',b'd']$, lo que es equivalente a demostrar $(ad+bc)b'd'=bd(a'd'+b'c')$.

   Dado que $[a,b]=[a',b']$ y $[c,d]=[c',d']$, entonces $ab'=ba'$ y $cd'=dc'$, con estas igualdades y con el hecho de que A es DI, se tiene que

$$\begin{aligned}(ad+bc)b'd' &= adb'd'+bcb'd'\\ &= ab'dd'+bb'cd'\\ &= ba'dd'+bb'dc'\\ &= bda'd'+bdb'c'\\ &= bd(a'd'+b'c')\end{aligned}$$

2. De nuestra hipótesis se deduce que $[ac,bd]=[a'c',b'd']$, lo que es equivalente a demostrar $(ac)b'd'=bd(a'c')$.

Dado que $[a,b] = [a',b']$ y $[c,d] = [c',d']$, entonces $ab' = ba'$ y $cd' = dc'$, con estas igualdades y con el hecho de que A es DI, se tiene que

$$(ac)b'd' = ab'cd' = ba'dc' = bd(a'c') \qquad \square$$

Proposición 2.13

Sea A un dominio de integridad y sea $A_S = \{[a,b] : (a,b) \in S\}$. La terna $(A_S; +, \cdot)$ es un campo.

Demostración. Tenemos que mostrar que: $(A_S; +)$ es un grupo abeliano, $(A_S; \cdot)$ es un grupo abeliano y que el producto es distributivo respecto a la suma.

1. El par $(A_S; +)$ es un grupo abeliano, ya que para todo $[a,b], [c,d], [e,f] \in A_S$ se tiene que,

   i. La suma es cerrada, se cumple por definición.

   ii. La suma es asociativa, ya que

   $$\begin{aligned}([a,b] + [c,d]) + [e,f] &= [ad + bc, bd] + [e,f] \\ &= [adf + bcf + bde, bdf] \\ &= [adf + b(cf + de), bdf] \\ &= [a,b] + [cf + de, df] \\ &= [a,b] + ([c,d] + [e,f])\end{aligned}$$

   iii. Existe el elemento neutro en A_S, dado por $[0,1]$ tal que,

   $$[a,b] + [0,1] = [a(1) + b(0), b(1)] = [a,b]$$

   iv. Elemento inverso, para todo $[a,b] \in A_S$ existe su inverso $[a,b]^{-1} = [-a,b] \in A_S$ tal que, $[a,b] + [-a,b] = [ab + (-ab), bb] = [0, bb] = [0,1]$.

   v. La suma es conmutativa, ya que

   $$[a,b] + [c,d] = [ad + bc, bd] = [cb + da, db] = [c,d] + [a,b]$$

   Por lo tanto, $(A_S; +)$ es un grupo abeliano.

2. El par $(A_S;\cdot)$ es un grupo abeliano, ya que para todo $[a,b],[c,d],[e,f] \in A_S$ se tiene que,

   i. El producto es cerrado, se cumple por definición.

   ii. El producto es asociativo, ya que

   $$([a,b][c,d])[e,f] = [ac,bd][e,f] = [ace,bdf] = [a(ce),b(df)]$$
   $$= [a,b][ce,df] = [a,b]([c,d][e,f])$$

   iii. Existe el elemento neutro en A_S, dado por $[1,1]$ tal que,

   $$[a,b][1,1] = [a(1),b(1)] = [a,b]$$

   iv. Elemento inverso, supongamos $[b,a] \in A_S$ es el inverso $[a,b] \in A_S$ no nulo. Veamos que $[a,b][b,a] = [1,1]$.

   Como $[a,b][b,a] = [ab,ba]$, pero ya que A es DI , tenemos $ab = ba$ se puede escribir como $ab(1) = ba(1)$ de modo que $(ab,ba) \sim (1,1)$, sigue que $[ab,ba] = [1,1]$ por lo tanto $[a,b][b,a] = [1,1]$.

   v. El producto es conmutativo, ya que

   $$[a,b][c,d] = [ac,bd] = [ca,db] = [c,d][a,b]$$

   Por lo tanto, $(A_S;\cdot)$ es un grupo abeliano.

3. El producto es distributivo respecto a la suma, ya que

$$\begin{aligned}[a,b]([c,d]+[e,f]) &= [a,b][cf+de,df] \\ &= [acf+ade,bdf] \\ &= [ac,bd]+[ae,bf] \\ &= [a,b][c,d]+[a,b][e,f]\end{aligned}$$

Por lo tanto, $(A_S;+,\cdot)$ es un campo. □

La estructura que acabamos de probar, se denomina **campo de fracciones**.

Ejemplos.

1. El campo de fracciones de $\mathbb{Z}$ es $\mathbb{Q}$, ya que $\mathbb{Z}$ es un dominio de integridad y sea el subconjunto $S = \mathbb{Q} = \{(a,b) : a,b \in \mathbb{Z},\ b \neq 0\}$. De donde se obtiene el conjunto de clases $\mathbb{Z}_S = \{[a,b] : (a,b) \in \mathbb{S}\}$ y junto con las operaciones suma y producto de clases definido en $\mathbb{Z}_S$, se tiene que la terna $(\mathbb{Z}_S; +, \cdot)$ es el campo de fracciones de $\mathbb{Z}$.

2. El campo de fracciones de $\mathbb{Z}[i]$ es $\mathbb{Q}[i] = \{a + ib : a,b \in \mathbb{Q}\}$, ya que $\mathbb{Z}[i]$ es un dominio de integridad y sea el subconjunto $\mathbb{Q}[i] = \{(x,y) : x,y \in \mathbb{Z}[i],\ y \neq 0\}$. De donde se obtiene el conjunto de clases $\mathbb{Z}[i]_{\mathbb{Q}[i]} = \{[x,y] : (x,y) \in \mathbb{Q}[i]\}$ y con las operaciones suma y producto de clases definidas en $\mathbb{Z}[i]_{\mathbb{Q}[i]}$, se tiene que la terna $(\mathbb{Z}[i]_{\mathbb{Q}[i]}; +, \cdot)$ es el campo de fracciones de $\mathbb{Z}[i]$.

2.6 Clausura

Con los módulos I y II hemos querido resaltar las características de dos estructuras algebraicas pilares de investigación en el Álgebra Abstracta. Se han detallado definiciones y propiedades de ambas estructuras, puntualizando en los resultados más relevantes.

Se espera que, con esta guía de estudios, que cubre los contenidos mínimos de la asignatura de Álgebra Abstracta de la carrera de Matemática de la ESPOCH, los estudiantes puedan entender las estructuras algebraicas de grupo y anillo, y le animen a profundizar sobre las aplicaciones de esta hermosa teoría.

Otras lecturas que pudiera seguir el lector interesado en el tópico son: la teoría de módulos y la teoría de Galois, de mucha relevancia dentro del estudio de la matemática ver ([Be19], [Bh94], [Cl84], [Du03], [Ga17], [La05]).

Bibliografía

[Al21] Alcock, L. (2021). *How to think about Abstract Alagebra*. Oxord University Press.

[Ar08] Arenas, L. (2008). *Anillos y Cuerpos*.

[Ayr04] Ayres F. & Jaisingh L. (2004). *Theory and problems of Abstract Algebra*. The McGraw-Hill Companies.

[Be19] Beachy, J., & Blair, W. (2019). *Abstract algebra*. Waveland Press.

[Bh94] Bhattacharya, P., Jain, S., & Nagpaul, S. (1994). *Basic abstract algebra*. Cambridge University Press.

[Bo22] Bóna, M. (2022). *Combinatorics of Permutations*. University Cambridge Massachusetts.

[Cl84] Clark, A. (1984). *Element of Abstract Algebra*. Courier Coorporation.

[Do96] Dorronsoro, J. & Hernández, E. (1996). *Números, grupos y anillos*. Addison-Wesley Iberoamericana España, S.A

[Du03] Dummit, D. & Foote, R. (2003). *Abstract Algebra*. University of Vermont.

[Ell92] Ellis, G. (1992). *Rings and fields*. Oxford University Press.

[Ga17] Gallian, J. (2017). *Contemporary Abstract Algebra.* Cengage Learning.

[Her96] Herstein, I. (1996). *Abstract Algebra*. Macmillan Publishing Company.

[Hum96] Humphreys, J. (1996). *A course in group theory*. Oxford University Press.

[Ju12] Judson, T (2012). *Abstract Algebra Theory and Applications*. Stephen F. Austin State University.

[La05] Lang, S. (2005). *Graduate Texts in Mathematics Algebra*. Springer.

[Ri96] Rivero, F. (1996). *Algebra: Estructura Algebraicas*. Universidad de Los Andes.

[Ro00] Rotman, J. (2000). *A first course in Abstract Algebra*. University of Illinois.

[Ta01] Tábara, J. L. (2001). *Introducción a la teoría de anillos*.

[Za07] Zaldívar, F. (2007). *Introducción a la teoría de grupos*. Reverte.

[Za14] Zaldívar, F. (2014). *Introducción a la teoría de números*. Fondo de Cultura Económica.