Fundamentos de matemáticas

Ricardo Ariel Pastrán Ramírez
Pedro Hernán Zambrano Ramírez

Facultad de Ciencias
Sede Bogotá

UNIVERSIDAD
NACIONAL
DE COLOMBIA

Fundamentos de matemáticas

Fundamentos de matemáticas

Ricardo A. Pastrán
Pedro H. Zambrano

UNIVERSIDAD
NACIONAL
DE COLOMBIA
Bogotá, D. C., Colombia, 2025

Primera edición, 2025

ISBN 978-958-505-975-7 (papel)
ISBN 978-958-505-976-4 (digital)

Edición
Alejandro Cano Moreno
Coordinación de Publicaciones - Facultad de Ciencias - Sede Bogotá
coorpub_fcbog@unal.edu.co

Corrección de estilo
Gloria Agudelo Molina

Diseño de carátula
Damián Crofort

Maqueta LaTeX
Camilo Cubides

Editado en Bogotá, D. C., Colombia

Catalogación en la publicación Universidad Nacional de Colombia

Pastrán Ramírez, Ricardo Ariel, 1979-
Fundamentos de matemáticas / Ricardo A. Pastrán, Pedro H. Zambrano. -- Primera edición. -- Bogotá: Universidad Nacional de Colombia. Facultad de Ciencias: Coordinación de Publicaciones Facultad de Ciencias, 2025.
1 recurso en línea (435 páginas): ilustraciones, diagramas. -- (Colección Notas de clase. Matemáticas)

Incluye referencias bibliográficas e índice
ISBN 978-958-505-976-4 (digital)

1. Matemáticas -- Enseñanza superior -- Problemas, ejercicios, etc. 2. Lógica matemática -- Estudio y enseñanza -- Ejercicios y problemas 3. Planificación de lecciones 4. Proposición (Lógica) 5. Cálculo proposicional 6. Teoría de la demostración 7. Inducción (Matemáticas) 8. Cálculo de predicados 9. Teorema de la deducción 10. Teoría de conjuntos -- Enseñanza superior -- Problemas, ejercicios, etc. 11. Funciones de conjuntos 12. Relaciones entre (Matemáticas) 13. Números cardinales 14. Teoría de los números 15. Aritmética -- Fundamentos -- Problemas, ejercicios, etc. I. Zambrano Ramírez, Pedro Hernán, 1981-, autor II. Título III. Serie

CDD-23 511.0711 / 2025

Contenido

Prólogo

Este libro fue escrito con el propósito de servir como guía y material de consulta del curso de primer semestre *Fundamentos de Matemáticas*, obligatorio para los estudiantes de las carreras de Matemáticas, Ciencias de la Computación y Estadística de la Facultad de Ciencias de la Universidad Nacional de Colombia, sede Bogotá. Este puede ser tomado por estudiantes de otras carreras de nuestra Universidad como, por ejemplo, Física, Ingenierías, Filosofía o, inclusive, Diseño Gráfico.

Lo que originó el presente texto, además de un viejo deseo de los autores, fue la necesidad de tener un libro para el curso de *Fundamentos de Matemáticas*, escrito en castellano, que esté adaptado al bagaje académico real con el que ingresan al pregrado nuestros estudiantes y que además les ayude a posicionarse en un nivel adecuado para tomar cursos más avanzados. Este libro no sería el primero de Fundamentos de Matemáticas de nuestra Facultad de Ciencias. El libro del profesor Fernando Zalamea [9], publicado en el 2007, es un excelente texto, de una gran riqueza académica, que lo hace una lectura obligatoria no solo de los cursos básicos, sino también de cursos más avanzados a lo largo de la carrera de Matemáticas. Su contenido está basado en el programa del curso que estaba vigente hasta antes de la última reforma del 2008, la cual dividió el antiguo curso de Fundamentos en los actuales cursos de *Fundamentos de Matemáticas* y de *Sistemas Numéricos*. Sin embargo, en nuestra experiencia dictando el curso nos hemos dado cuenta de que muchos de nuestros estudiantes no llegan con las bases adecuadas para poder aprovechar completamente el texto del profesor Zalamea. Adicionalmente, los libros guías que han sido utilizados en este curso en los últimos años están escritos en inglés ([1, 5]) y, aunque más temprano que tarde un estudiante de matemáticas debe leer textos matemáticos en ese idioma, esto puede añadir una dificultad adicional a los estudiantes de primer semestre debido a la deficiencia en el conocimiento de una segunda lengua por parte de los bachilleres colombianos. Estos textos, de los que hemos hecho referencia, no se pueden seguir al pie de la letra porque presuponen que los estudiantes ya tienen experiencias significativas, en cursos como Cálculo Diferencial, o algún tipo de "madurez matemática". Este no es el caso de la mayoría de nuestros estudiantes de primer semestre.

Es así como, con el propósito de que nuestros estudiantes tengan un mejor acceso a todo el conocimiento contenido en el curso y, además, que también sirva como guía para los profesores que lo impartan, tuvimos la idea de que cada lección de este libro, en la medida de lo posible, correspondiera a una clase magistral de dos horas. Creemos que esto puede facilitarle a los estudiantes una lectura más práctica de cada tema y al profesor la preparación de las clases. Aunque esta manera de presentar los temas podría mantener muy rígida la cantidad de material cubierto en cada lección, nuestra prioridad fue siempre realizar una exposición detallada y explícita de cada tópico sin dejarnos abrumar por esta limitación; aún más, lo presentado en estas notas supera lo que en términos reales se presenta en la clase. De hecho, es muy posible que la presentación del contenido de algunas lecciones lleve más o menos tiempo dependiendo, no solo de la agilidad del profesor exponiendo los temas, sino también de las demandas de los estudiantes o la rapidez con que ellos aprehendan las ideas. La elección de cada uno de los temas contenidos en las lecciones fue discutida y basada en nuestra propia experiencia dictando el curso. Adicionalmente, cada lección del libro está acompañada de una buena cantidad de ejemplos, que complementan y aclaran la teoría desarrollada, y de ejercicios que han sido escogidos cuidadosamente.

Queremos agradecer en primer lugar a los profesores con quienes tomamos el curso de Fundamentos de Matemáticas, cuando empezamos nuestro tránsito por este mundo inagotable de conocimiento, la profesora Myriam Margarita Acevedo y el profesor Marco Fidel Pita (QEPD). Ellos, dedicados y eminentes maestros, fueron quienes nos llevaron a experimentar esas primeras epifanías que nos cautivaron al mundo de las matemáticas. Agradecemos a la profesora Blanca Cecilia Marroquín, quien nos ha dado ánimo en la escritura de estas notas y no ha dejado de aconsejarnos sobre la manera como podemos orientar varios de los temas propios de este curso.

Agradecemos mucho a nuestras colegas, Margarita Ospina y Milena Cortés, y a nuestros colegas, John Jaime Rodríguez y Claudio Rodríguez, por su generosidad al haber leído versiones preliminares de estas notas y habernos indicado sugerencias y comentarios valiosos que ayudaron a mejorar este texto. Además, les agradecemos también a los profesores y profesoras del Departamento de Matemáticas, por todo el trabajo que se realizó de manera conjunta (preparación de los talleres y examénes parciales conjuntos) en la Universidad Nacional de Colombia, sede Bogotá, cuando hemos dictado este curso. Varios de los ejercicios que incluímos en este texto tienen su origen en este trabajo conjunto.

También, queremos agradecer a nuestros estudiantes del curso de Fundamentos de Matemáticas en la Universidad Nacional de Colombia, quienes nos han indicado algunos errores tipográficos e imprecisiones que aparecieron en versiones preliminares de nuestro documento. Agradecemos también a los profesores César Gómez, Mauricio Bogoya y Juan Carlos Hernández, en su momento directores del Departamento de Matemáticas de nuestra Universidad, por el apoyo brindado al facilitarnos el tiempo para la elaboración de este documento.

Prefacio para el docente

El presente texto recoge gran parte de la experiencia de los autores dictando el curso de Fundamentos de Matemáticas y las sugerencias que han surgido en discusiones con nuestros colegas. Enseñar el curso de Fundamentos requiere un tacto especial de parte del docente para cubrir las necesidades de los estudiantes porque ellos, además de estar dando el salto del colegio a la disciplina universitaria, están por primera vez cara a cara con la rigurosidad matemática de la cual no se puede escapar si realmente queremos que aprendan matemáticas. Teniendo en cuenta esto, pretendimos prioritariamente que nuestro libro en cada una de sus lecciones mantuviera una gran riqueza en su contenido y rigor. Es así como en muchas lecciones el tema expuesto sobrepasó lo que realmente puede ser abordado en una clase. Esto implica que cada docente, haciendo uso de su libertad de cátedra, podrá decidir qué temas tocará en el salón de clase y cuáles dejará como ejercicio de lectura; lo cual motiva el estudio individual.

Este texto está dividido en 26 lecciones, las cuales corresponden al número total de sesiones magistrales que se imparten en un semestre de 16 semanas, con dos sesiones por semana, porque los autores por lo regular hacemos tres exámenes parciales de este curso y una sesión exclusiva para preguntas y discusiones antes de cada examen, completando así 32 sesiones. Vale la pena aclarar que estas no son las únicas sesiones en las que los estudiantes hacen preguntas y pueden abrir discusiones. De hecho, mantener el diálogo abierto durante todo el semestre con los estudiantes y ofrecer atención individual de tal manera que ellos puedan recibir la retroalimentación necesaria es vital. Todos podemos aprender de nuestros errores si nos los señalan y nos sugieren formas de solucionarlos.

Los seis temas grandes que estudiamos en este curso son los siguientes:

1. Lógica clásica. Lecciones 1 a la 5.
2. Estrategias de demostración. Lecciones 6 a la 9.
3. Teoría intuitiva de conjuntos. Lecciones 10 a la 13.
4. Relaciones. Lecciones 14 a la 18.
5. Funciones. Lecciones 19 a la 23.
6. Cardinales. Lecciones 24 a la 26.

Sugerimos que aquellas sublecciones que aparece con asterisco (*) pueden ser omitidas en el salón de clase y dejadas como ejercicio de lectura para los estudiantes, según el criterio del docente.

En la última parte del libro presentamos dos apéndices. En el Apéndice A hacemos un pequeño esbozo de los axiomas de cuerpo y orden de los números reales. Este tema es también estudiado en las primeras semanas del curso de Cálculo Diferencial en una Variable, curso que usualmente los estudiantes estarían viendo de manera paralela a Fundamentos de Matemáticas. Durante el desarrollo del curso no estudiamos en detalle estos temas, puesto que presuponemos que los estudiantes o bien ya han tomado el curso de Cálculo Diferencial en una Variable o bien están viendo dicho curso de manera paralela con Fundamentos de Matemáticas y ya han cubierto ese tema. El propósito de incluir este apéndice en el texto es simplemente hacerlo lo más autocontenido posible.

En el Apéndice B presentamos los sistemas deductivos proposicional y de predicados clásicos. Estos temas hacían parte del programa oficial de Fundamentos de Matemáticas desde la reforma del 2008 hasta hace un par de años. Por tener un registro de estos, decidimos incluirlos en las presentes notas a manera de apéndice. A cambio de los sistemas deductivos, como resultado de la evaluación constante de nuestro curso con nuestros colegas, hemos acordado incluir en el curso los temas de Principio de Inducción Matemática (Lección 9) en la parte II, puesto que es una estrategia de demostración muy útil en todos los cursos de la carrera, y Definiciones recursivas (Lección 20) en la parte V, como aplicación del concepto de función. Vale la pena aclarar que tanto Inducción matemática como Definiciones recursivas son temas que se estudian con mayor profundidad en el curso de Sistemas Numéricos y que tener un primer contacto con estos temas desde Fundamentos de Matemáticas facilitará el acceso de los estudiantes a estas ideas.

Prefacio para el estudiante

Una de las preguntas más recurrentes que nos formulan a quienes decidimos estudiar matemáticas es: ¿qué es lo que estudian? La mayoría de las veces no es fácil explicar lo que estudiamos o lo que hacemos los matemáticos porque el imaginario popular, alimentado apenas por las matemáticas del colegio o por prejuicios sociales, se aleja bastante de las matemáticas universitarias. Responder esta pregunta refiriéndonos a los cursos que están en los pénsums de las carreras de matemáticas no ayuda mucho. También podríamos afirmar que las matemáticas son el fruto más excelso del pensamiento humano o, decir que, si uno las entiende, son realmente apasionantes, pero esto tampoco aclara nada. Un buen intento es recordarles una palabra que seguramente escucharon durante su educación secundaria: *teorema*. En efecto, los matemáticos, basados en sus intuiciones, abstracciones e identificación de patrones, crean o descubren teoremas pero, antes de ser matemáticos, mientras estudian matemáticas, lo que hacen es estudiar teoremas que otros matemáticos han creado o descubierto a lo largo de los siglos. Por ejemplo, uno de los más famosos es el Teorema de Pitágoras que fue descubierto por los Pitagóricos alrededor del siglo VI antes de Cristo.

La característica más importante de los teoremas es que la afirmación contenida es verdadera y es verdadera para todos y por siempre. Semejante cualidad, generalmente, no se establece así porque sí. Todo teorema debe tener una justificación o, mejor dicho, una demostración que nos deje claro que sí es verdad, es decir, un argumento contundente en el que no haya absolutamente ninguna sombra de duda acerca de su veracidad. Muchas veces entender lo que afirma un teorema no solo nos puede llevar a sorprender, sino que también nos invita a disfrutar de seguir un poderoso y elegante argumento que justifica la verdad de ese teorema eterno. Esto es solo comparable con los más bellos poemas, porque además de estar muy bien escritos, respetando todas las reglas de puntuación y de gramática, también se concatenan conceptos y resultados previos de maneras, muchas veces, asombrosas, sin perder el rigor matemático, dando así lugar a las ideas más fascinantes que han producido las mentes más brillantes de las matemáticas. En efecto, la imaginación, la creatividad y la intuición son tanto o, inclusive, más importantes en matemáticas como el rigor y el orden para comunicar nuestras ideas.

La mayoría de matemáticos aceptamos argumentos que están apoyados en la "lógica clásica", que es el tema principal de la primera parte de este libro. Quizás para algunos la lógica es solo sentido común pero no hay duda de que vale la pena precisar conceptos como proposiciones, conectivos lógicos, negación de proposiciones, predicados y cuantificadores. Todo esto nos permitirá hacer una exposición formal de las "estrategias de demostración", segunda parte del libro, que comúnmente son utilizadas por la comunidad matemática. Las ideas y conceptos descritos en estas dos primeras partes del libro conforman la base más profunda de las matemáticas.

Las matemáticas modernas están soportadas por la noción de *conjunto*. Es por esto que en la tercera parte del libro, "Teoría intuitiva de conjuntos", abordamos este concepto absolutamente fundamental para iniciar el camino por las matemáticas. En la cuarta parte estudiaremos las "relaciones" entre conjuntos y, como caso particular de estas, las "funciones", en la quinta parte. En la última parte de este libro, sobre "cardinales", se aclara la noción de contar los elementos que tiene un conjunto en la que se usan las funciones inyectivas y biyectivas.

Una de nuestras mayores prioridades en la elaboración de este libro fue escribir con un gran nivel de detalle las demostraciones de los teoremas contenidos y fuimos mucho más minuciosos en las primeras lecciones. En consecuencia, a medida que avanzamos en el libro dejamos abiertos algunos detalles de los argumentos presentados, los cuales pueden ser completados por los mismos estudiantes. Adicionalmente, vale la pena resaltar que las matemáticas no se aprenden contemplativamente, leyendo libros o viendo videos en internet. Las matemáticas se aprenden haciendo ejercicios, como los que aparecen al final de cada lección de este libro. Resolver ejercicios le permite al estudiante entender mejor los conceptos y detectar sus falencias; además de adquirir intuición y facilidad en la escritura matemática.

En resumen, la mejor respuesta a la pregunta inicial de este prefacio es: lo que estudian los estudiantes de matemáticas es lo que se enseña en los salones de nuestros edificios de matemáticas y, para tener una mejor noción de estas, y éxito en la carreras con alto contenido en matemáticas, no hay duda de que lo mejor es tomar inicialmente el curso de Fundamentos de Matemáticas.

Parte I

Lógica clásica

Lección *uno*

Proposiciones

En las primeras lecciones de estas notas haremos una introducción informal al cálculo proposicional clásico. Desde este punto de vista no estudiaremos la estructura interna de las afirmaciones sino que nos centraremos en la forma como están conectadas con otras, haciendo énfasis en reglas de formación de nuevas proposiciones a partir de proposiciones más sencillas.

1.1. ¿Qué es una proposición?

Entenderemos una *proposición*, desde el punto de vista clásico, como una afirmación que es verdadera o es falsa en un contexto determinado.

En general, especialmente en Filosofía, se entiende que las *proposiciones* son afirmaciones del lenguaje natural de las que podemos decir si son verdaderas o si son falsas en un contexto determinado, sin ambigüedades. Pero en general, en matemáticas no es de interés trabajar con el lenguaje natural sino con objetos en una estructura matemática fija.

Algunos textos, por ejemplo [8], no definen explícitamente lo que es una proposición, justamente para evitar discusiones que no se alejan del lenguaje natural y que están muy lejos de lo que realmente nos interesa en matemáticas.

En resumen, toda proposición es verdadera o falsa. 'Verdadero' y 'Falso' son llamados *valores de verdad* y son asignados a cada una de las proposiciones. Nótese que no existe otra opción distinta para cualquier proposición mas que tener o valor de verdad "verdadero" o tener valor de verdad "falso". Este principio es conocido como *principio del tercero excluido* porque una tercera opción para el valor de verdad de cualquier proposición no es posible.

Una conjetura, por ejemplo, es una afirmación matemática de la que, habiendo fijado un contexto, no se ha podido demostrar si es verdadera o si es falsa. Con seguridad, alguna de estas opciones debe ocurrir. Ante esta situación, algunas veces los matemáticos suponemos que dicha conjetura es verdadera y exploramos consecuencias de este supuesto. En este caso le hemos asignado un valor de verdad y de esta manera las conjeturas son, en efecto, proposiciones.

Ejemplos 1.1.1. Las siguientes afirmaciones son proposiciones:

1. A Pepe le gustan los autos azules.

2. Micifú es un gato pardo.

3. La Lógica estudia métodos para discernir cuando un argumento es válido o no.

4. La Universidad Nacional de Colombia es la principal Universidad Pública de Colombia.

5. La luna es de queso verde.

6. $2 + 2 = 5$.

7. Si hoy es martes entonces hoy hay clase de Fundamentos de Matemáticas.

8. La suma de la medida de los ángulos internos de cualquier triángulo es 180 grados.

Ejemplos 1.1.2. No son proposiciones:

1. ¿Micifú es un gato gris? Es una interrogación.

2. ¡Hoy será un bello día! Es una exclamación.

3. ¡Haz la tarea! Es una orden.

4. Ojalá me vaya bien en el curso. Es una expresión desiderativa, ya que expresa un deseo.

5. $2 + 2$. No es una proposición puesto que no se está diciendo nada sobre este objeto (no hay verbo) y por tanto ni siquiera es una afirmación.

6. $x^2 + 5x + 6 = 1$. No es proposición porque como x es una variable, representa un elemento indeterminado y, por tanto, el valor de verdad de esta afirmación depende del reemplazo que se haga de x.

Debemos tener especial cuidado con la dependencia de lugar y tiempo de algunas afirmaciones porque pueden modificar su valor de verdad. Por ejemplo, la afirmación "hoy es martes". Dependiendo del día de la semana esta afirmación va a ser verdadera o falsa (solo será verdadera si se enuncia un día martes). En general, lo importante para este tipo de afirmaciones es que podemos evitar estas ambigüedades si tenemos el cuidado de precisar un lugar y tiempo específicos. Así, tomarán un valor de verdad fijo.

En estas primeras lecciones de estas notas nos apoyamos un poco en proposiciones de nuestro lenguaje "natural" puesto que todos estamos más familiarizados con este tipo de afirmaciones. Sin embargo, poco a poco iremos pasando a trabajar con proposiciones en matemáticas las cuales evidentemente no tienen componentes ni de lugar ni de tiempo y, por lo tanto, no se deben hacer consideraciones al respecto.

En este documento representaremos (simbolizaremos) proposiciones arbritrarias por medio de letras griegas (α, β, γ, $\cdots$). Por ejemplo:

α : "A Pepe le gustan los autos azules".
β : "Micifú es un gato pardo".
γ : "La Lógica estudia métodos para discernir cuando un argumento es válido o no".

Nótese que en esta escritura usamos el símbolo dos puntos (:) para indicar que la letra griega nombra a la proposición que escribimos a cotinuación entre comillas. Reservamos el símbolo de igualdad (=) para expresar que lo que se encuentra a la izquierda y a la derecha del símbolo son el mismo objeto matemático. Por ejemplo, $2 + 2 = 4$. A lo largo del texto estudiaremos diferentes objetos matemáticos y puntualizaremos el significado de la igualdad en esos contextos.

1.2. Reglas para la construcción de nuevas proposiciones

Ahora que sabemos intuitivamente qué es una proposición, vamos a definir de manera más precisa este concepto. Para hacerlo, daremos unas reglas para construir nuevas proposiciones a partir de proposiciones más simples consideradas previamente.

1.2.1. Negación

Dada una proposición α, la *negación* de α corresponde a afirmaciones del tipo:

1. *No es cierto* que α,
2. *No es verdad* que α,
3. *No es el caso* que α,
4. *No se tiene* que α,
5. *Es falso* que se tenga α,

o afirmaciones similares. La negación de α se denota por $\neg(\alpha)$.

Decimos que la negación de una proposición α es *verdadera* únicamente cuando α es falsa. Es decir, $\neg(\alpha)$ toma el valor de verdad contrario al asignado a α. Esto se resume en la siguiente tabla:

α	$\neg(\alpha)$
V	F
F	V

Ejemplos 1.2.1.

1. A pepe *no* le gustan los autos azules.
2. *No es cierto que* Micifú es un gato pardo.
3. *Es falso que* la Lógica estudia métodos para discernir cuándo un argumento es válido o no.
4. La luna *no* es de queso verde.
5. *No se tiene que* $2 + 2 = 5$.

1.2.2. Conjunción

Dadas unas proposiciones α y β, la *conjunción* de α y β corresponde a afirmaciones del tipo:

1. α *y* β,
2. Es el caso que α *y* β,
3. Se tiene que α *y* β,
4. α *pero* β (el "pero" se usa para indicar que β tiene un sentido *negativo* respecto de α),

o afirmaciones similares. La conjunción de α y β es denotada por $(\alpha) \wedge (\beta)$.

Decimos que la conjunción $(\alpha) \wedge (\beta)$ es *verdadera* únicamente cuando α y β son verdaderas simultáneamente. En cualquier otro caso, se tomará como *falsa*. Es decir, $(\alpha) \wedge (\beta)$ es falsa en el caso de que alguna (o las dos) de esas afirmaciones α y β sean falsas.

α	β	$(\alpha) \wedge (\beta)$
V	V	V
V	F	F
F	V	F
F	F	F

Ejemplos 1.2.2.

1. Perencejo estudia Matemáticas *y* Sutano trabaja en una oficina.
2. Micifú es un gato pardo *y* Ruffo es un perro labrador.
3. A Juan le gusta ver películas *pero* José prefiere escuchar música.

1.2.3. Disyunción

Dadas unas proposiciones α y β, la *disyunción en el lenguaje natural* de α y β corresponde a afirmaciones del tipo:

1. α o β,

2. Es el caso que α o β,

3. Se tiene que α o β,

4. O bien α o bien β,

o afirmaciones similares. La disyunción de α y β es denotada por $(\alpha) \vee (\beta)$.

Decimos que la disyunción $(\alpha) \vee (\beta)$ es *falsa* únicamente cuando α y β son falsas simultáneamente. En cualquier otro caso, se tomará como *verdadera*. Es decir, $(\alpha) \vee (\beta)$ es verdadera en el caso de que alguna (o las dos) de esas afirmaciones α y β sean verdaderas.

α	β	$(\alpha) \vee (\beta)$
V	V	V
V	F	V
F	V	V
F	F	F

Vale la pena mencionar que este conectivo $\vee$ no corresponde exactamente a la disyunción (o) de nuestro lenguaje natural puesto que esta muchas veces excluye la posibilidad de que tanto α como β sean verdaderas simultáneamente. En efecto, es común ver en textos el conectivo *y/o* que corresponde a la disyunción que acabamos de definir. Esta disyunción es también llamada *disyunción inclusiva* y la que más es usada en nuestro lenguaje es conocida como *disyunción exclusiva*. El uso del *y/o* prueba que el significado de la disyunción (o) en nuestro lenguaje es exclusivo la mayoría de las veces. Por ejemplo, en los anuncios o en el menú de un restaurante de comidas rápidas se pueden encontrar opciones para escoger por cierto precio un combo donde la bebida es gaseosa *o* té helado. Esta disyunción se entiende en el sentido de que solo podemos escoger *una sola bebida* y claramente excluye la posibilidad de tomar las dos.

También, algunas otras veces una disyunción en nuestro lenguaje *no excluye* la posibilidad de que se den las dos opciones que se plantean; por ejemplo, en la afirmación: "El Gobierno dará un subsidio a aquellas personas que estudien o trabajen", entendemos que basta que una persona cumpla al menos una de estas opciones, podría darse la posibilidad de tenerse las dos al tiempo, para que el Gobierno le dé el subsidio a aquella persona. Es en este sentido en el que entendemos la disyunción que usamos en matemáticas. Tener clara esta distinción es crucial para un buen entendimiento de las matemáticas; de lo contrario, el significado de la disyunción (o) en nuestro idioma puede infectar la noción que estamos construyendo.

Ejemplos 1.2.3.

1. La luna es de queso verde *o* $2+2=5$.
2. Firulais es un perro maltés *o* Micifú es un gato pardo.
3. Martha toma el trabajo *o* lo rechaza.
4. O bien un número complejo es algebraico *o* es trascendente.

1.2.4. Condicional

Dadas unas proposiciones α y β, el *condicional* con antecedente α y consecuente β corresponde a afirmaciones del tipo:

1. α implica β,
2. β, si α,
3. si α entonces β,
4. si α, β,
5. α solo si β,
6. α es condición suficiente para β,
7. β es condición necesaria para α,

o afirmaciones similares. Dicho condicional es denotado por $(\alpha) \to (\beta)$.

Decimos que el condicional $(\alpha) \to (\beta)$ es *falso* únicamente en el caso que α es verdadera y β es falsa. En cualquier otro caso, se tomará como *verdadero*. Es decir, de una verdad no podemos concluir una falsedad.

α	β	$(\alpha) \to (\beta)$
V	V	V
V	F	F
F	V	V
F	F	V

Una crítica que se hace a la manera como es definido el condicional desde este punto de vista es que realmente no está codificando, en el sentido estricto, situaciones de la forma causa-consecuencia. Note que afirmaciones de la forma: “Si Bogotá es la capital de Colombia entonces la nieve es blanca”, resultan verdaderas dado que tanto antecedente como consecuente son verdaderas. Sin embargo, el hecho de la nieve ser blanca no es consecuencia de Bogotá ser la capital de Colombia. Para efectos prácticos de lo que pretendemos, dar una introducción a la manera como se argumenta en matemáticas, es suficiente el desarrollo clásico que describimos en estas notas. Desde este punto de vista, entendemos el condicional de manera que de una afirmación verdadera no podemos concluir otra afirmación que sea falsa, a pesar de que a priori sepamos que la tesis β no es consecuencia de tener α, como en el ejemplo que consideramos líneas arriba.

Ejemplos 1.2.4.

1. $2 = 2 \cdot 1$ *implica* que 2 es un número par.
2. *Si* amas a Dios *entonces* amas a tu hermano.
3. *Si* 3 y 5 son números pares *entonces* $3 + 5$ es par.
4. Que el agua alcance una temperatura de $100^o C$ es *condición suficiente* para que hierva.
5. Que $23 > 2$ sea entero primo es *condición suficiente* para que 23 sea impar.
6. Que 51^2 sea entero impar es *condición necesaria* para que 51 sea un entero impar (según el criterio dado anteriormente, esto es lo mismo que decir que si 51 es un entero impar *entonces* 51^2 es un entero impar; **no** se debe interpretar de otra manera).

Observación 1.2.5 (Variantes del condicional)**.** Si consideramos el condicional $(\alpha) \to (\beta)$, algunas variantes que consideramos son las siguientes:

1. $(\beta) \to (\alpha)$ (recíproca),
2. $(\neg(\beta)) \to (\neg(\alpha))$ (contrarrecíproca),
3. $(\neg(\alpha)) \to (\neg(\beta))$ (contraria).

Ejemplo 1.2.6. Consideremos la afirmación: “Si hoy es martes, entonces hoy hay clase de Fundamentos de Matemáticas”, la cual es un condicional de la forma $(\alpha) \to (\beta)$ tomando

α: “Hoy es martes”
y
β: “Hoy hay clase de Fundamentos de Matemáticas”.

La *recíproca* de $(\alpha) \to (\beta)$ corresponde a $(\beta) \to (\alpha)$, que en nuestro lenguaje es la afirmación: “Si hoy hay clase de Fundamentos de Matemáticas, entonces hoy es martes”.

La afirmación *contrarrecíproca* de este condicional es $(\neg(\beta)) \to (\neg(\alpha))$, que corresponde a la afirmación: “Si hoy no hay clase de Fundamentos de Matemáticas, entonces hoy no es martes”.

La *contraria* de $(\alpha) \to (\beta)$ corresponde a $(\neg(\alpha)) \to (\neg(\beta))$, que en nuestro lenguaje corresponde a la afirmación: “Si hoy no es martes, entonces hoy no hay clase de Fundamentos de Matemáticas”.

1.2.5. Bicondicional

Dadas dos proposiciones α y β, el *bicondicional* de α y β en nuestro lenguaje corresponde a afirmaciones del tipo:

1. α si y solo si β,
2. α es equivalente a β,
3. α implica a β y β implica a α,
4. α es condición suficiente y necesaria para β,

o afirmaciones similares. Denotamos el bicondicional de α y β como $(\alpha) \leftrightarrow (\beta)$.

Decimos que $(\alpha) \leftrightarrow (\beta)$ es *verdadero* en aquellos casos donde α y β toman el mismo valor de verdad. En otras palabras, $(\alpha) \leftrightarrow (\beta)$ es falso en los casos donde α y β toman valores de verdad diferentes.

α	β	$(\alpha) \leftrightarrow (\beta)$
V	V	V
V	F	F
F	V	F
F	F	V

Ejemplos 1.2.7.

1. a es un entero par *si y solo si* a^2 es un entero par.

2. Que a número real sea diferente de cero es *condición suficiente y necesaria* para que $a^2 > 0$.

3. Que un entero no sea par es *equivalente* a que dicho entero sea impar.

1.3. Ejercicios

Ejercicio 1.3.1. Si la proposición $((\alpha) \wedge (\beta)) \longrightarrow (\gamma)$ es falsa, dé, si es posible, el valor de verdad de las siguientes proposiciones, justificando su respuesta:

1. $((\beta) \vee (\gamma)) \wedge (\alpha)$.

2. $((\gamma) \wedge (\delta)) \longrightarrow (\alpha)$.

3. $((\beta) \vee (\delta)) \longrightarrow (\alpha)$.

4. $((\neg(\alpha)) \wedge (\beta)) \longrightarrow ((\gamma) \wedge (\delta))$.

5. $(\neg ((\gamma) \longrightarrow (\delta))) \wedge ((\alpha) \wedge (\beta)))$.

6. $((\alpha) \vee (\delta)) \wedge (\gamma)$.

7. $(\neg(((\gamma) \wedge (\alpha)) \vee (\beta))) \longrightarrow ((\delta) \vee (\alpha)))$.

Ejercicio 1.3.2. Encuentre una proposición que involucre los conectivos $\neg$, $\wedge$ y $\vee$ que tenga la siguiente tabla de verdad:

α	β	¿ ?
V	V	F
V	F	V
F	V	F
F	F	V

Ejercicio 1.3.3. Encuentre una proposición que involucre los conectivos $\neg$, $\wedge$ y $\vee$ que tenga la siguiente tabla de verdad:

α	β	¿ ?
V	V	F
V	F	V
F	V	V
F	F	F

Lección *dos*

Equivalencia semántica

2.1. Lenguaje lógico

Diremos que una proposición está expresada en *lenguaje lógico* si su escritura está expresada usando los símbolos definidos en la Lección 1 ($\neg$, $\wedge$, $\vee$, $\rightarrow$ y $\leftrightarrow$, los cuales denominaremos *conectivos*). El último conectivo utilizado en la formación de una proposición que no sea simple se denomina *conectivo principal* de dicha proposición.

Para asignarle un valor de verdad a una proposición arbitraria es esencial escribir tal proposición en lenguaje lógico. Para esto debemos determinar cuáles son las proposiciones más simples que la conforman, en otras palabras, determinar aquellas afirmaciones de las que podemos decir si son verdaderas o falsas, y que no involucran ninguna de las reglas de formación de nuevas proposiciones descritas al final de la Lección 1. Estas afirmaciones más simples las denotaremos con letras minúsculas $p, q, r, s, t, \cdots$, las cuales denominaremos *letras proposicionales* o *proposiciones simples*.

A partir de las proposiciones simples y utilizando las reglas de formación de nuevas proposiciones estudiadas atrás, podemos construir nuevas proposiciones que aumentan en nivel de complejidad. Hemos escogido denotar cualquier proposición con letras griegas α, β, γ, δ, $\cdots$. Consecuentemente, estas proposiciones más complejas son denotadas con letras griegas. Por ejemplo: $\alpha = (p) \wedge (q)$ y $\beta = ((p) \vee (q)) \rightarrow (r)$.

Denominaremos una proposición no simple por el nombre de su conectivo principal. Por ejemplo, diremos que $\alpha = (p) \wedge (q)$ es una *conjunción* y $\beta = ((p) \vee (q)) \rightarrow (r)$ es un *condicional*.

Ejemplo 2.1.1. En este ejemplo escribiremos en lenguaje lógico una proposición dada en español. Consideremos la proposición: "Si Joan estudia y no pospone hacer el trabajo, entonces obtendrá una buena calificación". Lo primero que hacemos es determinar aquellas proposiciones que no involucran conectivos (afirmaciones que denominamos *simples*), las cuales denotaremos con letras proposicionales. En este caso, tenemos las siguientes afirmaciones simples:

p: "Joan estudia",
q: "Joan pospone hacer el trabajo",
r: "Joan obtendrá una buena calificación".

Vemos que la proposición completa es un *condicional*, donde el antecedente es una *conjunción* (Joan estudia y no pospone hacer el trabajo) y el consecuente es una afirmación simple (Joan obtendrá una buena calificación, que habíamos denotado por r). Analizando el antecedente, vemos que se trata de la conjunción de una afirmación simple (Joan estudia, que habíamos denotado por p) y la negación de una afirmación simple (Joan pospone hacer el trabajo, que habíamos denotado por q); así que dicho antecedente queda denotado en lenguaje lógico por $(p) \wedge (\neg(q))$. De esta manera, el condicional que corresponde a la afirmación dada inicialmente corresponde a $((p) \wedge (\neg(q))) \rightarrow (r)$.

2.2. Importancia de los paréntesis

La importancia de los paréntesis radica en que evitan ambigüedades al construir proposiciones complejas, como veremos más adelante en el ejemplo 2.2.4. Sin embargo, para simplificar y no recargar la notación, algunos de ellos los podemos suprimir si no hay lugar a confusiones. Eliminaremos los paréntesis en los siguientes casos:

1. Paréntesis que encierren letras proposicionales.
2. Paréntesis que encierren una negación.
3. Paréntesis que encierren letras griegas.

Ejemplo 2.2.1. Para ilustrar la anterior regla 3., vemos que las proposiciones $(\alpha) \wedge (\beta)$, $(\alpha) \vee (\beta)$, $(\alpha) \rightarrow (\beta)$, $(\alpha) \leftrightarrow (\beta)$, y $\neg(\alpha)$ podemos escribirlas simplemente como $\alpha \wedge \beta$, $\alpha \vee \beta$, $\alpha \rightarrow \beta$, $\alpha \leftrightarrow \beta$ y $\neg\alpha$ sin riesgo de ambigüedades.

Ejemplo 2.2.2. Consideremos la siguiente proposición: "Si Pepe pide unas papas y Juan una hamburguesa, entonces la cuenta va a salir barata". Identificamos primero las afirmaciones que no son construidas a partir de las reglas de formación de nuevas proposiciones descritas anteriormente (es decir, las proposiciones más simples), las cuales denotaremos con las siguientes letras minúsculas:

p: "Pepe pide unas papas",
q: "Juan pide una hamburquesa",
r: "La cuenta va a salir barata".

Analizando la manera como está escrita esta proposición, vemos que corresponde a un condicional donde su antecedente corresponde a la conjunción: “Pepe pide unas papas y Juan una hamburguesa”, y cuyo consecuente corresponde a la proposición: “La cuenta va a salir barata”. El antecedente de esta proposición corresponde a la conjunción de “Pepe pide unas papas” y “Juan pide una hamburguesa’, así que lo simbolizamos como $(p) \wedge (q)$; eliminando los paréntesis de las letras proposicionales obtenemos $p \wedge q$. Entonces la forma como debemos simbolizar esta proposición es $(p \wedge q) \rightarrow (r)$. Finalmente, eliminando los paréntesis que encierran a la proposición simple r obtenemos $(p \wedge q) \rightarrow r$.

A continuación, mostraremos otros ejemplos sobre las reglas de eliminación de paréntesis.

Ejemplos 2.2.3.

1. p, q y r son proposiciones al ser letras proposicionales.

2. $\neg(p)$ es proposición al ser negación de la letra proposicional p. Aplicando las reglas de eliminación de paréntesis, podemos simplificarla a $\neg p$.

3. $(\neg p) \wedge (q)$ es proposición, ya que es la conjunción de las proposiciones $\neg p$ y q. Aplicando las reglas de eliminación de paréntesis podemos simplificarla a $\neg p \wedge q$; en este caso, se sobreentiende que la negación solo alcanza a la letra proposicional p. Nótese que es muy diferente considerar $\neg(p \wedge q)$.

4. $(\neg p \wedge q) \vee (r)$ es proposición, ya que es la disyunción de las proposiciones $\neg p \wedge q$ y r. Aplicando las reglas de eliminación de paréntesis podemos simplificarla a $(\neg p \wedge q) \vee r$.

5. $(q) \vee (r)$ es proposición al ser disyunción de las letras proposicionales q y r. Aplicando las reglas de eliminación de paréntesis podemos simplificarla a $q \vee r$.

6. $(\neg p) \wedge (q \vee r)$ es proposición al ser la conjunción de las proposiciones $\neg p$ y $q \vee r$. Aplicando las reglas de eliminación de paréntesis podemos simplificarla a $\neg p \wedge (q \vee r)$.

Siempre debemos tener cuidado con el orden que empleamos en la construcción de las proposiciones, porque el sentido de las afirmaciones podría cambiar dependiendo de dicho orden que consideremos. Observe que las proposiciones 4. y 6. en los Ejemplos 2.2.3 de la lección anterior, aunque son parecidas, fueron construídas en orden diferente. La manera como se interpretan estas afirmaciones, es decir los valores de verdad que toman, va a ser diferente. Por esta razón, es muy importante el uso de paréntesis con el fin de determinar el orden en que fue construída cada proposición.

Ejemplo 2.2.4. Consideremos las proposiciones $(p \wedge q) \vee r$ y $p \wedge (q \vee r)$. Veamos la tabla de verdad de cada una de estas proposiciones.

p	q	r	$p \quad \wedge \quad (q \vee r)$	$(p \wedge q) \quad \vee \quad r$
V	V	V	V V	V V

En este primer caso, tanto p, q y r son verdaderas, por lo tanto, $q \vee r$ es verdadera (porque alguna de las dos proposiciones q y r es verdadera) y $p \wedge q$ es verdadera (porque tanto p como q son verdaderas). Por consiguiente, $p \wedge (q \vee r)$ es verdadera (p y $q \vee r$ son verdaderas en este caso) y $(p \wedge q) \vee r$ es verdadera también (al menos una de las dos proposiciones $p \wedge q$ y r es verdadera, en particular ambas lo son en este caso).

p	q	r	$p \quad \wedge \quad (q \vee r)$	$(p \wedge q) \quad \vee \quad r$
V	V	F	V V	V V

En este segundo caso, p y q son verdaderas y r es falsa, por lo tanto, $q \vee r$ es verdadera (porque alguna de las dos proposiciones q y r es verdadera, en este caso q) y $p \wedge q$ es verdadera (porque tanto p como q son verdaderas). Por consiguiente, $p \wedge (q \vee r)$ es verdadera (p y $q \vee r$ son verdaderas en este caso) y $(p \wedge q) \vee r$ es verdadera también (al menos una de las dos proposiciones $p \wedge q$ y r es verdadera, en este caso $p \wedge q$).

p	q	r	$p \quad \wedge \quad (q \vee r)$	$(p \wedge q) \quad \vee \quad r$
V	F	V	V V	F V

En este tercer caso, p y r son verdaderas y q es falsa, por lo tanto, $q \vee r$ es verdadera (porque alguna de las dos proposiciones q y r es verdadera, en este caso r) y $p \wedge q$ es falsa (alguna de las proposiciones

p y q es falsa, en este caso q es falsa). Por consiguiente, $p \wedge (q \vee r)$ es verdadera (p y $q \vee r$ son verdaderas en este caso) y $(p \wedge q) \vee r$ es verdadera también (al menos una de las dos proposiciones $p \wedge q$ y r es verdadera, en este caso r).

p	q	r	p	$\wedge$	$(q \vee r)$	$(p \wedge q)$	$\vee$	r
V	F	F		F	F	F	F	

En este cuarto caso, q y r son falsas y p es verdadera, por lo tanto, $q \vee r$ es falsa (porque ambas proposiciones q y r son falsas) y $p \wedge q$ es falsa (alguna de las proposiciones p y q es falsa, en este caso q es falsa). Por consiguiente, $p \wedge (q \vee r)$ es falsa (alguna de las proposiciones p y $q \vee r$ es falsa, en este caso lo es $q \vee r$) y $(p \wedge q) \vee r$ es falsa (tanto $p \wedge q$ como r son falsas).

p	q	r	p	$\wedge$	$(q \vee r)$	$(p \wedge q)$	$\vee$	r
F	V	V		F	V	F	V	

En este quinto caso, q y r son verdaderas pero p es falsa, por lo tanto, $q \vee r$ es verdadera (porque alguna de las dos proposiciones q y r es verdadera, en este caso en particular ambas lo son) y $p \wedge q$ es falsa (porque alguna de las proposiciones p y q es falsa, en este caso p). Por consiguiente, $p \wedge (q \vee r)$ es falsa (alguna de las proposiciones p y $q \vee r$ es falsa, en este caso por lo menos p lo es) y $(p \wedge q) \vee r$ es verdadera (al menos una de las dos proposiciones $p \wedge q$ y r es verdadera, en este caso r lo es).
Nótese que en este caso, sin importar el valor de verdad de $q \vee r$, la proposición $p \wedge (q \vee r)$ ya es falsa porque p lo es.

Observemos que en este caso, los valores de verdad de $p \wedge (q \vee r)$ y de $(p \wedge q) \vee r$ son diferentes, por lo tanto, en cuanto a su interpretación lógica (semántica) son diferentes. Esta es la principal razón del por qué los paréntesis son muy importantes al escribir una proposición en notación lógica, porque nos permite evitar ambigüedades en la escritura de estas que pueden llevar a confusiones en su interpretación.

Ejercicio 2.2.5. Completar la tabla de verdad de las proposiciones $p \wedge (q \vee r)$ y $(p \wedge q) \vee r$.

2.3. Tautologías, contradicciones y contingencias

A continuación haremos una clasificación de las proposiciones con respecto a los valores de verdad que toman.

Definición 2.3.1 (Tautología)**.** Sea α una proposición. Decimos que α es una *tautología* si y solo si al analizar sus valores de verdad, en cualquier caso siempre es verdadera.

Observación 2.3.2. Si p es una letra proposicional, no es tautología, ya que a priori se supone que puede tomar valor de verdad verdadero o valor de verdad falso.

Ejemplo 2.3.3. Sean α y β proposiciones. Veamos que $\alpha \to (\beta \to \alpha)$ es una tautología.
En el caso de que α sea falsa, como es el antecedente del condicional $\alpha \to (\beta \to \alpha)$, en ese caso $\alpha \to (\beta \to \alpha)$ es verdadera.
En el caso de que α sea verdadera, nótese que el condicional $\beta \to \alpha$ va a ser siempre verdadero sin importar el valor de verdad de β (puesto que el único caso en el que $\beta \to \alpha$ sería falsa es cuando β es verdadera y α es falsa, y en este caso α es verdadera); luego, como tanto antecedente como consecuente de $\alpha \to (\beta \to \alpha)$ son verdaderos entonces dicho condicional es verdadero también en este caso.
En cualquier caso $\alpha \to (\beta \to \alpha)$ es verdadera, es decir, es una tautología.

Ejemplo 2.3.4. Consideremos la proposición $(\alpha \wedge \beta) \to \neg\alpha$. Nótese que en el caso de que α y β sean verdaderas, $\alpha \wedge \beta$ es verdadera y $\neg\alpha$ tiene que ser falsa; como el antecedente de $(\alpha \wedge \beta) \to \neg\alpha$ es verdadero y su consecuente es falso, entonces dicho condicional es falso en este caso. Como hay al menos un caso donde $(\alpha \wedge \beta) \to \neg\alpha$ es falsa, entonces no es tautología.

Definición 2.3.5 (Contradicción)**.** Sea α una proposición. Decimos que α es una *contradicción* si y solo si al analizar sus valores de verdad, en cualquier caso siempre es falsa.

Ejemplo 2.3.6. Sea α una proposición. Veamos que $\alpha \wedge \neg\alpha$ es una contradicción.

En el caso de que α sea verdadera, $\neg\alpha$ tiene que ser falsa, por lo tanto, la conjunción $\alpha \wedge \neg\alpha$ es falsa en este caso (porque una de las afirmaciones en dicha conjunción es falsa).
Si sucede que α es falsa, como es una de las proposiciones en la conjunción $\alpha \wedge \neg\alpha$ entonces dicha conjunción es falsa.
En cualquier caso $\alpha \wedge \neg\alpha$ es falsa, por lo tanto, es una contradicción.

Ejemplo 2.3.7. Consideremos la proposición $(\alpha \wedge \beta) \to \neg\alpha$ dada en el ejemplo 2.3.4. Nótese que cuando α sea falsa, sin importar el valor de verdad de β, $\alpha \wedge \beta$ es falsa. Como en este caso el antecedente de $(\alpha \wedge \beta) \to \neg\alpha$ es falso, entonces dicho condicional es verdadero. Como hay un caso donde $(\alpha \wedge \beta) \to \neg\alpha$ es verdadero, entonces no es contradicción.

Definición 2.3.8 (Contingencia). Sea α una proposición. Decimos que α es una *contingencia* si y solo si no es ni tautología ni contradicción; es decir, hay al menos un caso donde es verdadera y un caso donde es falsa.

Ejemplo 2.3.9. Sean α y β proposiciones. El condicional $(\alpha \wedge \beta) \to \neg\alpha$ es contigencia, dado que en el ejemplo 2.3.4 vimos que hay un caso donde es falsa y en el ejemplo 2.3.7 vimos que hay un caso donde es verdadera.

2.4. Equivalencia semántica

Hay algunos pares de proposiciones que a pesar de escribirse diferente, en todos los casos, ambas proposiciones toman exactamente los mismos valores de verdad; es decir, tienen el mismo significado semántico.

Definición 2.4.1 (Equivalencia semántica). Decimos que α y β son *equivalentes semánticamente* (o simplemente *equivalentes*), lo que denotaremos por $\alpha \equiv \beta$ si y solo si el bicondicional $\alpha \leftrightarrow \beta$ es tautología.

Observación 2.4.2. Hay autores (e.g., [1]) que denotan la equivalencia semántica con el símbolo $\Leftrightarrow$. Por la experiencia que hemos tenido dictando el curso, algunos estudiantes confunden el símbolo $\Leftrightarrow$ (que es usado para relacionar dos proposiciones) con el conectivo $\leftrightarrow$, por lo que preferimos usar el símbolo $\equiv$ en estas notas. Adicionalmente, en textos de *lógica matemática* y *teoría de modelos* (por ejemplo

[4]) esta noción es denotada por $=\!\!|\!\!\models$. Los símbolos $\Leftrightarrow$ y $=\!\!|\!\!\models$ no serán usados en este documento.

Ejemplo 2.4.3 (Doble negación). Sea α una proposición. Tenemos que $\alpha \equiv \neg\neg\alpha$:

α	$\neg$	$\neg$	α
V	V	F	

En este primer caso, estamos suponiendo que el valor de verdad de α es verdadero. Por lo tanto, $\neg\alpha$ es falso. Así, la negación de $\neg\alpha$ que es $\neg\neg\alpha$ sería verdadera.

α	$\neg$	$\neg$	α
F	F	V	

En este segundo caso, estamos suponiendo que el valor de verdad de α es falso. Por lo tanto, $\neg\alpha$ es verdadero. Así, la negación de $\neg\alpha$ que es $\neg\neg\alpha$ sería falsa.

En resumen, la tabla de verdad de α y $\neg\neg\alpha$ es las siguiente:

α	$\neg$	$\neg$	α
V	V	F	
F	F	V	

Nótese que en cada uno de los casos tanto α como $\neg\neg\alpha$ toman los mismos valores de verdad. Por lo tanto, son equivalentes (lo que denotamos por $\alpha \equiv \neg\neg\alpha$). Esta equivalencia la conocemos como *ley de la doble negación*.

Ejemplo 2.4.4 (Conmutatividad de la conjunción). Sean α y β proposiciones. Veamos que $\alpha \wedge \beta \equiv \beta \wedge \alpha$:

α	β	$\alpha \wedge \beta$	$\beta \wedge \alpha$
V	V	V	V
V	F	F	F
F	V	F	F
F	F	F	F

En la primera fila, tanto $\alpha \wedge \beta$ como $\beta \wedge \alpha$ son verdaderas, porque tanto α como β son verdaderas.

En la segunda fila, $\alpha \wedge \beta$ es falsa porque β es falsa, por la misma razón $\beta \wedge \alpha$ es falsa (en ambos casos, hay al menos una proposición que es falsa).

En la tercera fila, $\alpha \wedge \beta$ es falsa porque α es falsa, por la misma razón $\beta \wedge \alpha$ es falsa (en ambos casos, hay al menos una proposición que es falsa).

En la cuarta fila, ambas proposiciones son falsas, porque al menos una de las proposiciones consideradas en ambas conjunciones es falsa, de hecho las dos son falsas.

Ejemplo 2.4.5 (Ley de De Morgan 1). Dadas α y β proposiciones, haciendo un argumento similar a los hechos anteriormente, podemos ver que $\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta$:

α	β	$\neg$	$(\alpha \wedge \beta)$	$\neg\alpha$	$\vee$	$\neg\beta$
V	V	F	V	F	F	F
V	F	V	F	F	V	V
F	V	V	F	V	V	F
F	F	V	F	V	V	V

2.4.1. Análisis usando asignaciones de verdad

Analizar los posibles valores de verdad de las proposiciones mediante tablas de verdad puede ser engorroso, además de ser un ejercicio mecánico sin ningún beneficio sustancial. Así que aquí exploramos una manera adicional para comprobar que dos proposiciones son en efecto *equivalentes*.

Sean α y β proposiciones. Supongamos que deseamos demostrar que $\alpha \equiv \beta$. Por la Definición 2.4.1 de equivalencia semántica debemos ver que la proposición $\alpha \leftrightarrow \beta$ es una tautología. Por el Ejercicio 2.5.5, numeral 7 (significado del bicondicional), esto sería equivalente a ver que $(\alpha \to \beta) \wedge (\beta \to \alpha)$ es una tautología, puesto que $\alpha \leftrightarrow \beta \equiv (\alpha \to \beta) \wedge (\beta \to \alpha)$. De esta manera, esto es equivalente a analizar que tanto $\alpha \to \beta$ como $\beta \to \alpha$ son tautologías. Esto lo podemos hacer haciendo un análisis de asignaciones de valores de verdad.

Esta manera de razonar se vuelve bastante útil, e incluso eficiente, en comparación con el caso en el que tengamos que hacer tablas de verdad con muchas filas (por ejemplo, tener solo 4 letras proposicionales conformando una proposición hace automáticamente que una tabla de verdad que las involucre tenga $2^4 = 16$ filas, lo que lo haría bastante laborioso de hacer).

Ejemplo 2.4.6. Aunque en el Ejemplo 2.4.5 analizamos que $\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta$ utilizando tablas de verdad, hagamos un análisis de valores de verdad para determinar esta equivalencia.

1. Veamos primero que $\neg(\alpha \wedge \beta) \rightarrow (\neg\alpha \vee \neg\beta)$ es tautología. En el caso de que $\neg(\alpha \wedge \beta)$ sea verdadera, por definición de asignación de valores de verdad de una negación tenemos que $\alpha \wedge \beta$ es falsa, por lo tanto, tenemos que o bien α es falsa o β es falsa. Si α es falsa, entonces por definición de asignación de valores de verdad de una negación tenemos que $\neg\alpha$ es verdadera; si β es falsa entonces por definición de asignación de valores de verdad de una negación tenemos que $\neg\beta$ es verdadera. En cualquier caso, $\neg\alpha \vee \neg\beta$ es verdadera (asignación de valores de verdad de una disyunción). Por lo tanto, en este caso podemos concluir que $\neg(\alpha \wedge \beta) \rightarrow (\neg\alpha \vee \neg\beta)$ es verdadera. En los demás casos donde $\neg(\alpha \wedge \beta)$ sea falsa, por asignación de valores de verdad de un condicional tenemos que $\neg(\alpha \wedge \beta) \rightarrow (\neg\alpha \vee \neg\beta)$ es verdadera (el antecedente es falso). Por lo tanto, tenemos que como en cualquier caso $\neg(\alpha \wedge \beta) \rightarrow (\neg\alpha \vee \neg\beta)$ es verdadera, entonces dicha proposición es una *tautología*.

2. Veamos ahora que $(\neg\alpha \vee \neg\beta) \rightarrow \neg(\alpha \wedge \beta)$ es una tautología. En el caso de que $\neg(\alpha \wedge \beta)$ sea falsa, tenemos por asignación de valores de verdad de una negación que $\alpha \wedge \beta$ es verdadera, por lo tanto, por asignación de valores de verdad de una conjunción tenemos que tanto α como β son verdaderas. Por asignación de valores de verdad de una negación, tenemos que $\neg\alpha$ y $\neg\beta$ son ambas falsas, por lo tanto, por la forma como definimos la asignación de valores de verdad de una disyunción tenemos que $\neg\alpha \vee \neg\beta$ es falsa, luego en este caso $(\neg\alpha \vee \neg\beta) \rightarrow \neg(\alpha \wedge \beta)$ es verdadera. En el caso de que $\neg(\alpha \wedge \beta)$ sea verdadera, $(\neg\alpha \vee \neg\beta) \rightarrow \neg(\alpha \wedge \beta)$ es verdadera (cuando el consecuente es verdadero, dicho condicional va a ser verdadero por la forma como definimos la asignación de

valores de verdad de un condicional). Como en cualquier caso $(\neg\alpha \vee \neg\beta) \rightarrow \neg(\alpha \wedge \beta)$ es verdadera, entonces dicha proposición es una tautología.

De esta manera, como $\neg(\alpha \wedge \beta) \rightarrow (\neg\alpha \vee \neg\beta)$ y $(\neg\alpha \vee \neg\beta) \rightarrow \neg(\alpha \wedge \beta)$ son tautologías, por lo observado anteriormente tenemos que $\neg(\alpha \wedge \beta) \equiv (\neg\alpha \vee \neg\beta)$.

2.5. Ejercicios

Ejercicio 2.5.1. Use las letras p, q y r para abreviar las proposiciones "Arnoldo va a la fiesta", "Betty compra los pasabocas' y "Carlos lleva la música para la reunión", respectivamente.

1. Simbolice las siguientes proposiciones:

   a) Arnoldo va a la fiesta y Betty compra los pasabocas.

   b) O Arnoldo va a la fiesta o Betty compra los pasabocas, pero no ambas cosas.

   c) Carlos no lleva la música para la reunión.

   d) Si Arnoldo va a la fiesta o Betty compra los pasabocas, entonces Carlos lleva la música para la reunión.

   e) Es suficiente que Betty compre los pasabocas para que Carlos lleve música a la reunión.

   f) Betty compra los pasabocas y Arnoldo va a la fiesta, si y solo si, Carlos lleva música para la reunión.

   g) No es el caso que si Arnoldo va a la fiesta, entonces Betty compra los pasabocas y Carlos lleva música para la reunión.

   h) Que Arnoldo vaya a la fiesta es una condición suficiente para que Carlos lleve la música para la reunión.

2. Escriba en correcto español, usando las interpretaciones dadas, las proposiciones simbolizadas por:

   a) $(p \wedge q) \rightarrow r$.

b) $\neg(p \wedge r) \rightarrow \neg q$.

c) $(p \rightarrow q) \vee r$.

d) $r \rightarrow (p \wedge q)$.

e) $r \rightarrow (p \vee q)$.

f) $p \vee (q \wedge r)$.

g) $(p \vee q) \rightarrow r$.

h) $\neg r \rightarrow \neg(p \vee q)$.

i) $\neg((p \rightarrow q) \rightarrow r))$.

Ejercicio 2.5.2. Considere las siguientes proposiciones:

(a) Si practica algún deporte, tiene buen estado físico.

(b) Combinar adecuadamente los condimentos es suficiente para tener una buena comida.

1. Simbolícelas.
2. Encuentre su recíproca, su contraria y su contrarrecíproca.
3. Escriba en correcto español las proposiciones encontradas en 2.

Ejercicio 2.5.3. Ponga la mínima cantidad de paréntesis necesarios para que la expresión:

$$\neg q \wedge r \rightarrow s \vee t,$$

simbolice:

1. Un condicional.
2. Una disyunción.
3. La negación de una disyunción.
4. Una conjunción.
5. Un condicional con antecedente la negación de una conjunción.

Ejercicio 2.5.4. Determine cuáles de las siguientes expresiones son tautologías, justificando su respuesta:

i. $(p \to q) \leftrightarrow (\neg p \wedge q)$.
ii. $(p \to q) \leftrightarrow (\neg p \vee q)$.
iii. $(p \to (q \to r)) \leftrightarrow ((p \wedge q) \to r)$.
iv. $\neg((p \wedge (p \to q)) \to q)$.
v. $((p \to q) \wedge p) \leftrightarrow (p \wedge q)$.

Ejercicio 2.5.5. Demuestre las siguientes equivalencias lógicas:

1. $\neg(\alpha \vee \beta) \equiv \neg\alpha \wedge \neg\beta$ (ley de De Morgan 2).
2. $\neg(\alpha \to \beta) \equiv \alpha \wedge \neg\beta$ (negación del condicional).
3. $(\alpha \vee \beta) \vee \gamma \equiv \alpha \vee (\beta \vee \gamma)$ (asociatividad $\vee$).
4. $(\alpha \wedge \beta) \wedge \gamma \equiv \alpha \wedge (\beta \wedge \gamma)$ (asociatividad $\wedge$).
5. $\alpha \to \beta \equiv \neg\alpha \vee \beta$ (significado del condicional).
6. $\alpha \to \beta \equiv \neg\beta \to \neg\alpha$ (contrarrecíproca del condicional).
7. $\alpha \leftrightarrow \beta \equiv (\alpha \to \beta) \wedge (\beta \to \alpha)$ (significado del bicondicional).
8. $\neg(\alpha \leftrightarrow \beta) \equiv (\alpha \wedge \neg\beta) \vee (\beta \wedge \neg\alpha)$ (negación del bicondicional).

Ejercicio 2.5.6. En cada caso, encuentre una proposición equivalente a la dada que no utilice el conectivo $\to$.

1. $(p \to q) \to r$.
2. $p \to (q \to r)$.

Ejercicio 2.5.7. Determine si se tienen las siguientes equivalencias, justificando su respuesta:

1. $(\alpha \wedge \beta) \to \gamma \equiv \alpha \to (\beta \to \gamma)$.
2. $\alpha \to (\beta \to \gamma) \equiv \beta \to (\alpha \to \gamma)$.

Lección *tres*

Negación de proposiciones. Implicación semántica

3.1. Negación de proposiciones

Cuando tenemos una afirmación en matemáticas, muchas veces es muy importante saber qué significa que dicha afirmación no sea verdadera. Desde el punto de vista del cálculo proposicional, solo tenemos en cuenta la estructura externa de dichas afirmaciones (es decir, la manera como están conectadas con otras proposiciones utilizando los conectivos vistos anteriormente). Más adelante estudiaremos cómo analizar afirmaciones que involucran cuantificadores y su estructura interna (predicados). Seguiremos las siguientes indicaciones:

1. Lo primero que tenemos que hacer es traducir dichas afirmaciones en lenguaje lógico.

2. Luego determinamos una proposición que sea semánticamente equivalente a la negación de nuestra afirmación original.

3. Por último, reescribimos esta proposición en español usando el significado de cada uno de los conectivos utilizados en ella y la interpretación que se haya hecho de las letras proposicionales.

Ejemplo 3.1.1. Neguemos la siguiente afirmación: "2 es un número par y es un número primo". Las proposiciones más simples utilizadas en esta afirmación son las siguientes:

p: "2 es un número par",
q: "2 es un número primo".

El único conectivo involucrado en esta afirmación es una *conjunción* ("2 es un número par **y** es un número primo"), luego en lenguaje lógico esta afirmación es escrita como $p \wedge q$. Por la Ley de De Morgan (1) (Ejemplo 2.4.5), $\neg(p \wedge q) \equiv \neg p \vee \neg q$, luego la negación de nuestra afirmación inicial es equivalente a "2 no es un número par o no es un número primo".

Ejemplo 3.1.2. Neguemos la siguiente afirmación: "Si n es par, entonces n^2 es par". Las proposiciones más simples (es decir, que no involucran conectivos) son las siguientes:

p: "n es par",
q: "n^2 es par".

El conectivo principal de esta afirmación es un condicional. Entonces nuestra afirmación escrita en lenguaje lógico es $p \to q$. Utilizando la equivalencia 2, dada en el Ejercicio 2.5.5 (negación del condicional), sabemos que $\neg(p \to q) \equiv p \wedge \neg q$.

Traduciendo esta última proposición a español, obtenemos que la negación de la afirmación dada atrás es equivalente a decir que se tiene que n es par (p) y que no es cierto que n^2 sea par ($\neg q$).

Ejemplo 3.1.3. Neguemos la siguiente afirmación: "Si n es un número natural, entonces n es múltiplo de 2 o es múltiplo de 3". Las proposiciones más simples de esta proposición son las siguientes:

p: "n es un número natural".
q: "n es múltiplo de 2".
r: "n es múltiplo de 3".

Avanzando en el nivel de complejidad de esta afirmación, la proposición que debe tenerse en cuenta es "n es múltiplo de 2 *o* es múltiplo de 3" que corresponde a la disyunción $q \vee r$. Finalmente, el conectivo principal de la afirmación original es un condicional cuyo antecedente es la proposición "n es un número natural" y cuyo consecuente es la proposición "n es múltiplo de 2 o es múltiplo de 3". El antecedente de esta afirmación es "n es un número natural" que denotamos atrás por la letra proposicional p y el consecuente es la disyunción $q \vee r$; así que en lenguaje lógico esta proposición es denotada por $p \to (q \vee r)$. Utilizando la equivalencia 2, dada en el Ejercicio 2.5.5 (negación de un condicional), sabemos que $\neg(p \to (q \vee r)) \equiv p \wedge \neg(q \vee r)$. Por la Ley de De Morgan (2) (Ejercicio 2.5.5 1) sabemos que $\neg(q \vee r) \equiv \neg q \wedge \neg r$, luego no es complicado verificar que $\neg(p \to (q \vee r)) \equiv p \wedge (\neg q \wedge \neg r)$ (queda como ejercicio para el lector). De esta manera, la negación de la afirmación dada inicialmente es equivalente a "n es un número natural que no es múltiplo de 2 y no es múltiplo de 3". Nótese que en español la expresión "y no" se puede reemplazar por "ni".

3.2. Implicación semántica

Una de las nociones más importantes en argumentación es la noción de consecuencia. Desde épocas remotas, la lógica se ha utilizado como herramienta para justificar la validez de argumentos. Entenderemos por *argumento* una sucesión de afirmaciones por medio de las cuales se pretende justificar que de unas afirmaciones iniciales (que llamaremos *premisas*) podemos deducir cierta afirmación (que llamaremos *conclusión*). En esta subsección, estudiaremos este concepto desde el punto de vista semántico.

Definición 3.2.1. Sean $\alpha_1, \cdots, \alpha_n, \beta$ proposiciones. Decimos que $\alpha_1, \cdots, \alpha_n$ *implican semánticamente* β (lo cual vamos a denotar por $\alpha_1, \cdots, \alpha_n \models \beta$) si y solo si $(\alpha_1 \wedge \cdots \wedge \alpha_n) \to \beta$ es tautología.

Observación 3.2.2. Hay autores que denotan la implicación lógica por $\Rightarrow$ (e.g., [1]). Nosotros preferimos utilizar en estas notas el símbolo $\models$ (que es estándar en libros más recientes de lógica matemática y teoría de modelos) con el propósito de evitar cualquier confusión en los estudiantes con el conectivo $\to$.

Observación 3.2.3. Nótese que $\alpha_1, \cdots, \alpha_n \models \beta$ es equivalente al hecho de que en los casos que $\alpha_1, \cdots, \alpha_n$ sean verdaderas simultáneamente (es decir, la conjunción $\alpha_1 \wedge \cdots \wedge \alpha_n$ es verdadera), β es verdadera en esos casos también. En otras palabras, esto es equivalente a que en los casos en que β sea falsa, alguna de las proposiciones $\alpha_1, \alpha_2, \cdots \alpha_n$ es falsa (por lo tanto, la conjunción $\alpha_1 \wedge \cdots \wedge \alpha_n$ es falsa en ese caso).

Ejemplo 3.2.4 (Modus Ponens)**.** Sean α y β proposiciones. Veamos que $\alpha \to \beta, \alpha \models \beta$.

α	β	$((\alpha \to \beta)$	$\wedge$	$\alpha)$	$\to$	β
V	V	V	V	V	V	V
V	F	F	F	V	V	F
F	V	V	F	F	V	V
F	F	V	F	F	V	F

Por lo tanto, $((\alpha \to \beta) \wedge \alpha) \to \beta$ es tautología y por consiguiente $\alpha \to \beta, \alpha \models \beta$.

En este caso, no es muy engorroso hacer la tabla de verdad de $((\alpha \to \beta) \wedge \alpha) \to \beta$. Sin embargo, hagamos un análisis usando asignaciones de valores de verdad para justificar que $((\alpha \to \beta) \wedge \alpha) \to \beta$ es tautología: supongamos que β es falsa, luego veamos que alguna de las proposiciones $\alpha \to \beta$ y α debe ser falsa. Si α es falsa, no tenemos nada que probar. Así que supongamos que α es verdadera, como β

es falsa entonces $\alpha \to \beta$ debe ser falsa (¿por qué?). Por lo tanto, no se puede dar el caso de que $(\alpha \to \beta) \wedge \alpha$ es verdadera y β es falsa, luego en cualquier caso $((\alpha \to \beta) \wedge \alpha) \to \beta$ es verdadera; es decir, es tautología. Este último tipo de argumento es muy útil cuando hacer la tabla de verdad del condicional, que necesitamos estudiar, se vuelve muy laborioso.

Ejemplo 3.2.5 (Eliminación de la conjunción 1)**.** Sean α y β proposiciones. Veamos que $\alpha \wedge \beta \models \alpha$. Una forma de hacerlo es verificando, usando tablas de verdad, que $(\alpha \wedge \beta) \to \alpha$ es tautología, lo que dejamos como ejercicio para el lector.

En este caso, es sencillo hacer este análisis usando tablas de verdad. Pero en el caso de que tengamos más letras proposicionales, el número de filas crece de manera exponencial, así que debemos explorar maneras más sencillas y efectivas de justificar que se tiene este tipo de implicaciones. Supongamos que α es falsa, en ese caso $\alpha \wedge \beta$ es falsa (¿por qué?), por lo tanto, $(\alpha \wedge \beta) \to \alpha$ no puede ser falsa. Luego $(\alpha \wedge \beta) \to \alpha$ es tautología y por consiguiente $\alpha \wedge \beta \models \alpha$.

Ejemplo 3.2.6 (Modus Ponens erróneo)**.** Veamos que no es verdad que $\alpha \to \beta, \beta \models \alpha$. Si sucede que α es falsa y β es verdadera, notemos que $\alpha \to \beta$ es verdadera. En este caso, tanto $\alpha \to \beta$ como β son verdaderas, entonces $(\alpha \to \beta) \wedge \beta$ es verdadera. Pero como α es falsa, entonces $((\alpha \to \beta) \wedge \beta) \to \alpha$ es falsa.

α	β	$((\alpha \to \beta)$	$\wedge \beta)$	$\to \alpha$
F	V	V	V	F

Como $((\alpha \to \beta) \wedge \beta) \to \alpha$ no es tautología (hay un caso en el que es falsa), entonces no se tiene que $\alpha \to \beta, \beta \models \alpha$, lo que denotamos por $\alpha \to \beta, \beta \not\models \alpha$.

Como ilustración, veremos con un caso particular por qué este razonamiento falla. Tomemos las siguientes proposiciones:

α: "a es un número natural",
β: "a es un número entero".

El hecho de que tengamos como verdadero β (es decir, que a sea un número entero) *no* nos permite decir que α sea verdadera (es decir, que dicho número sea un natural), incluso si tenemos $\alpha \to \beta$ como verdadera. Tomando por ejemplo a como -2, vemos que como el antecedente α es falso en este caso (-2 no es un número natural), $\alpha \to \beta$ es verdadera, tenemos que β es verdadera (-2 es un número entero) pero esto *no* nos permite concluir que α es verdadera (es decir, de esto no podemos concluir que -2 es un número natural).

3.3. Reducción al absurdo

Algunas veces no se puede hacer un argumento de manera directa. El siguiente resultado es muy importante, porque en él están basados argumentos indirectos que usaremos más adelante en el sistema deductivo de la lógica proposicional clásica y como estrategia de demostración utilizada en matemáticas (ver Sección 7.2).

Proposición 3.3.1. *Sean* $\alpha_1, \cdots, \alpha_n, \beta$ *proposiciones y* $\perp$ *una contradicción. Si* $\alpha_1, \cdots, \alpha_n, \neg\beta \models \perp$ *entonces* $\alpha_1, \cdots \alpha_n \models \beta$.

Demostración. Como $\alpha_1, \cdots, \alpha_n, \neg\beta \models \perp$ por hipótesis, entonces $(\alpha_1 \wedge \cdots \wedge \alpha_n \wedge \neg\beta) \to \perp$ es una tautología. En el caso de que alguna de las fórmulas $\alpha_1, \cdots, \alpha_n$ sea falsa, entonces $\alpha_1 \wedge \cdots \wedge \alpha_n$ es falsa, por lo tanto, en ese caso el condicional $(\alpha_1 \wedge \cdots \wedge \alpha_n) \to \beta$ es verdadero. En el caso de que $\alpha_1, \cdots, \alpha_n$ sean verdaderas simultáneamente, como en ese caso $(\alpha_1 \wedge \cdots \wedge \alpha_n \wedge \neg\beta) \to \perp$ también es verdadera por ser tautología y como el consecuente $\perp$ es falsa por ser contradicción entonces el antecedente $\alpha_1 \wedge \cdots \wedge \alpha_n \wedge \neg\beta$ debe ser falso; como $\alpha_1, \cdots, \alpha_n$ se están suponiendo verdaderas simultáneamente, entonces $\neg\beta$ debe ser falsa, por tal razón, β debe ser verdadera. Así, $(\alpha_1 \wedge \cdots \wedge \alpha_n) \to \beta$ es tautología y por consiguiente $\alpha_1, \cdots, \alpha_n \models \beta$. ☑

Este resultado nos dice que siempre que queramos ver que unas proposiciones $\alpha_1, \cdots, \alpha_n$ implican semánticamente β, basta ver que agregando $\neg\beta$ a las proposiciones $\alpha_1, \cdots, \alpha_n$ estas implican semánticamente una contradicción.

3.4. Teorema de la deducción

Otro resultado que nos lleva a una regla de deducción indirecta es el conocido como *Teorema de la deducción*. Es utilizado cuando lo que queremos implicar semánticamente es un condicional.

Proposición 3.4.1. *Consideremos las proposiciones* $\alpha_1, \cdots, \alpha_n, \alpha, \beta$. *Si* $\alpha_1, \cdots, \alpha_n, \alpha \models \beta$ *entonces* $\alpha_1, \cdots, \alpha_n \models \alpha \to \beta$

Demostración. En el caso de que alguna de las proposiciones $\alpha_1, \cdots, \alpha_n$ sea falsa, el antecedente de $(\alpha_1 \wedge \cdots \wedge \alpha_n) \to (\alpha \to \beta)$ es falso y, por tanto, este condicional es verdadero. Suponiendo que que $\alpha_1, \cdots, \alpha_n$ sean verdaderas simultáneamente, tenemos dos casos: si α es falsa, entonces el condicional $\alpha \to \beta$ es verdadero sin importar el valor de verdad de β y, por ende, $(\alpha_1 \wedge \cdots \wedge \alpha_n) \to (\alpha \to \beta)$ es verdadera; si en cambio α es verdadera, como por hipótesis tenemos que $\alpha_1, \cdots, \alpha_n, \alpha \models \beta$, entonces $(\alpha_1 \wedge \cdots \wedge \alpha_n \wedge \alpha) \to \beta$ es tautología. En particular, puesto que $\alpha_1, \cdots, \alpha_n, \alpha$ son verdaderas, entonces β debe ser verdadera, por consiguiente, tanto $\alpha_1 \wedge \cdots \wedge \alpha_n$ como $\alpha \to \beta$ son verdaderas y, por tal razón, $(\alpha_1 \wedge \cdots \wedge \alpha_n) \to (\alpha \to \beta)$ es verdadera. Entonces $(\alpha_1 \wedge \cdots \wedge \alpha_n) \to (\alpha \to \beta)$ es tautología, lo que nos dice que $\alpha_1, \cdots, \alpha_n \models \alpha \to \beta$. ☑

3.5. Ejercicios

Ejercicio 3.5.1. A continuación encontrará una lista de proposiciones.

(a) Simbolice cada una de ellas.

(b) Niegue las proposiciones dadas en el literal (a) anterior utilizando equivalencias lógicas.

(c) Escriba en correcto español las negaciones dadas en el literal (b).

1. Los cursos de fundamentos y de cálculo son a las 9 de la mañana.
2. Si María tiene 18 años, tiene la misma edad de Lucía.
3. Ramiro está inscrito en fundamentos o en cálculo.
4. Obtienes una beca si tienes el mejor promedio.
5. Vas a la fiesta o a cine pero no a ambas partes.
6. Si te inscribes en el curso de fundamentos y lo apruebas, puedes tomar álgebra el próximo semestre.

7. Los cursos de geometría elemental y de matemáticas básicas son a las 11 de la mañana.
8. Si Paola estudia estadística, entonces estudia la misma carrera que Luisa.
9. Rafael está inscrito en el curso de inglés o en el curso de francés.
10. Obtienes una medalla si ganas el campeonato.
11. O inscribes fundamentos de matemáticas o sistemas numéricos, pero no ambas.
12. Si te inscribes en el curso de fundamentos y lo apruebas, puedes tomar sistemas numéricos el próximo semestre.
13. n es un número impar y n^2 es un número impar.
14. O n es un número par o n^2 es un número impar.
15. O n es un número impar o n^2 es un número impar, pero n no es un número impar ni n^2 es un número impar simultáneamente.
16. n no es un número primo.
17. Si n es un número impar o n^2 es un número impar, entonces n es un número primo.
18. Es suficiente que n^2 sea un número impar para que n sea un número primo.
19. n es un número primo solo si n es un número impar y n^2 es un número impar.
20. n^2 es un número impar y n es un número impar si y solo si n es un número primo.
21. No es el caso que si n es un número impar, entonces n^2 es un número impar y n es un número primo.
22. Que n sea un número impar es una condición suficiente para que n^2 sea un número impar.
23. Que n sea un número impar es una condición necesaria para que n sea un número primo.

24. O bien n es un número primo o es el caso de que n es un número impar y n^2 es un número impar.

Ejercicio 3.5.2. Demuestre las siguientes implicaciones lógicas:

1. $\alpha \to \beta, \neg\beta \models \neg\alpha$ (modus tollendo tollens).
2. $\alpha \wedge \beta \models \beta$ (eliminación de la conjunción 2).
3. $\alpha, \beta \models \alpha \wedge \beta$ y $\beta, \alpha \models \alpha \wedge \beta$ (introducción de la conjunción).
4. $\alpha \models \alpha \vee \beta$ y $\beta \models \alpha \vee \beta$ (introducción de la disyunción).
5. $\alpha \vee \beta, \neg\alpha \models \beta$ y $\alpha \vee \beta, \neg\beta \models \alpha$ (modus tollendo ponens).
6. $\alpha \leftrightarrow \beta \models \alpha \to \beta$ y $\alpha \leftrightarrow \beta \models \beta \to \alpha$ (bicondicional-condicional).
7. $\alpha \to \beta, \beta \to \gamma \models \alpha \to \gamma$ (silogismo hipotético).
8. $\alpha \to \beta, \gamma \to \delta, \alpha \vee \gamma \models \beta \vee \delta$ (dilema constructivo).

Ejercicio 3.5.3. Determine una proposición semánticamente equivalente a las siguientes, usando a lo sumo solamente $\neg$ y $\wedge$. Justifique su respuesta:

1. $p \to p$.	2. $p \to \neg q$.	3. $(p \wedge q) \to p$.	4. $p \vee (q \vee r)$.
5. $\neg p \to \neg q$.	6. $\neg(p \vee (q \to r))$.	7. $\neg(\neg p \vee \neg q)$.	8. $p \to (q \to r)$.

Lección *cuatro* Predicados y cuantificadores

Como vimos en la lecciones anteriores, el tipo de afirmaciones que podemos trabajar desde el punto de vista de la *lógica proposicional clásica* involucra las conexiones externas entre proposiciones por medio de los conectivos (síntesis), sin tener en cuenta la estructura interna de ellas (análisis). Para ampliar este punto de vista, debemos enriquecer un poco lo hecho anteriormente de manera que podamos trabajar con la estructura interna de las afirmaciones. Una forma de hacerlo es desarrollando lo que denominamos *lógica de predicados clásica*.

4.1. Predicados

Un concepto central en este nuevo desarrollo es el concepto de *predicado*. Recordemos que en gramática una oración se compone de sujeto (de quién se está hablando) y predicado (descripción de la acción que ejecuta el sujeto). En estas notas un *predicado* será entendido como una *propiedad* que objetos matemáticos pueden satisfacer o no; aunque en algunos pocos ejemplos podremos referirnos a personas, animales o cosas. Más precisamente, un predicado es una afirmación que se realiza sobre un sujeto indeterminado que está en un universo de referencia (por defecto, será siempre no vacío) y que esencialmente describe una propiedad.

Denominaremos los sujetos indeterminados, de un cierto universo de referencia U, como *variables* y los simbolizaremos con las letras u, v, w, x, y, z, o estas letras con subíndices. Los predicados los denotaremos por letras latinas mayúsculas, e involucrarán en su definición una o más variables; que representarán los sujetos indeterminados. Por ejemplo, $P(x)$, $Q(x,y)$, $R(x,y,z)$ son símbolos de predicados y, más generalmente, $P(x_1, \cdots, x_n)$.

A los predicados no se les puede asignar valor de verdad porque no son proposiciones. No obstante, cuando las variables en los predicados son reemplazadas por objetos de un universo específico obtendremos proposiciones de las cuales claramente podremos decir si son verdaderas o falsas.

Definición 4.1.1. Entenderemos por *interpretación* de un símbolo de predicado $P(x_1, \cdots, x_n)$, con $x_1, \cdots, x_n$ variables, en un universo de referencia U, un *predicado* o *propiedad* que tenga sentido en el universo U que involucra las variables $x_1, \cdots, x_n$, la cual denotaremos por $P^U(x_1, \cdots, x_n)$.

Observación 4.1.2. Para no sobrecargar la notación, abusando del lenguaje, quitaremos el superíndice U si el universo de referencia es claro. A pesar de que el símbolo $P(x_1, \cdots, x_n)$ no es técnicamente un predicado, abusaremos del lenguaje y llamaremos al símbolo $P(x_1, \cdots, x_n)$ *predicado*.

Ejemplo 4.1.3. Considere como conjunto de referencia U el conjunto de los números naturales y $P(x)$ un predicado con variable x; una posible interpretación de $P(x)$ en este universo puede ser

$$P(x)\text{: “}x\text{ es un número par”.}$$

Ejemplo 4.1.4. Considere como conjunto de referencia U la colección de seres humanos y $M(x, y)$ un predicado con variables x y y; una posible interpretación de $M(x, y)$ en este universo puede ser

$$M(x, y)\text{: “}x\text{ es madre biológica de }y\text{”.}$$

Ejemplo 4.1.5. Consideremos la siguiente afirmación: “Si n es un natural que es par, entonces n^2 es par”. A pesar de que tanto antecedente como consecuente de esta implicación hablan del mismo objeto n, desde el punto de vista de la lógica proposicional clásica solo se puede expresar de la forma $\alpha \rightarrow \beta$, puesto que ahí solo podemos analizar la estructura externa de dicha afirmación. Por esta razón, si queremos analizar la estructura interna de dichas afirmaciones, debemos extraer de ellas cuáles son las propiedades más simples que estamos considerando sobre dicho objeto n. En este caso, considerando U como el conjunto de los números enteros, dichas propiedades básicas son descritas por los predicados:

1. $N(x)$: “x es natural”,
2. $P(x)$: “x es par”.

Extrayendo dichas propiedades básicas que se dicen de los objetos n y n^2, escribimos la afirmación original en lenguaje lógico con predicados. En este caso, la afirmación “n es un natural” la simbolizamos por $N(n)$, la afirmación “n es un número par” la simbolizamos como $P(n)$ y la afirmación “n^2 es un número par” quedaría simbolizada como $P(n^2)$. Nótese que la afirmación original es un condicional cuyo antecedente es la conjunción “n es un número natural que es par”, que simbolizamos por $N(n) \wedge P(n)$, y cuyo consecuente es “n^2 es par”, que simbolizamos como $P(n^2)$. La simbolización de dicho condicional quedaría $(N(n) \wedge P(n)) \rightarrow P(n^2)$.

Ejemplo 4.1.6. Consideremos el predicado $P(x, y)$: "$x + y > 0$". Los términos x y y representan objetos indeterminados en un universo de referencia, razón por lo que los denominamos *variables*. Los predicados nos permiten construir proposiciones cuando reemplazamos las variables x y y por objetos de un universo que tomemos como referencia. Por ejemplo, si tomamos como universo de referencia U el conjunto de los números enteros y reemplazamos x por 2 y y por 4, la proposición $P(2, 4)$ afirma que $2 + 4 > 0$. En este caso dicha afirmación es verdadera. Pero si reemplazamos x por 2 y y por -3, la proposición $P(2, -3)$ nos dice que $2 + (-3) > 0$, lo cual es falso porque $2 + (-3) = -1$.

Entonces los pasos a seguir en la traducción de afirmaciones al lenguaje lógico con predicados son los siguientes:

1. Identificar cuáles son los predicados (propiedades) más simples que se están considerando. Simbolizamos cada uno de estos con un letra latina mayúscula.

2. Reemplazar las variables que se usaron para definir los predicados por los objetos de los cuáles se están hablando en dichas afirmaciones.

3. Aumentar progresivamente en complejidad en la simbolización de dichas afirmaciones, utilizando los conectivos vistos en la lógica proposicional clásica.

4.2. Cuantificadores

Vimos que predicados como "x es madre biológica de y", "x es un número par" o "$x + y > 0$" no son proposiciones porque, simplemente, son afirmaciones a las que no les podemos asignar un valor de verdad. De todos modos, estos predicados nos permiten construir proposiciones reemplazando las variables por objetos de un universo de referencia.

En el caso de predicados con una sola variable, por ejemplo $P(x)$, una vez sea escogido el universo de referencia, hemos visto que al reemplazar x por algún a, objeto del universo de referencia, la proposición $P(a)$ puede ser verdadera pero falsa cuando reemplazamos x por otros. En algunas ocasiones nos gustaría saber *cuántos* objetos del universo al tomar el lugar de x, en el predicado $P(x)$, hacen que obtengamos proposiciones verdaderas. En particular, queremos decir si todos los elementos, o si existe algún elemento, del universo que satisfacen la propiedad descrita por el predicado $P(x)$. Por lo tanto, introduciremos dos símbolos más, llamados *cuantificadores*, que nos ayudarán a construir nuevas proposiciones que expresan estas ideas. El valor de verdad de estas proposiciones dependerá de si al reemplazar la variable x por cualquier objeto del universo obtenemos proposiciones verdaderas o de si existe al menos un elemento en el universo que haga verdadera la proposición obtenida cuando reemplazamos la variable por tal objeto, según sea el caso. En resumen, los cuantificadores nos sirven para determinar en alguna medida cuántos elementos de un universo específico satisfacen una propiedad, sin decir explícitamente el número de elementos que la cumplen.

Uno de estos tipos de proposiciones que encontramos en las matemáticas es por ejemplo: "$|\sin x| \leq 1$ para todo número real x". La frase "para todo número real x" hace referencia a un tipo de cuantificador. Otro tipo de cuantificador es el que aparece en la siguiente proposición: "$\sin x = 0$ para algún número real x". En estos dos ejemplos es claro que el universo de referencia es el de los números reales $\mathbb{R}$. Esto significa que la variable x será reemplazada por números reales. En el primer caso, x debe ser reemplazada por cualquier número real y verificar que se cumpla la propiedad para cada uno de ellos para concluir que la afirmación es verdadera, en caso contrario será falsa. Y en el segundo caso, basta con exhibir al menos un número real que, al reemplazar a x, satisfaga la propiedad para decir que tal proposición es verdadera. Si no existe ningún número real que satisfaga la propiedad, la proposición será falsa.

Definamos primero la semántica (es decir, el significado) que le vamos a dar a los dos cuantificadores clásicos con los que iremos a trabajar.

Primero que todo, especifiquemos qué vamos a entender por *universo de referencia* en este contexto y qué entenderemos por *interpretación* de un predicado.

Definición 4.2.1. Sea U un universo de referencia no vacío y $P(x)$ un predicado (propiedad) con una *variable libre* x (es decir, x no está bajo el alcance de un cuantificador previo). Decimos que afirmaciones de la forma:

1. Para todo x en U se cumple $P(x)$,
2. Para cada x en U, $P(x)$ es verdadera,
3. La afirmación $P(x)$ es verdadera para todo x en U,
4. Todos los posibles reemplazos de x por objetos en U satisfacen $P(x)$,

o afirmaciones similares, que denotaremos por $\forall x(P(x))$, es verdadera en el universo U si y solo si para cualquier reemplazo de x por cualquier elemento a de U se tiene que la proposición $P(a)$ es verdadera (es decir, a satisface la propiedad descrita por P). Este tipo de afirmaciones las denominaremos *universales*.

Ejemplo 4.2.2. Examinemos la proposición: "Todos los smartphones se pueden conectar a internet". Consideremos como universo de referencia U a la colección de todos los smartphones y el siguiente predicado:

$$I(x)\text{: "}x\text{ se puede conectar a internet".}$$

Vemos que la proposición a considerar corresponde en símbolos a $\forall x(I(x))$. Ahora analicemos su valor de verdad. Sea a cualquier elemento de U, es decir, a representa a cualquier smartphone. Si lograramos probar que $I(a)$ es siempre verdadera, es decir, que sin importar qué smartphone a tomemos, vemos que $I(a)$ es siempre verdadera, concluiríamos que en este universo tenemos que $\forall x(I(x))$ es verdadera.
Caso contrario ocurriría si encontraramos solo un smartphone b que no se pueda conectar a internet, es decir que $I(b)$ es falsa. Esto mostraría que existe un reemplazo de x para el cual no se cumple la propiedad. Si así fuera, la proposición $\forall x(I(x))$ sería falsa en este universo.

Definición 4.2.3. Sea U un universo de referencia no vacío y $P(x)$ un predicado (propiedad) con variable libre x. Decimos que afirmaciones de la forma:

1. Existe x en U que cumple $P(x)$,
2. Para algún x en U, $P(x)$ es verdadera,
3. Existe al menos un reemplazo de x por un objeto de U para el cual $P(x)$ ocurre,

o afirmaciones similares, que denotaremos por $\exists x(P(x))$, es verdadera en el universo U si y solo si existe al menos un reemplazo de x por algún elemento a de U para el cual la proposición $P(a)$ es verdadera (es decir, a satisface la propiedad descrita por P). Este tipo de afirmaciones las denominaremos *existenciales*.

Ejemplo 4.2.4. Consideremos como universo U el conjunto de los números enteros y el predicado

$$P(x)\text{: “}x\text{ es un número par”.}$$

Sabemos que 2 es un número entero que además es par, por lo tanto, la proposición $P(2)$ es verdadera. Como encontramos un reemplazo de la variable x por un objeto en el universo -2- tal que esa instancia del predicado $P(x)$ es verdadera, podemos decir que la afirmación $\exists x(P(x))$ es verdadera en este universo U.

4.3. Implicación semántica

Definición 4.3.1. Dadas φ y ψ proposiciones con predicados y cuantificadores clásicos, diremos que φ *implica semánticamente* ψ (lo que denotaremos por $\varphi \models \psi$) si y solo si para *cualquier universo de referencia* U y *cualesquiera interpretaciones* en U de los predicados involucrados en la escritura de φ y ψ, el hecho de que φ sea verdadera en dicho universo U implica que allí mismo ψ debe ser verdadera.

Observación 4.3.2. $\varphi \not\models \psi$ quiere decir que *existe* un universo de referencia U e interpretaciones de los predicados involucrados en la escritura de φ y ψ, tales que en U tenemos que φ es verdadera pero ψ es falsa.

Ejemplo 4.3.3. Denotemos por $P(x)$ algún predicado con una sola variable (en este caso x) y consideremos las proposiciones $\varphi := \forall x P(x)$ y $\psi := \exists x P(x)$. Veamos que $\varphi \models \psi$.

Sea U cualquier universo de referencia (no vacío) y $P(x)$ lo interpretamos de cualquier manera dentro de U. Si $\forall x P(x)$ fuese verdadera en U; esto quiere decir que para cualquier reemplazo de x por elementos a de U, tenemos que $P(a)$ es verdadera. Como U es un universo de referencia, tomando b algún elemento fijo de U, en particular, tenemos que $P(b)$ es verdadera. Como hemos exhibido al menos un elemento b de U para el cual $P(b)$ es verdadera, tenemos que en este universo $\exists x P(x)$ es verdadera. Como U era arbitrario y la interpretación de $P(x)$ en U también era arbitraria, entonces tenemos que $\forall x P(x) \models \exists x P(x)$.

Ejemplo 4.3.4. Veamos que $\exists x(P(x) \wedge Q(x)) \not\models \forall x(P(x) \wedge Q(x))$. Tomemos como universo de referencia $U := \mathbb{N}$ e intepretemos los predicados $P(x)$: "x es un número primo" y $Q(x)$: "x es par". Notemos que con este universo y estas interpretaciones la proposición $\exists x(P(x) \wedge Q(x))$ es verdadera porque, tomando $x := 2$, vemos que la proposición $P(2) \wedge Q(2)$: "2 es un número primo y par" es verdadera. Sin embargo, la afirmación $P(x)$ no es cierta para cualquier reemplazo de x por elementos de $\mathbb{N}$, de hecho, si tomamos $x := 4$, vemos que $P(4) \wedge Q(4)$ es falsa (a pesar de que $Q(4)$ es verdadera, tenemos que $P(4)$ es falsa porque 4 no es un número primo). Como hay al menos un universo de referencia e interpretaciones de los predicados $P(x)$ y $Q(x)$ en dicho universo de referencia donde $\exists x(P(x) \wedge Q(x))$ es verdadera pero $\forall x(P(x) \wedge Q(x))$ es falsa, entonces tenemos que $\exists x(P(x) \wedge Q(x)) \not\models \forall x(P(x) \wedge Q(x))$.

4.4. Equivalencia semántica

Definición 4.4.1. Dadas φ y ψ proposiciones con predicados y cuantificadores clásicos, diremos que φ es *equivalente semánticamente* a ψ (lo que denotaremos por $\varphi \equiv \psi$) si y solo si para *cualquier universo de referencia* U y *cualesquiera interpretaciones* en U de los predicados involucrados en la escritura de φ y ψ, φ es verdadera en dicho universo U si y solo si allí mismo ψ es verdadera (es decir, φ y ψ toman el mismo valor de verdad en U).

Observación 4.4.2. Como en la lógica proposicional clásica, tenemos que $\varphi \equiv \psi$ es equivalente al hecho de que $\varphi \models \psi$ y $\psi \models \varphi$.

Observación 4.4.3. $\varphi \not\equiv \psi$ quiere decir que *existe* un universo de referencia U e interpretaciones de los predicados involucrados en la escritura de φ y ψ tales que en U tenemos que φ y ψ tienen diferentes valores de verdad (es decir, una es verdadera y la otra es falsa en U).

Ejemplo 4.4.4. Denotemos por $P(x)$ algún predicado con una variable y consideremos las proposiciones $\varphi := \forall x P(x)$ y $\psi := \exists x P(x)$. Tenemos que $\varphi \not\equiv \psi$ puesto que no es difícil ver que $\exists x P(x) \not\models \forall x P(x)$ (lo que dejamos como ejercicio para el lector) puesto que podemos encontrar un universo de referencia U y una interpretación del predicado $P(x)$ donde $\exists x P(x)$ es verdadera pero $\forall x P(x)$ es falsa (de manera similar al Ejemplo 4.3.4).

4.5. Negación de cuantificadores

En esta parte, estudiaremos afirmaciones equivalentes a la negación de afirmaciones que involucran cuantificadores.

Observación 4.5.1 (Negación de una proposición universal)**.** Sean $P(x)$ un predicado (no necesariamente simple) y U un universo de referencia. Decir que la afirmación $\forall x\, P(x)$ *no* es cierta en U quiere decir que no es cierto que al reemplazar x por todos los elementos a de U se tenga que $P(a)$ es verdadera; esto quiere decir que encontraremos por lo menos un reemplazo de x por un elemento b en U para el cual la afirmación $P(b)$ es falsa. En otras palabras, la afirmación $\exists x \neg P(x)$ sería verdadera. Esto lo denotamos por:

$$\neg \forall x\, P(x) \equiv \exists x\, \neg P(x).$$

Observación 4.5.2 (Negación de una proposición existencial)**.** Sean $P(x)$ un predicado y U un universo de referencia. Decir que la afirmación $\exists x\, P(x)$ *no* es cierta en U quiere decir que no es cierto que podamos encontrar al menos un elemento de a en U que al reemplazarlo por x se tenga que $P(a)$ es verdadera; esto quiere decir que para ningún reemplazo de x por elementos b en U la afirmación $P(b)$ será verdadera. En otras palabras, la afirmación $\forall x\, \neg P(x)$ sería verdadera. Esto lo denotamos por:

$$\neg \exists x\, P(x) \equiv \forall x\, \neg P(x).$$

Ejemplo 4.5.3. Veamos las negaciones de las proposiciones consideradas en los Ejemplos 4.2.2 y 4.2.4. En el Ejemplo 4.2.2 se consideró la proposición

$$\forall x\, I(x) : \text{“Todos los smartphones se pueden conectar a internet”.}$$

Consideramos como universo de referencia a la colección de todos los smartphones. Aplicando lo estudiado en la Observación 4.5.1 tenemos que la negación de esta proposición es:

$$\neg\forall x\, I(x) \equiv \exists x\, \neg I(x) : \text{“Hay un smartphone que no se puede conectar a internet”.}$$

En el Ejemplo 4.2.4 se consideró la proposición

$$\exists x\, P(x)\text{: “Existe un entero que es par.”}$$

Consideramos como universo de referencia al conjunto de los números enteros. Aplicando lo estudiado en la Observación 4.5.2 tenemos que la negación de esta proposición es:

$$\neg\exists x\, P(x) \equiv \forall x\, \neg P(x) : \text{“Ningún entero es par”.}$$

Ejemplo 4.5.4. Consideremos la afirmación “todo entero es par o impar”. Observemos que esta proposición es universal, dado que el cuantificador involucrado es de este tipo. La afirmación que se está cuantificando puede ser vista como un condicional, donde el consecuente es una disyunción. Considerando los predicados $P(x)$: “x es entero”, $Q(x)$: “x es par” y $R(x)$: “x es impar”, esta afirmación queda simbolizada lógicamente como $\forall x\, (P(x) \rightarrow (Q(x) \vee R(x)))$. Veamos cómo negar esta proposición mediante el uso de equivalencias semánticas.

$$\begin{aligned}
\neg\forall x\, (P(x) \rightarrow (Q(x) \vee R(x))) &\equiv \exists x\, \neg(P(x) \rightarrow (Q(x) \vee R(x))) \\
&\ \text{(negación de un universal es un existencial)} \\
&\equiv \exists x\, (P(x) \wedge \neg(Q(x) \vee R(x))) \\
&\ \text{(negación de un condicional)} \\
&\equiv \exists x\, (P(x) \wedge (\neg Q(x) \wedge \neg R(x))) \\
&\ \text{(leyes de De Morgan).}
\end{aligned}$$

Esta última línea nos dice que la negación de la proposición "todo entero es par o impar" es equivalente a la proposición "existe un entero que no es par y tampoco impar".

Ejemplo 4.5.5. Veamos la negación de la proposición $\exists x\, \forall y\, P(x, y)$ donde $P(x, y)$:"$x + y = 0$" y el universo de referencia es $U := \mathbb{Z}$. Aplicando sucesivamente lo estudiado en las observaciones 4.5.1 y 4.5.2 tenemos que

$$\begin{aligned} \neg\exists x\, \forall y\, P(x, y) &\equiv \forall x\, \neg\forall y\, P(x, y) \\ &\quad \text{(negación de un existencial)} \\ &\equiv \forall x\, \exists y\, \neg P(x, y) \\ &\quad \text{(negación de un universal)} \end{aligned}$$

Por lo tanto, la negación de la proposición $\exists x\, \forall y\, P(x, y)$: "existe un entero x tal que para todo y entero se cumple que $x + y = 0$", es la proposición $\forall x\, \exists y\, \neg P(x, y)$: "para todo entero x existe un entero y tal que $x + y \neq 0$".

4.6. Ejercicios

Ejercicio 4.6.1. Dado el conjunto de referencia $U = \{0, 1, 2, 3, 4, 5\}$, determine el valor de verdad de las siguientes proposiciones. Justifique su respuesta.

1. $\forall y(y + 4 < 11)$.
2. $\exists z(z^3 = 1)$.
3. $\forall x(x + 4 > 7)$.
4. $\exists y(y^3 = 216)$.
5. $\forall x \forall y[(x + y < 5) \to (x + y < 8)]$.
6. $\exists x \forall y(x - y = 0)$.
7. $\exists x[(x + 1 = 10) \vee (2x = 4)]$.
8. $\forall x \exists y(x + y = x)$.

Ejercicio 4.6.2. Dé ejemplos de predicados, en algún universo, que muestren que las siguientes equivalencias o implicaciones semánticas no son válidas:

1. $\exists x\, P(x) \wedge \exists x\, Q(x) \models \exists x(P(x) \wedge Q(x))$.

2. $\forall x(P(x) \vee Q(x)) \models \forall x\, P(x) \vee \forall x\, Q(x)$.

3. $\exists x\, P(x) \models \forall x\, P(x)$.

Ejercicio 4.6.3. Negación de cuantificadores.

1. Simbolice, en lenguaje lógico, cada una de las siguientes proposiciones.

2. Simbolice su negación.

3. Escriba en correcto español su negación (evite expresiones de la forma: "No es cierto que ...", donde los puntos suspensivos corresponden a la proposición original). Use equivalencias semánticas.

   a) Todas las personas que viven en Bogotá se transportan en transmilenio o en bus.

   b) Todas las parejas de casados tienen discusiones.

   c) A todas las personas les agrada al menos dos personas.

   d) A Juan le agrada exactamente una sola persona.

   e) Todo conjunto infinito tiene un subconjunto enumerable.

   f) Algún entero es divisible por 7.

   g) Para cada entero x, hay un entero y tal que $xy = 1$.

   h) Hay un par de enteros x y y tales que $xy = 1$.

   i) Hay un entero x tal que para todo entero y se tiene que $xy = 1$.

   j) Todo conjunto no vacío de reales acotado superiormente tiene extremo superior.

   k) Todo par de triángulos congruentes tienen la misma área.

   l) Existe un número racional r tal que $\frac{1}{r} < \frac{\pi}{100}$.

   m) No existen números naturales m y n tales que $m+n = 100$ y su máximo común divisor es 3.

   n) Para cada número real x, existe un número real y tal que $xy = 1$.

   ñ) El valor absoluto de la suma de dos números reales es menor o igual que la suma de sus valores absolutos.

   o) Toda función derivable es una función continua.

   p) Para todo entero positivo n, $\frac{d}{dx}x^n = nx^{n-1}$.

q) Existe un número real x tal que $xy = y$ para cada número real y.

r) No todos los números primos son impares.

s) Existe un número natural que es mayor o igual que todos los naturales.

t) Existe un número natural tal que su recíproco es $\frac{1}{4}$.

u) Para todo número natural n existe un natural m tal que $m < n$.

v) Existe un número real x tal que para todo número real y se tiene que $xy = 0$.

w) Todos los números racionales son enteros.

x) Ningún número real elevado al cuadrado es -1.

y) Todo número natural es par o impar.

z) Todo número natural primo y par es el número 2.

Ejercicio 4.6.4. Considerando como universo el conjunto de los números enteros, si el predicado $P(x)$ significa "x es un número par" y el predicado $Q(x)$ significa "x es un múltiplo de seis", escriba en correcto español las siguientes proposiciones y sus negaciones. ¿Cuáles de ellas son ciertas?

1. $\neg\exists x(P(x) \vee Q(x))$.	2. $\exists x(P(x) \wedge Q(x))$.
3. $\forall x(P(x) \longrightarrow Q(x))$.	4. $\forall x(Q(x) \longrightarrow P(x))$.
5. $\neg\forall x(P(x) \wedge Q(x))$.	6. $\exists x(\neg P(x) \vee \neg Q(x))$.

Lección *cinco*

Cuantificación múltiple

5.1. Cuantificación múltiple

En esta parte estudiaremos las posibles combinaciones de cuantificadores sobre dos variables. Hay que tener especial cuidado, puesto que como veremos en los siguientes ejemplos, el sentido de la afirmación podría variar sustancialmente si cambiamos el orden en la cuantificación. Estudiaremos también algunas implicaciones que hay entre estas posibles combinaciones.

Ejemplo 5.1.1. Algunas veces los cuantificadores aparecen implícitos en la redacción de las afirmaciones. Analicemos la siguiente afirmación: "Toda persona tiene una madre". Para esta proposición, podemos considerar un predicado simple definido en el universo U de todas las personas:

$$M(y, x)\text{:“}y \text{ es madre de } x\text{”}.$$

Lo que nos dice esta afirmación es que en el universo U de las personas, para cualquier reemplazo de x por cualquier elemento a podemos encontrar al menos un reemplazo de y, digamos b, en ese mismo universo (la madre de a), para el cual la propiedad $M(b, a)$ es verdad (es decir, b es madre de a). Esta proposición corresponde en símbolos a $\forall x\, (\exists y\, (M(y, x)))$. Vale la pena aclarar que $\exists y\, (M(y, x))$ es un predicado con una sola variable libre x. Más precisamente, este predicado corresponde en español a $\exists y\, (M(y, x))$:"x tiene una madre".

Observación 5.1.2 (Eliminación de paréntesis)**.** Con el fin de no sobrecargar la notación, podemos eliminar los paréntesis que encierren afirmaciones universales o aquellas que encierren afirmaciones existenciales, sin tener ambigüedades. Adicionalmente, podemos eliminar los paréntesis que encierren símbolos de predicados generales.

Como veremos en el siguiente ejemplo, el valor de verdad de un predicado depende fuertemente del universo que estemos considerando.

Ejemplo 5.1.3. Consideremos el predicado $P(x, y)$: "$x + y = 0$" y el universo de referencia $U := \mathbb{N}$ el conjunto de los números naturales. Estudiemos el valor de verdad de la proposición "para todo y existe x tal que $x + y = 0$", que es denotada por $\forall y(\exists x(x + y = 0))$. Podemos eliminar los paréntesis que encierran la afirmación existencial, quedando esta expresión como $\forall y \exists x(x + y = 0)$, entendiéndose sin ambigüedad lo que queremos decir. Esta proposición no es verdadera en el universo $U := \mathbb{N}$ puesto que *no* es cierto que para cualquier reemplazo de y por elementos en $\mathbb{N}$, digamos a, se tenga que la proposición $\exists x(x + a = 0)$ sea verdadera. En particular, reemplazando y por el natural 2, sabemos que no hay un reemplazo de x por algún elemento de $\mathbb{N}$, tal que $x+2 = 0$; de hecho, el posible reemplazo de x que haría verdadera esa proposición es -2, el cual no es un número natural. No obstante, si consideramos como universo $U := \mathbb{Z}$ el conjunto de los números enteros, la proposición será verdadera, porque al tomar cualquier reemplazo de y por cualquier entero fijo a, sabemos que podemos encontrar un reemplazo para x en $\mathbb{Z}$, tal entero es $-a$ (el opuesto aditivo de a en $\mathbb{Z}$). Así, $a+(-a) = 0$, es decir, $P(a, -a)$ es verdadera. Este tipo de afirmaciones son denominadas *universal-existencial*, porque primero debemos verificar que la propiedad vale para reemplazos de la variable cuantificada con el universal (en este ejemplo, y) por cualquier elemento en el universo de referencia y luego para ese elemento arbitrario pero fijo, encontramos un reemplazo de la segunda variable (en este ejemplo, x) por un elemento en el universo considerado (que generalmente va a depender de la primera elección que hicimos), para la cual la afirmación es verdadera. Nótese que en este ejemplo, al tomar a un elemento arbitrario pero fijo en el conjunto de los números enteros, existe un elemento en $\mathbb{Z}$ (en nuestro ejemplo $-a$, que como se observa depende de la elección que hayamos hecho de a) para el cual la afirmación $P(a, -a)$ es verdadera.

Ejemplo 5.1.4. Consideremos el mismo predicado del ejemplo anterior $P(x, y)$: "$x+y = 0$" y consideremos la proposición $\exists x \forall y\ P(x, y)$ (note que el orden de los cuantificadores considerados fue cambiado con respecto al ejemplo anterior). Este tipo de afirmaciones, denominadas *existencial-universal*, son verdaderas cuando existe un reemplazo de la variable x, por algún elemento en nuestro universo de referencia, de manera que para cualquier reemplazo de la variable y, por cualquier elemento del universo de referencia, la propiedad $P(x, y)$ se satisface. La diferencia con el ejemplo anterior es que en este caso debemos encontrar un reemplazo de la variable x que debería funcionar para cualquier reemplazo de la variable y; diferente a lo que ocurre en el ejemplo anterior, donde el reemplazo para la variable x dependía fuertemente de la elección previa que se había hecho del reemplazo de la variable y. En el universo $U := \mathbb{Z}$ esta afirmación es falsa porque no podemos encontrar un elemento fijo en $\mathbb{Z}$, digamos a, que al sumarlo con cualquier elemento arbitrario de $\mathbb{Z}$ nos arroje como resultado 0. En efecto, si fijamos un elemento a entero existe un reemplazo de y en $\mathbb{Z}$ (por ejemplo $-a+1$, que sigue siendo entero) tal que $a + y = a + (-a + 1) = (a + (-a)) + 1 = 0 + 1 = 1 \neq 0$.

A continuación, estudiaremos algunas implicaciones y equivalencias semánticas que involucran afirmaciones con cuantificación múltiple; aunque para hacer esto debemos considerar cualquier universo de referencia U y cualquier posible interpretación en U de los predicados. Con el fin de ilustrar lo anterior, lo haremos en un caso particular. Tomemos como universo de referencia el conjunto de personas y de temas en matemáticas. Definamos el predicado $E(x, y)$ como "la persona x es especialista en el tema y". Veamos algunas de las posibles combinaciones al cuantificar las variables x, y y analicemos su significado en este ejemplo.

1. $\forall x \forall y\ E(x, y)$: "cualquier persona es especialista en cualquier tema".

2. $\exists x \forall y\ E(x, y)$: "hay al menos una persona que es especialista en todos los temas".

3. $\forall y \exists x\ E(x, y)$: "dado cualquier tema, hay al menos una persona que es especialista en ese tema".

4. $\exists y \exists x\ E(x, y)$: "existe al menos un tema en el que al menos una persona es especialista".

5. $\forall y \forall x\ E(x, y)$: "dado cualquier tema, cualquier persona es especialista en ese tema".

6. $\exists y \forall x\ E(x, y)$: "hay al menos un tema en el que todas las personas son especialistas".

7. $\forall x \exists y\ E(x, y)$: "cualquier persona es especialista en al menos un tema".

8. $\exists x \exists y\ E(x, y)$: "existe una persona que es especialista en al menos un tema".

Los siguientes razonamientos de algunas implicaciones semánticas, que involucran cuantificación múltiple, están basados solamente en nuestro ejemplo anterior a manera de ilustración, pero esto no quiere decir que si analizamos únicamente un ejemplo de un universo U y una sola interpretación de predicados en U sea suficiente para determinar una implicación semántica. Los argumentos hechos en las siguientes líneas se pueden replicar para cualquier U y cualquier interpretación del predicado $E(x, y)$ en U.

1. $\forall x \forall y \ E(x, y) \models \exists x \forall y \ E(x, y)$: si todas las personas son especialistas en todos los temas, en ese caso existiría al menos una persona (podemos escoger cualquiera en particular) que es especialista en todos los temas.

2. $\exists x \forall y \ E(x, y) \models \forall y \exists x \ E(x, y)$: si existe por lo menos una persona (llamémosla Sutana) que es especialista en todos los temas, podemos concluir que dado cualquier tema podemos encontrar al menos una persona (Sutana) que es especialista en ese tema (en este caso, en todos los temas podemos encontrar al menos una persona que se especializa en ese tema, en este caso siempre podremos exhibir a Sutana). Nótese que no podemos concluir el recíproco, en efecto, si dado cualquier tema hay una persona que se especializa en ese tema, no podemos concluir que haya una persona en común que se especialice en todos los temas simultáneamente (de hecho, es factible que haya temas que no tengan especialistas en común).

3. $\forall y \exists x \ E(x, y) \models \exists y \exists x \ E(x, y)$: si dado cualquier tema hay al menos una persona que se especializa en este, podemos concluir que por lo menos hay un tema (podemos escoger en particular, el que queramos) en el cual hay una persona que se especializa en ese tema. No podemos concluir el recíproco, porque si hay al menos un tema que tiene por lo menos un especialista, no podemos concluir que lo mismo ocurra para todos los temas (en ese caso, podría ocurrir a pesar de que haya un tema con al menos un especialista pueda existir un tema que no tenga especialistas).

4. $\exists x \exists y \ E(x, y) \equiv \exists y \exists x \ E(x, y)$: en este ejemplo que estamos estudiando, la frase de la izquierda dice que hay una persona que es especialista en algún tema. La frase de la derecha dice

que hay un tema en el que alguien es especialista. Si alguien es especialista (llamémoslo Perencejo) en un tema, para ese tema tenemos que hay un especialista en ese tema (Perencejo), luego tenemos la implicación $\exists x \exists y E(x, y) \models \exists y \exists x E(x, y)$. Por otro lado, si existe un tema (llamémoslo el tema X) para el cual hay un especialista (digamos Benito), entonces podemos decir que hay una persona (Benito) que es especialista en algún tema (el tema X). Por lo tanto, tenemos la otra implicación $\exists y \exists x \ E(x, y) \models \exists x \exists y \ E(x, y)$. En conclusión, ambas expresiones son equivalentes semánticamente hablando.

Es importante aclarar que para que tengamos las implicaciones y equivalencias analizadas atrás, el análisis anterior debe realizarse sin importar la interpretación que le hayamos dado al predicado $E(x, y)$. Nos centramos en este ejemplo particular, solo con el fin de analizar esas implicaciones dentro de un ejemplo particular.

5.2. Algunos ejemplos de cuantificación múltiple: axiomas sobre los números reales

El propósito de esta pequeña sección es presentar las propiedades más fundamentales de los números reales usando cuantificación múltiple (vea la Sección A.1 en el Apéndice A). Como es sabido, el conjunto de los números reales es denotado por $\mathbb{R}$. Usaremos el siguiente predicado $R(x)$:"x es un número real". Los símbolos '+' y '·' representan las operaciones adición y multiplicación de números reales, respectivamente. Vale la pena aclarar que cuando escribimos $x + y = z$, x y y son llamados *sumandos* y z es llamado *suma* o *resultado*. También, cuando escribimos $x \cdot y = z$, x y y son llamados *factores* y z es llamado *producto*.

1. $\forall x \forall y \ R(x+y)$: esta afirmación nos dice que para cualesquiera x y y números reales se tiene que la adición entre x y y, es decir, $x + y$, es también un número real. Esta propiedad es conocida como *ley clausurativa o de cerradura para la adición de reales*.

2. $\forall x \forall y \ (x + y = y + x)$: esta afirmación nos asegura que para cualesquiera x y y números reales se cumple que la suma de x y y es igual a la suma de y y x. Es decir, el orden de los sumandos no altera el resultado. Esta propiedad es conocidad como *ley conmutativa para la adición de reales*.

3. $\forall x \forall y \forall z \ ((x + y) + z = x + (y + z))$: esta propiedad es conocida como *ley asociativa para la adición de reales* y nos dice que para x, y y z reales arbitrarios vale que la suma entre $x + y$ y z es igual a la suma entre x y $y + z$. Esta propiedad también nos enseña cómo sumar tres o más números.

4. $\exists z \forall x \ (x + z = x)$: esta afirmación nos asegura que existe al menos un real z tal que para cualquier real x el resultado de sumar x y z no se modifica y continua siendo x. Esta propiedad es conocida como *ley modulativa* o *ley de elemento neutro para la adición de reales*. Cualquier z que satisfaga esta propiedad es llamado *módulo* o *elemento neutro* de la adición de reales. Uno de estos elementos z será representado por el símbolo 0, que es llamado *cero*. Es decir, $x + 0 = 0 + x = x$ sin importar la escogencia del número x. Aquí usamos que la adición de reales es conmutativa.

5. $\forall x \exists y \ (x + y = 0)$: en este caso la propiedad nos dice que para cada número real x siempre existe al menos un real y tal que la adición entre x y y es cero 0. Cualquier número y que satisfaga esta propiedad es llamado *opuesto aditivo* de x. Nótese que la existencia de y depende de x, es decir, si tomamos valores distintos de x, encontramos valores distintos para y. Por ejemplo, tomando $x = \pi$, y será $-\pi$, pero si $x = 2$, $y = -2$. Esta propiedad es conocida como *ley de los opuestos aditivos*.

6. $\forall x \forall y \ R(x \cdot y)$: esta afirmación nos dice que para cualesquiera x y y números reales se tiene que la multiplicación entre x y y, es decir, $x \cdot y$, es también un número real. Esta propiedad es conocidad como *ley clausurativa o de cerradura para la multiplicación de reales*.

7. $\forall x \forall y \ (x \cdot y = y \cdot x)$: esta afirmación nos dice que para cualesquiera x y y números reales se cumple que la multiplicación de x y y es igual a la multiplicación de y y x. Es decir, el orden de

los factores no altera el producto. Esta propiedad es conocida como *ley conmutativa para la multiplicación de reales*.

8. $\forall x \forall y \forall z\ ((x \cdot y) \cdot z = x \cdot (y \cdot z))$: esta propiedad es conocida como *ley asociativa para la multiplicación de reales* y nos dice que para x, y y z reales arbitrarios vale que la multiplicación entre $x \cdot y$ y z es igual a la multiplicación entre x y $y \cdot z$. Esta propiedad también nos enseña cómo multiplicar tres o más números.

9. $\exists z \forall x\ (x \cdot z = x)$: esta propiedad nos asegura que existe al menos un real z tal que para cualquier real x el producto de multiplicar x con z no se altera y continua siendo x. Esta propiedad es conocida como *ley modulativa* o *ley de elemento neutro para la multiplicación de reales*. Cualquier z que satisfaga esta propiedad es llamado módulo o elemento neutro de la multiplicación de reales. Uno de estos elementos z será representado por el símbolo 1, que es llamado *uno*. Es decir, $x \cdot 1 = 1 \cdot x = x$ sin importar la escogencia del número x. Aquí usamos que la multiplicación de reales es conmutativa.

10. $\forall x \exists y\ (\neg(x = 0) \to x \cdot y = 1)$: en este caso la propiedad nos dice que para cada número real x diferente de cero siempre existe al menos un real y tal que la multiplicación entre x y y es 1. Cualquier real y que satisfaga esta propiedad es llamado *inverso multiplicativo* de x. Nótese que la existencia de y depende de x, es decir, si tomamos valores distintos de x, encontramos valores distintos para y. Por ejemplo, tomando $x = \pi$, y será $\frac{1}{\pi}$, pero si $x = 2$, $y = \frac{1}{2}$. Esta propiedad es conocida como *ley de los inversos multiplicativos*.

11. $\forall x \forall y \forall z\ (x \cdot (y + z) = x \cdot y + x \cdot z)$: esta propiedad es conocida como *ley distributiva de la multiplicación respecto a la adición*, y afirma que para cualesquiera reales x, y y z se cumple que la multiplicación entre x y $y + z$ es igual a la adición entre $x \cdot y$ y $x \cdot z$. Aquí vemos que al lado izquierdo de la igualdad x está multiplicando a la adición entre x y y. En cambio al lado derecho x multiplica a y y este producto está sumado con la multiplicación entre x y z. Observando la igualdad de izquierda a derecha vemos que la x se distribuye multiplicando a y y a z. Como las igualdades son simétricas vale la pena mencionar que si observamos la igualdad de derecha a izquierda vemos que la

x no es distribuída sino mas bien recolectada. Vemos a x como factor del producto $x \cdot (y + z)$. Debido a esta observación, esta ley es también conocida como *factor común*.

5.3. Ejercicios

Ejercicio 5.3.1. Sean $U_1 := \mathbb{N}$, $U_2 := \mathbb{Z}$, $U_3 := \mathbb{Q}$ y $U_4 := \mathbb{R}$. Determine si las siguientes afirmaciones son verdaderas o falsas en cada uno de los anteriores conjuntos de referencia. Justifique su respuesta.

1. Para todo x y todo y, existe un z tal que $x - y = z$.
2. Para todo x existe un y tal que $x + y = y + x = 0$.
3. Para todo x existe un y tal que $xy = yx = 1$.
4. Para todo x existe un y tal que $y^2 = x$.
5. Para todo $x \geq 0$ existe y tal que $y^2 = x$.

Ejercicio 5.3.2. Tomando como base la intrepretación del predicado $E(x, y)$ dado atrás, escriba en correcto español las siguientes afirmaciones:

1. $\forall y \forall x \; E(x, y)$.
2. $\exists y \forall x \; E(x, y)$.
3. $\forall x \exists y \; E(x, y)$.
4. $\exists x \exists y \; E(x, y)$.

Ejercicio 5.3.3. Tomando como referencia la interpretación del predicado $E(x, y)$ dado atrás, analice las siguientes implicaciones y equivalencias y determine si en este ejemplo particular se satisfacen o no:

1. $\forall x \forall y E(x, y) \equiv \forall y \forall x E(x, y)$.
2. $\forall y \forall x \; E(x, y) \models \exists y \forall x \; E(x, y)$.
3. $\exists y \forall x \; E(x, y) \models \forall x \exists y \; E(x, y)$.
4. $\forall x \exists y \; E(x, y) \models \exists x \exists y \; E(x, y)$.

Ejercicio 5.3.4. Simbolice la negación de cada uno de los axiomas sobre los números reales presentados en la subsección 5.2 y luego escriba en correcto español su negación. Evite expresiones de la forma: "No es cierto que ...", donde los puntos suspensivos corresponden a la proposición original. Use equivalencias semánticas.

Ejercicio 5.3.5. Dé un ejemplo de un predicado, en algún universo, que muestre que la siguiente equivalencia semántica no es válida: $\exists x \forall y\, P(x, y) \equiv \forall y \exists x\, P(x, y)$.

Parte II

Estrategias de demostración

Lección *seis*

Demostraciones directas

Son conocidos al menos tres tipos de razonamiento que son usados contidianamente para construir conocimiento, estos son: *intuitivo*, *inductivo* y *deductivo*. El método intuitivo está basado en decidir qué es válido o verdadero dependiendo de algún tipo de corazonada o intuición. La inducción consiste en obtener afirmaciones válidas a partir de algunos hechos conocidos o circunstancias repetitivas. Es decir, se dictan generalidades a partir de algunas premisas particulares. Finalmente, el método deductivo parte de principios generales, axiomas o hechos que son verdaderos para llegar a conclusiones particulares. De estos, únicamente el método deductivo es el que aplicamos en las matemáticas, puesto que los métodos intuitivo e inductivo no son confiables y nos pueden llevar a cometer errores.

6.1. ¿Cómo se argumenta en matemáticas?

Una teoría matemática se compone de los siguientes tipos de afirmaciones:

- Axiomas o postulados: afirmaciones que suponemos que son verdad y en las cuales vamos a basar la teoría que queremos estudiar. Generalmente son contingencias (es decir, afirmaciones en las que hay contextos donde son verdaderas y hay contextos donde son falsas). La idea es deducir nuevas afirmaciones matemáticas que se siguen de las afirmaciones que tomamos como axiomas o postulados.

- Definiciones basadas en los axiomas, definiciones más simples o en afirmaciones demostradas dentro de una teoría.

- Afirmaciones que se derivan de los axiomas y definiciones, siguiendo las estrategias de demostraciones válidas que estudiaremos en la presente y las siguientes lecciones.
    - *Teorema:* afirmación central en una teoría.
    - *Proposición:* afirmación importante que no es muy significativa en una teoría.
    - *Lema:* afirmación probada previamente para demostrar teoremas y proposiciones.

- *Corolario:* afirmación que se sigue casi que inmediatamente de una afirmación central de la teoría.
- *Hecho*: afirmación que no es demostrada en el documento pero que es bastante conocida y se referencia de otros textos o es dejada como ejercicio para el lector.

6.2. Primer ejemplo: aritmética en el conjunto de los números enteros

En esta parte fijaremos algunas proposiciones básicas sobre la adición y la multiplicación de números enteros que tomaremos como axiomas. El conjunto de los números enteros será denotado por $\mathbb{Z}$. Los símbolos '+' y '·' representan las operaciones binarias *adición* y *multiplicación* de números enteros, respectivamente, y el símbolo '<' representa la relación binaria *ser menor que* en los números enteros.

1. $\mathbb{Z}$ es *cerrado* bajo la adición (+); es decir, para cualesquiera x, y enteros, se tiene que $x + y$ es también un número entero.

2. La operación adición (+) es *asociativa*; esto es, para todo x, y, z números enteros se tiene que $(x + y) + z = x + (y + z)$.

3. La operación adición (+) es *conmutativa*; es decir, para todo x, y números en $\mathbb{Z}$ se tiene que $x + y = y + x$.

4. Existe al menos un *neutro* en $\mathbb{Z}$ para la adición (+). Más precisamente, existe al menos un entero 0 tal que para todo x número entero se tiene que $x + 0 = x = 0 + x$.

5. Todo elemento en $\mathbb{Z}$ tiene un *opuesto aditivo*; es decir, para todo entero x existe y en $\mathbb{Z}$ tal que $x + y = 0$.

6. $\mathbb{Z}$ es *cerrado* bajo la multiplicación (·); es decir, para todo x, y números enteros, vale que $x \cdot y$ es también un número entero.

7. La operación multiplicación (·) es *asociativa*; es decir, para todo x, y, z en $\mathbb{Z}$ se tiene que $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

8. La operación multiplicación (·) es *conmutativa*; es decir, para cualesquiera x, y enteros se tiene que $x \cdot y = y \cdot x$.

9. Existe al menos un *neutro* en $\mathbb{Z}$ para la multiplicación $(\cdot)$; esto es, existe un entero 1 tal que para todo entero x se tiene que $x \cdot 1 = x$.

10. La operación multiplicación $(\cdot)$ *distribuye* con respecto a la adición $(+)$; es decir, para cualesquiera x, y, z números enteros se tiene que $x \cdot (y + z) = x \cdot y + x \cdot z$.

11. Los enteros *no tienen divisores de cero*; más precisamente, dados x, y enteros, si $x \neq 0$ y $y \neq 0$ entonces $x \cdot y \neq 0$.

12. La relación menor que $(<)$ es *irreflexiva* en los enteros; es decir, para todo x entero **no** se tiene que $x < x$ (lo que denotaremos por $x \not< x$).

13. La relación menor que $(<)$ es *transitiva* en $\mathbb{Z}$; es decir, para todo x, y, z números enteros tenemos que si $x < y$ y $y < z$ entonces $x < z$.

14. La relación menor que $(<)$ satisface *tricotomía* en $\mathbb{Z}$; es decir, dados x, y enteros, se tiene **una y solo una** de las siguientes afirmaciones: $x < y$ o $x = y$ o $y < x$.

15. La relación menor que $(<)$ es *monótona con respecto a la adición* $(+)$ en $\mathbb{Z}$; es decir, dados x, y, z enteros si $x < y$ entonces $x+z < y + z$.

16. La relación menor que $(<)$ es *monótona con respecto a la multiplicación* $(\cdot)$ en $\mathbb{Z}$; es decir, dados x, y, z enteros si $x < y$ y $0 < z$ entonces $x \cdot z < y \cdot z$.

17. $0 \neq 1$.

A partir de estos supuestos elementales (axiomas), estudiaremos la parte más fundamental de la teoría que se ha construido sobre la estructura de los números enteros, conformada por $\mathbb{Z}$, las operaciones adición $(+)$ y multiplicación $(\cdot)$, y la relación menor que $(<)$. Estos axiomas nos servirán como apoyo para ilustrar las estrategias de demostración que serán expuestas en esta y en las próximas lecciones.

La siguiente definición (ser menor o igual que) está basada en la noción "ser menor estricto que", de la que hemos axiomatizado atrás sus propiedades.

Definición 6.2.1. Dados x, y enteros, decimos que:

- Escribiremos $y > x$ como alternativa para $x < y$. Leeremos y *es mayor que* x.
- Diremos que x *es menor o igual que* y si y solo si $x < y$ o $x = y$. Escribiremos $x \leq y$.
- Escribiremos $y \geq x$ como alternativa para $x \leq y$. Leeremos y es mayor o igual que x.

A continuación, enunciaremos un hecho muy conocido en $\mathbb{Z}$ que se denomina *Algoritmo de la división*. Una demostración de este hecho puede ser encontrada en [7].

Teorema 6.2.2 (Algoritmo de la división). *Sean a entero cualquiera y b entero mayor que 0. Existen únicos enteros q y r tales que $0 \leq r$ y $r < b$ y $a = q \cdot b + r$. El entero q se denomina cociente y el entero r se denomina residuo.*

Aplicando el *Algoritmo de la división* al caso particular en el que $b = 2$, que es mayor que 0, obtenemos el siguiente resultado:

Corolario 6.2.3. *Sea a cualquier entero. Existen únicos enteros q y r tales que $0 \leq r$ y $r < 2$ y $a = 2 \cdot q + r$.*

Nótese que en este caso las únicas posibilidades para r son 0 y 1 y *solo una de esas posibilidades se puede dar*. Es decir, cualquier entero a es de la forma $2 \cdot q + 0$ (denominado número *par*) o de la forma $2 \cdot q + 1$ (denominado número *impar*), pero solo una de esas posibilidades se puede tener. Más formalmente:

Definición 6.2.4. Sea a número entero cualquiera.

- Decimos que a es un número *par* si y solo si existe $k \in \mathbb{Z}$ tal que $a = 2 \cdot k$.
- Decimos que a es un número *impar* si y solo si existe un número entero k tal que $a = 2 \cdot k + 1$.

6.3. Cuantificadores en demostraciones

6.3.1. Universales

Muchas veces debemos decidir si afirmaciones que contienen un cuantificador universal relativas a un cierto universo de referencia U; es decir, proposiciones de la forma $\forall x \varphi(x)$, son verdaderas o no. En el caso de que sean verdaderas, debemos elaborar una justificación que sea absolutamente clara. Recordemos que la afirmación $\forall x \varphi(x)$ es verdadera cuando cada una de las proposiciones $\varphi(a)$ son verdaderas para cada uno de los elementos a del universo de referencia U. Sin embargo, algunos universos de referencia tienen demasiados elementos, y verificar que para cada uno de los elementos a del universo de referencia U la afirmación $\varphi(a)$ es verdadera, puede ser un tarea tediosa e incluso imposible. Así que presentamos el siguiente *esquema*, para escribir demostraciones de afirmaciones universales, en el que usamos un objeto fijo que representa a cualquier elemento del universo de referencia.

Demostración. Sea a en U cualquiera pero fijo.

$$\vdots$$

Por lo tanto, $\varphi(a)$ es verdadera. Como a está en U y es arbitrario, concluimos que la afirmación "para todo x en U tenemos que $\varphi(x)$" es verdadera. ☑

Como un primer ejemplo de demostración de afirmaciones universales presentamos el siguiente hecho:

Corolario 6.3.1. *Todo entero es par o es impar, y no se da que simultáneamente sea par e impar.*

Demostración. Sea n número entero cualquiera pero fijo. Por el Corolario 6.2.3, tenemos que existen únicos enteros q y r, tales que $0 \leq r$ y $r < 2$ y $n = 2 \cdot q + r$. Vemos que las únicas posibilidades para r son $r = 0$ y $r = 1$. En el caso de que $r = 0$, tenemos que $n = 2 \cdot q$.

Esto significa por Definición 6.2.4 que n es par. Si sucede que $r = 1$, tenemos que $n = 2 \cdot q + 1$. Por la Definición 6.2.4 esto equivale a que n es impar. No se pueden dar las dos posibilidades, gracias a la unicidad de tal residuo r dada por el Teorema 6.2.2 del *Algoritmo de la división* y a que estamos suponiendo que $0 \neq 1$. ☑

6.3.2. Existenciales

Las afirmaciones existenciales son muy populares también, por lo que es necesario decidir, en muchas ocasiones, si una proposición de la forma $\exists x \varphi(x)$, relativa a un conjunto de referencia U, es verdadera o no. Para justificar plenamente que una proposición existencial es verdadera, esencialmente basta con exhibir al menos un elemento a del conjunto de referencia U para el cual la proposición $\varphi(a)$ es verdadera. A continuación, presentamos el siguiente *esquema* para escribir demostraciones de afirmaciones existenciales.

Demostración. Tomemos $x := a$ un elemento fijo en U (algunas veces debemos justificar en esta parte el por qué dicho elemento a está en el universo de referencia U).

$$\vdots$$

Por lo tanto, $\varphi(a)$ es verdadera. Como a es un elemento fijo de U tal que $\varphi(a)$ es verdadera, concluimos que la afirmación “existe x en U tal que $\varphi(x)$” es verdadera. ☑

Ejemplo 6.3.2. Existe un número entero x tal que $x + x = x$.

Demostración. Tomemos $x := 0$, el cual es entero gracias al *axioma de existencia de elemento neutro* para la suma de enteros. Como 0 es neutro para la suma en los enteros y en particular 0 es un número entero, entonces $0 + 0 = 0$. ☑

Teoremas compuestos por proposiciones existenciales son llamados *teoremas de existencia*. En el siguiente ejemplo no exhibimos propiamente un elemento del correspondiente universo de referencia que haga verdadera la proposición, pero apoyados en otro resultado se concluye la veracidad de la afirmación existencial involucrada.

Ejemplo 6.3.3. Existe un entero x tal que $x + 1 = 0$.

Demostración. Puesto que 1 es un número entero (su existencia está garantizada por el *axioma de existencia de elemento neutro* para la multiplicación de enteros), el axioma de *existencia de opuestos aditivos* en los números enteros nos garantiza la existencia de al menos un entero x tal que $x + 1 = 0$.

☑

6.4. Demostraciones directas

Usualmente, las afirmaciones en matemáticas y en las ciencias tienen la forma "Si ϕ entonces ψ", donde tanto ϕ como ψ no necesariamente son proposiciones simples, sino posiblemente proposiciones más complejas conformadas por cualquiera de los conectivos y los cuantificadores estudiados en las lecciones anteriores. En esta implicación, al conjunto de afirmaciones en ϕ las denominaremos *hipótesis* y a la afirmación ψ la denominaremos *conclusión*.

Dado que esta es la primera aproximación de algunos estudiantes a la manera como argumentamos en matemáticas, escribiremos explícitamente cuáles son las hipótesis y cuál es la conclusión antes de realizar las demostraciones de las primeras afirmaciones que vamos a estudiar.

En la estrategia de demostración, conocida como *demostración directa*, suponemos que las afirmaciones que conforman ϕ tienen valores de verdad, tales que hacen a ϕ verdadera y, por medio de argumentos coherentes, más precisamente, basados en la lógica y usando axiomas, definiciones u otras proposiciones que sean verdaderas, tenemos como propósito concluir que la afirmación ψ es también verdadera.

A manera de ilustración, haremos nuestra primera demostración en esta teoría sobre $\mathbb{Z}$ que estamos estudiando en estas notas.

Teorema 6.4.1. *Sea $0'$ un número entero que cumple la condición de ser neutro para la adición (+); es decir, para todo número entero x se tiene que $0' + x = x + 0' = x$. Sea 0 el neutro de la adición (+) descrito en el axioma de existencia de neutro dado atrás (axioma 4). Entonces $0' = 0$.*

Como anunciamos, presentamos las hipótesis y la conclusión de este teorema.

Hipótesis: 0 y $0'$ satisfacen la condición de ser neutro para la adición (+) en $\mathbb{Z}$; es decir, para todo número entero x se tiene que $0 + x = x + 0 = x$ y $0' + x = x + 0' = x$.

Conclusión: $0 = 0'$.

A continuación, presentaremos una *demostración directa* de este teorema; es decir, supondremos las hipótesis como ciertas (0 y $0'$ son neutros para la adición (+) en $\mathbb{Z}$) y mediante argumentos coherentes y totalmente justificados llegaremos a que $0 = 0'$.

Demostración. Sea $0'$ elemento en $\mathbb{Z}$ que es neutro para la adición (+) en $\mathbb{Z}$ y sabemos que 0 también es neutro para la adición (+) en $\mathbb{Z}$ (gracias al axioma de existencia de elemento neutro para + en $\mathbb{Z}$); es decir, para todo x en $\mathbb{Z}$ se tiene que $0 + x = x + 0 = x$ y para todo x en $\mathbb{Z}$ se tiene que $0' + x = x + 0' = x$. Por lo tanto,

$$\begin{aligned} 0 &= 0 + 0' && (0' \text{ es neutro de } + \text{ y tome } x \text{ como } 0, \\ & && \text{que es un elemento de } \mathbb{Z} \text{ fijo}) \\ &= 0' && (0 \text{ es neutro de } + \text{ y tome } x \text{ como } 0', \\ & && \text{que es un elemento de } \mathbb{Z} \text{ fijo}). \end{aligned}$$

☑

Nótese que en la demostración anterior, supusimos como verdad las hipótesis de ese enunciado (0 y $0'$ son neutros de la adición (+) de $\mathbb{Z}$) y a partir del significado de ser *elemento neutro* de la adición (+) pudimos concluir que 0 y $0'$ son en realidad el mismo elemento. Este resultado nos dice que solo existe un único elemento neutro para +.

A continuación, demostraremos algunas propiedades de la adición (+) y la multiplicación ($\cdot$) de números pares e impares.

Proposición 6.4.2. *Sean m, n números enteros cualesquiera.*

1. *Si m y n son pares, entonces $m + n$ es par.*
2. *Si m y n son impares, entonces $m + n$ es par.*
3. *Si m es par y n es impar, entonces $m + n$ es impar.*

1. **Hipótesis:** m y n son números pares.
   Conclusión: $m + n$ es par.

   Demostración. Sean m y n números enteros. Supongamos que m y n son números pares. Por Definición 6.3.1 de número par, existen k, l números en $\mathbb{Z}$ tales que $m = 2 \cdot k$ y $n = 2 \cdot l$. Por lo tanto,

$$
\begin{array}{rcll}
m + n & = & (2 \cdot k) + (2 \cdot l) & \text{(reemplazando } m \text{ por } 2 \cdot k \text{ y } n \\
 & & & \text{por } 2 \cdot l) \\
 & = & 2 \cdot (k + l) & \text{(distributividad de } \cdot \text{ con respecto} \\
 & & & \text{a } +).
\end{array}
$$

   Como k y l son números enteros, por la cerradura de la adición (+) en $\mathbb{Z}$, axioma 1, tenemos que $k + l$ es un número entero. Llamando q al número entero $k + l$, se tiene que $m + n = 2 \cdot q$. Entonces por Definición 6.3.1 de número par se concluye que $m + n$ es un número par.

   ☑

2. **Hipótesis:** m y n son impares.
   Conclusión: $m + n$ es par.

   Demostración. Sean m y n números enteros cualesquiera. Supongamos que m y n son impares. Por Definición 6.3.1 de número impar, existen números enteros k y l tales que $m = 2 \cdot k + 1$ y $n = 2 \cdot l + 1$. Por lo tanto,

$$
\begin{array}{rcll}
m + n & = & (2 \cdot k + 1) + (2 \cdot l + 1) & \text{(reemplazando } m \text{ por} \\
 & & & 2 \cdot k + 1 \text{ y } n \text{ por } 2 \cdot l + 1) \\
 & = & (2 \cdot k + 2 \cdot l) + (1 + 1) & \text{(asociatividad y conmuta-} \\
 & & & \text{tividad de } + \text{ en } \mathbb{Z}) \\
 & = & 2 \cdot (k + l) + (1 + 1) & \text{(distributividad de } \cdot \text{ con} \\
 & & & \text{respecto a } +) \\
 & = & 2 \cdot (k + l) + 2 & \text{(definición del número 2)} \\
 & = & 2 \cdot (k + l) + 2 \cdot 1 & \text{(1 es neutro de } \cdot \text{ en } \mathbb{Z}) \\
 & = & 2 \cdot ((k + l) + 1) & \text{(distributividad de } \cdot \text{ con} \\
 & & & \text{respecto a } +).
\end{array}
$$

Como k y l son números enteros, por la cerradura de la adición $(+)$ en $\mathbb{Z}$, axioma 1, tenemos que $k+l$ es un número entero. Como 1 es entero también, axioma 9, y de nuevo por la cerradura de la adición en $\mathbb{Z}$, axioma 1, obtenemos que $q := (k + l) + 1$ es un número entero. Por lo tanto, como $m + n = 2 \cdot q$, por la Definición 6.3.1 de número par, se concluye que $m + n$ es un número par.

☑

3. Es dejado como ejercicio para el lector.

Lema 6.4.3. *Para todo* $b \in \mathbb{Z}$, $0 \cdot b = 0$.

Hipótesis: b es número entero arbitrario.
Conclusión: $0 \cdot b = 0$.

Demostración. Sea b número entero arbitrario. Puesto que $0 \cdot b$ es un entero (por la *cerradura del producto en los números enteros*), por el *axioma de existencia de opuestos aditivos en los números enteros* existe un entero y tal que $0 \cdot b + y = y + 0 \cdot b = 0$. Por lo tanto,

$$
\begin{aligned}
0 &= 0 \cdot b + y \\
&\quad\ (y \text{ es un opuesto aditivo de } 0 \cdot b, \text{ hipótesis}) \\
&= (0 + 0) \cdot b + y \\
&\quad\ (0 + 0 = 0 \text{ puesto que } 0 \text{ es neutro de } + \text{ en } \mathbb{Z}) \\
&= (0 \cdot b + 0 \cdot b) + y \\
&\quad\ (\text{distributividad de } \cdot \text{ con respecto a } + \text{ en } \mathbb{Z} \\
&\quad\ \text{y conmutatividad de } \cdot \text{ en } \mathbb{Z}) \\
&= 0 \cdot b + [0 \cdot b + y] \\
&\quad\ (\text{asociatividad de } + \text{ en } \mathbb{Z}) \\
&= 0 \cdot b + 0 \\
&\quad\ (y \text{ es un opuesto aditivo de } 0 \cdot b, \text{ hipótesis}) \\
&= 0 \cdot b \\
&\quad\ (0 \text{ es el neutro de } + \text{ en } \mathbb{Z}).
\end{aligned}
$$

Con esto, terminamos la demostración del Lema 6.4.3. ☑

Proposición 6.4.4 (Unicidad de opuestos aditivos). *Sea a número entero cualquiera. Si existen b y c números enteros tales que $a+b=b+a=0$ y $a+c=c+a=0$; es decir, b y c son opuestos aditivos de a, entonces $b=c$.*

Hipótesis: a es cualquier número entero.
Existen b y c números enteros opuestos aditivos de a.
Conclusión: $b=c$.

Demostración. Sea a número entero cualquiera. Supongamos que existen b y c números enteros tales que b y c son opuestos aditivos de $a \in \mathbb{Z}$. Esto es, $a+b=b+a=0$ y $a+c=c+a=0$. Por lo tanto,

$$\begin{aligned} b &= b+0 \\ &\quad \text{(0 es neutro de + en } \mathbb{Z}) \\ &= b+(a+c) \\ &\quad (a+c=0,\ c \text{ es opuesto aditivo de } a) \\ &= (b+a)+c \\ &\quad \text{(asociatividad de + en } \mathbb{Z}) \\ &= 0+c \\ &\quad (b+a=0,\ b \text{ es opuesto aditivo de } a) \\ &= c \\ &\quad \text{(0 es neutro de + en } \mathbb{Z}). \end{aligned}$$

☑

Por el *axioma de existencia de opuestos aditivos* (axioma 5) sabemos que todo entero x tiene al menos un opuesto aditivo. Con lo demostrado arriba tenemos que tal opuesto aditivo es *único*. Por esta razón, dejaremos de referirnos a *un* opuesto aditivo de x y pasaremos a referirnos a *el* opuesto aditivo de x. La unicidad del opuesto aditivo para cada entero x nos permite denotarlo de una manera bien especial. Lo denotaremos por $-x$. Por lo tanto, si queremos mostrar que cierto entero y es $-x$, el opuesto aditivo de x, basta con mostrar que al sumarlo con x nos da como resultado 0, porque debido a la unicidad demostrada tendremos que ese entero y será el único opuesto aditivo de x.

Proposición 6.4.5. *Para todo a, b números enteros, $-(a \cdot b)=(-a) \cdot b$.*

Hipótesis: a y b son números enteros cualesquiera.
Conclusión: $(-a) \cdot b$ es *el* opuesto aditivo de $a \cdot b$.

Demostración. Sean a, b números enteros arbitrarios. Veamos que $(-a)\cdot b$ es el opuesto aditivo de $a \cdot b$. Para esto basta probar que $(-a) \cdot b + a \cdot b = 0$.

$$\begin{aligned}
(-a) \cdot b + a \cdot b &= (-a + a) \cdot b \\
&\quad \text{(distributividad de } \cdot \text{ con respecto a + en } \mathbb{Z} \\
&\quad \text{y conmutatividad de } \cdot \text{ en } \mathbb{Z}) \\
&= 0 \cdot b \\
&\quad (-a \text{ es opuesto aditivo de } a) \\
&= 0 \\
&\quad \text{(Lema 6.4.3)}.
\end{aligned}$$

Usando la Proposición 6.4.4, que nos dice que los opuestos aditivos son únicos, concluimos que $(-a) \cdot b$ es el opuesto aditivo de $a \cdot b$; es decir, $(-a) \cdot b = -(a \cdot b)$. ☑

A continuación, exploramos algunas propiedades de otra noción importante en los números enteros: la *divisibilidad*.

Definición 6.4.6 (Divisibilidad)**.** Sean a, b números enteros arbitrarios. Decimos que *a divide a b*, o que *b es múltiplo de a*, si y solo si existe $k \in \mathbb{Z}$ tal que $b = a \cdot k$. Este hecho será denotado por $a|b$.

Observación 6.4.7. Dados a y b números enteros, nótese que $a|b$ no es lo mismo que $a/b = \frac{a}{b}$; lo primero denota una relación entre a y b (a divide a b), mientras que lo segundo denota un número racional siempre que $b \neq 0$.

Proposición 6.4.8. *Sean a, b y c números enteros cualesquiera. Si $a|b$ y $b|c$ entonces $a|c$.*

Hipótesis: a, b y c son enteros arbitrarios tales que $a|b$ y $b|c$.
Conclusión: $a|c$.

Demostración. Sean a, b y c números enteros cualesquiera. Supongamos que $a|b$ y $b|c$. Como $a|b$, por Definición 6.4.6, existe k entero tal que

$$b = a \cdot k. \tag{6.1}$$

Como $b|c$, por Definición 6.4.6, existe m entero tal que

$$c = b \cdot m. \tag{6.2}$$

Reemplazando la igualdad (6.1) en (6.2), tenemos que

$$\begin{aligned} c &= b \cdot m \\ &= (a \cdot k) \cdot m \\ & \text{(reemplazamos } b \text{ por } a \cdot k) \\ &= a \cdot (k \cdot m). \\ & \text{(asociatividad de } \cdot \text{ en } \mathbb{Z}). \end{aligned}$$

Como k y m son enteros, por la cerradura de la multiplicación $(\cdot)$ en $\mathbb{Z}$, tenemos que $k \cdot m$ es también un número entero. Luego denotando $n := k \cdot m$, podemos escribir que $c = a \cdot n$. Finalmente, por la Definición 6.4.6 de divisibilidad concluimos que $a|c$. ☑

Proposición 6.4.9. *Todo entero divide a* 0.

En la hipótesis de esta proposición el sujeto no está explícito pero aquí lo dejaremos en evidencia y lo llamaremos b.

Hipótesis: b es un número entero arbitrario.
Conclusión: b divide a 0.

Demostración. Sea b un número entero cualquiera. Como por el Lema 6.4.3, $0 \cdot b = 0$, tomamos $k := 0$ que es entero por el *axioma de existencia de elemento neutro para + en los números enteros* (axioma 4). Así tenemos que la afirmación existe k entero tal que $b \cdot k = 0$ es verdadera, es decir, b divide a 0. ☑

6.5. Ejercicios

Ejercicio 6.5.1. Haga una demostración directa de las siguientes afirmaciones:

1. El producto de dos números enteros impares es impar.

2. Si n es un entero impar entonces $3n$ es impar.
3. Para todo a, b y c enteros se tiene que si a divide a b y a divide a c entonces a divide a $b + c$.
4. Si un entero es impar entonces es la suma de dos enteros consecutivos.
5. Si un entero es la suma de dos enteros consecutivos entonces es impar.

Ejercicio 6.5.2. Dados a, b enteros, decimos que:

- a es *positivo* si y solo si $0 < a$.
- a es *negativo* si y solo si $a < 0$.

La suma $a + (-b)$ la denotamos simplemente por $a - b$.
Sean a, b, c y d enteros. Demuestre las siguientes afirmaciones:

1. Si $a < b$, entonces $b - a$ es positivo.
2. Si $b - a$ es positivo, entonces $a < b$.
3. Si b es positivo, entonces $-b$ es negativo.
4. Si b es negativo, entonces $-b$ es positivo.
5. Si $-b$ es negativo, entonces b es positivo.
6. Si $-b$ es positivo, entonces b es negativo.
7. Si $a < b$, entonces $-b < -a$.
8. Si $b < a$ y $c < 0$, entonces $a \cdot c < b \cdot c$.
9. Si a y b son positivos, entonces $a + b$ es positivo.
10. Si a y b son positivos, entonces $a \cdot b$ es positivo.
11. Si a es positivo y b es negativo, entonces $a \cdot b$ es negativo.
12. Si a y b son negativos, entonces $a \cdot b$ es positivo.
13. Si $a \neq 0$, entonces $a^2 > 0$.

14. $0 \leq a^2$.

15. $-1 < 0 < 1$.

16. Definiendo $2 := 1 + 1$, $1 < 2$.

17. Si $a < b$ y $c < d$, entonces $a + c < b + d$.

Lección

siete

Demostraciones indirectas

7.1. Demostraciones por contrarrecíproca

Muchas de las afirmaciones en matemáticas son condicionales que tienen la forma $(\phi_1 \wedge \cdots \wedge \phi_n) \rightarrow \psi$, donde cada ϕ_j, con $j = 1, \cdots, n$, representa una de las hipótesis de la afirmación y ψ es la conclusión. Hemos visto que las demostraciones directas consisten en suponer como verdaderas las hipótesis $\phi_1, \cdots, \phi_n$ y a partir de ellas, por medio de razonamientos coherentes donde podemos usar axiomas, definiciones o afirmaciones previamente probadas, tenemos que llegar a que ψ es verdadera. Sin embargo, algunas veces este método de demostración no brinda los resultados esperados porque o bien estas demostraciones pueden ser muy engorrosas o porque simplemente no es posible llegar directamente a que ψ es también verdadera. Por el Ejercicio 2.5.5 6.

$$(\phi_1 \wedge \cdots \wedge \phi_n) \rightarrow \psi \equiv \neg\psi \rightarrow \neg(\phi_1 \wedge \cdots \wedge \phi_n),$$

que nos dice que la contrarrecíproca del condicional es semánticamente equivalente a la afirmación original, vemos que otra forma de probar ψ a partir de las hipótesis $\phi_1, \cdots, \phi_n$ es demostrar que de la hipótesis $\neg\psi$ se puede concluir $\neg(\phi_1 \wedge \cdots \wedge \phi_n)$.

Proposición 7.1.1. *Dado n en $\mathbb{Z}$, si n^2 es impar entonces n es impar.*

Notemos que al intentar hacer una demostración directa de este hecho, deberíamos partir de que n^2 es impar. Luego existiría un entero k tal que $n^2 = 2 \cdot k + 1$. Pero observemos que directamente de este hecho no podremos concluir que n (que intuitivamente sería una de las dos raíces cuadradas de $2 \cdot k + 1$) es impar también. Así que debemos hacer una demostración indirecta, probando un enunciado equivalente; en este caso demostraremos su afirmación contrarrecíproca: supondremos por hipótesis que n no es impar y por medio de argumentos coherentes concluiremos que es verdad que n^2 tampoco es impar.

Demostración. Sea n en $\mathbb{Z}$ cualquiera. Supongamos que n no es impar. Por el Corolario 6.3.1 tenemos que n es par. Por lo tanto, por

Definición 6.3.1, existe k en $\mathbb{Z}$ tal que $n = 2 \cdot k$. Por consiguiente,

$$\begin{aligned} n^2 &= (2 \cdot k) \cdot (2 \cdot k) \quad \text{(reemplazando } n \text{ por } 2 \cdot k\text{)}, \\ &= 2 \cdot (k \cdot (2 \cdot k)) \quad \text{(asociatividad de } \cdot \text{ en } \mathbb{Z}\text{)}. \end{aligned}$$

Como 2 y k son enteros, por la cerradura de la multiplicación en $\mathbb{Z}$ tenemos que $2{\cdot}k$ está en $\mathbb{Z}$ y así mismo que $k{\cdot}(2{\cdot}k)$ también está en $\mathbb{Z}$. Consecuentemente, tomando $m := k{\cdot}(2{\cdot}k)$ obtenemos que $n^2 = 2{\cdot}m$. Por Definición 6.3.1, concluimos que n^2 es par. Finalmente, como en el Corolario 6.3.1 se vió que un entero no puede ser simultáneamente par e impar, entonces n^2 no es impar. ☑

7.2. Demostraciones por reducción al absurdo

En la Proposición 3.3.1 vimos que si queremos demostrar que una afirmación ψ es verdadera a partir de ciertas hipótesis $\phi_1, \cdots, \phi_n$ supuestas verdaderas; es decir, queremos demostrar que $(\phi_1 \wedge \cdots \wedge \phi_n) \rightarrow \psi$, es suficiente con agregar $\neg\psi$ entre las hipótesis y demostrar que todas estas implican semánticamente una contradicción. Más precisamente, basta con tomar adicionalmente como hipótesis auxiliar la negación de ψ para demostrar que

$$\phi_1 \wedge \cdots \wedge \phi_n \wedge \neg\psi$$

implican una contradicción. Se obtiene una contradicción cuando se concluye, por ejemplo, la negación de alguna de las hipótesis ϕ_j, donde j es alguno de los subíndices $1, \cdots, n$, porque se tendría que ϕ_j y $\neg\phi_j$ serían verdaderas, es decir, $\phi_j \wedge \neg\phi_j$ sería verdadera, lo que es absurdo. Similarmente, otra forma de obtener una contradicción es demostrar la negación de algún hecho demostrado anteriormente.
Como, en este caso, no llegamos a mostrar directamente la conclusión a partir de las hipótesis sino que usamos un argumento auxiliar, este tipo de estrategia de demostración se conoce como *demostración indirecta*. Uno de los argumentos más famosos que usa esta estrategia de demostración es el hecho de que hay infinitos números primos. Precisemos la noción de número primo.

Definición 7.2.1. Sea n entero positivo. Decimos que n es *primo* si y solo si $n \neq 1$ y sus únicos divisores positivos son 1 y n.

A continuación, enunciaremos uno de los teoremas centrales de la teoría de números básica sobre $\mathbb{Z}$, el cual nos dice que todo entero positivo diferente de 1 es o bien primo o se puede escribir de manera única (salvo el orden) como producto de potencias de primos. Este resultado se conoce como el *Teorema fundamental de la aritmética* y lo usaremos para probar que hay infinitos números primos. No haremos su demostración en estas notas porque nos desviaría de nuestro objetivo que es introducir las diferentes estrategias de demostración en matemáticas; los lectores interesados pueden encontrar esta demostración en [1].

Teorema 7.2.2 (Teorema fundamental de la aritmética)**.** *Dado cualquier entero positivo $n \neq 1$, existen únicos primos $p_1, \cdots p_k$ y únicos enteros positivos $m_1, \cdots m_k$ tales que*

$$n = p_1^{m_1} \cdot \cdots \cdot p_k^{m_k}.$$

Volviendo a la infinitud del conjunto de los números primos, mostraremos aquí la prueba dada por Euclides. Su argumento consistió en suponer que no habían infinitos primos y a partir de ese supuesto se llega a una contradicción; esto es suficiente para demostrar que de hecho hay inifinitos primos, a la luz de la estrategia de demostración *reducción al absurdo*.

Aquí vamos a apelar a la intuición que tenemos de los conceptos de *finitud* e *infinitud*, sin embargo estos conceptos serán precisados en estas notas en las Lecciones 25 y 26.

Proposición 7.2.3. *Existen infinitos números primos.*

Demostración. Razonamos por reducción al absurdo. Supongamos que no hay infinitos números primos. Esto significa que existe una cantidad finita de ellos, digamos $p_1, \cdots, p_k$. Consideremos el entero positivo $n := (p_1 \cdot \cdots \cdot p_k) + 1$. Como cada p_j, $j = 1, 2, \ldots, k$, es primo, entonces $1 < p_j$. Nótese que $p_j \nmid n$ porque de lo contrario (obsérvese que volvemos a usar aquí reducción al absurdo) existiría q en $\mathbb{Z}$ tal que $n = p_j \cdot q$ y así

$$n = p_j \cdot (p_1 \cdot \cdots p_{j-1} \cdot p_{j+1} \cdot \cdots \cdot p_k) + 1 = p_j \cdot q.$$

Esto contradice la unicidad del residuo al dividir n entre p_j usando el Algoritmo de la división (Teorema 6.2.2). Como este razonamiento es válido para cualquier $j = 1, 2, \ldots, k$, entonces n no es divisible por ningún primo.

Pero el *Teorema fundamental de la aritmética* 7.2.2 nos dice, precisamente lo contrario, que hay algunos primos que dividen a n (contradicción). Por lo tanto, existen infinitos números primos. ☑

Vale la pena aclarar que en la demostración que acabamos de presentar, suponiendo que hay apenas finitos primos, obtuvimos que existe un entero $n > 1$ que no es divisible por ningún primo lo cual negaría el Teorema fundamental de la aritmética 7.2.2. Es decir, en esta demostración se negó un hecho que se aclaró previamente que es verdadero.

Otra de las demostraciones clásicas que utiliza la estrategia de demostración *reducción al absurdo* es el hecho de que $\sqrt{2}$ no es un número racional o, equivalentemente, la ecuación $x^2 = 2$ no tiene solución en los números racionales. Precisaremos primero algunas nociones que están detrás de este resultado.

Definición 7.2.4. Un número *racional* es todo aquel número que se pueda escribir de la forma $\frac{a}{b}$ donde a y b están en $\mathbb{Z}$ y $b \neq 0$. Si un número real no es racional, diremos que es *irracional*.

Definición 7.2.5. Dados a, b enteros diferentes de cero, el *máximo común divisor* de a y b es el mayor entero positivo que es divisor tanto de a como de b.

En esta parte supondremos que el lector está familiarizado con los *axiomas* de los números reales, que son estudiados con más cuidado en el curso de *Cálculo Diferencial en Una Variable*, aún así hacemos una presentación en el Apéndice A.

Hecho 7.2.6. *Para todo a real no negativo existe un único real x no negativo tal que $x^2 = a$. Dicho real se denota por $\sqrt{a}$.*

La demostración de este hecho se encuentra en el Apéndice A, en la prueba del Teorema A.4.2. La prueba es consecuencia directa del *Axioma de completez de los números reales*. En particular, como 2 es un real positivo entonces existe un único real no negativo x (que denotamos por $\sqrt{2}$) tal que $x^2 = 2$.

Habiendo precisado estas nociones, ahora sí podemos proceder a demostrar que $\sqrt{2}$ no es racional. En este caso es más sencillo suponer lo contrario (es decir, que $\sqrt{2}$ sí es racional) y a partir de este supuesto deducir una contradicción.

Proposición 7.2.7. *$\sqrt{2}$ no es racional.*

Demostración. Razonamos por *reducción al absurdo*. Supongamos que $\sqrt{2}$ es racional. Esto significa que existirían enteros a, b, con $b \neq 0$ tales que $\sqrt{2} = \frac{a}{b}$. Podemos suponer que esta expresión no se puede simplificar (si se pudiera simplificar, tome $a' \in \mathbb{Z}$ tal que $a = a' \cdot mcd(a, b)$ y $b' \in \mathbb{Z}$ tal que $b = b' \cdot mcd(a, b)$; nótese que $\frac{a}{b} = \frac{a'}{b'}$, donde $\frac{a'}{b'}$ no se puede simplificar más).

$$\begin{aligned} 2 &= \left(\sqrt{2}\right)^2 \text{ (definición de } \sqrt{2}) \\ &= \left(\frac{a}{b}\right)^2 \text{ (reemplazando } \sqrt{2} = \frac{a}{b}) \\ &= \frac{a^2}{b^2} \text{ (operaciones entre racionales).} \end{aligned}$$

Por lo tanto, $a^2 = 2 \cdot b^2$, esto es, a^2 es par. De esto, podemos concluir que a es par (por reducción al absurdo, si a no fuese par debería ser impar –por el Corolario 6.3.1– y en virtud del Ejercicio 6.5.1(1) tendríamos que a^2 sería impar, contradiciendo el Corolario 6.3.1). Como a es par, existe k en $\mathbb{Z}$ tal que $a = 2 \cdot k$, luego reemplazando el valor de a en las igualdades anteriores obtenemos que

$$2 \cdot b^2 = a^2 = (2 \cdot k)^2 = 4 \cdot k^2.$$

Por lo tanto,

$$b^2 = (4 \cdot k^2)/2 = 2 \cdot k^2.$$

Como k^2 es entero, concluimos que b^2 sería par. Realizando un argumento análogo, como el que hicimos para probar que a^2 par implica que a es par, podemos concluir que b es también par. Pero esto diría que $\frac{a}{b}$ se podría simplificar más. Esto contradice nuestro supuesto sobre a y b. Luego $\sqrt{2}$ no es racional. ☑

Obsérvese que en esta demostración no se negó una afirmación previamente probada, como se argumentó en la demostración de la prueba de la Proposición 7.2.3, sino que se obtuvo la contradicción al concluir como verdadera la negación de una proposición supuesta verdadera dentro de la misma demostración.

7.3. Ejercicios

Ejercicio 7.3.1. Demuestre por reducción al absurdo (para aquellos enunciados sobre números reales, pueden usar los axiomas de cuerpo y de orden de los números reales estudiados en cálculo diferencial):

1. Dos enteros consecutivos no pueden ser pares.
2. Si la suma de dos primos es primo, entonces uno de los primos es dos.
3. $\sqrt{3}$ es un número irracional.
4. $\sqrt{6}$ es un número irracional.
5. El producto de un racional no nulo y un irracional es un irracional.
6. Si c un entero positivo no primo, entonces existe un entero positivo b tal que b divide a c y $b \leq \sqrt{c}$.

Ejercicio 7.3.2. Utilice la contrarrecíproca para demostrar:

1. Para a, b, y c naturales, si a no divide al producto de b y c, entonces a no divide a b.
2. Para a y b naturales, si la suma de a y b no es par, entonces no es cierto que a y b son ambos pares o ambos impares.

Lección *ocho*

Demostraciones indirectas II. Refutando afirmaciones

En esta lección continuaremos presentando otros tipos de estrategias de demostraciones indirectas, esto es, demostraciones de teoremas en los que la proposición contenida es semánticamente equivalente a otra que nos muestra otro camino para realizar la demostración. Veremos demostraciones de bicondicionales, por casos (la hipótesis es una disyunción), y de disyunciones. También presentaremos cómo abordar demostraciones de afirmaciones que involucran cuantificación múltiple y también cómo refutar afirmaciones universales y existenciales.

8.1. Demostraciones de bicondicionales

Recordemos que dadas dos proposiciones ϕ y ψ, tenemos que el bicondicional $\phi \leftrightarrow \psi$ es semánticamente equivalente a $(\phi \rightarrow \psi) \wedge (\psi \rightarrow \phi)$. Esto quiere decir que si queremos demostrar afirmaciones de la forma ϕ si y solo si ψ, tenemos que demostrar primero que tomando como hipótesis ϕ podemos concluir ψ y también que tomando como hipótesis ψ podemos demostrar ϕ.

Como un ejemplo, daremos una demostración del siguiente hecho:

Proposición 8.1.1. *Sean m, n enteros. $m \cdot n$ es impar si y solo si m y n son impares.*

En esta afirmación debemos tomar como hipótesis que el producto $m \cdot n$ es impar, y de esto debemos demostrar que tanto m como n son impares. Luego, tomamos como hipótesis que, si m y n son impares simultáneamente entonces el producto $m \cdot n$ es impar.

Análisis del sentido ($\rightarrow$): sean m, n enteros, si $m \cdot n$ es impar entonces m y n son impares.

Hipótesis: $m \cdot n$ es impar.
Conclusión: m y n son impares.

Esta implicación es más sencilla de demostrar por el método de demostración indirecta conocido por *contrarrecíproca*.

Análisis del sentido ($\leftarrow$): sean m, n enteros, si m y n son impares entonces $m \cdot n$ es impar.

Hipótesis: m y n son impares.
Conclusión: $m \cdot n$ es impar.

En este caso, es sencillo hacer un argumento directo.

Demostración. ($\rightarrow$) Razonamos por contrarrecíproca. Supongamos que o bien m no es impar o bien n no es impar. Sin pérdida de generalidad podemos suponer que m no es impar. Por el Corolario 6.3.1 tenemos que m es par, luego por Definición 6.2.4 de número par tenemos que existe k entero tal que $m = 2 \cdot k$. De esta manera, por la propiedad asociativa de la multiplicación en $\mathbb{Z}$ tenemos que $m \cdot n = (2 \cdot k) \cdot n = 2 \cdot (k \cdot n)$. Como $k \cdot n$ es también entero (cerradura de $\cdot$ en $\mathbb{Z}$, puesto que $k, n \in \mathbb{Z}$), entonces $m \cdot n$ es par. En virtud del Corolario 6.3.1 nuevamente, como un entero no puede ser par e impar simultáneamente, entonces $m \cdot n$ no es impar.

($\leftarrow$) Recíprocamente, supongamos que tanto m como n son impares, entonces por Definición 6.2.4 de número impar existen enteros k, l tales que $m = 2 \cdot k + 1$ y $n = 2 \cdot l + 1$. De esta manera,

$$
\begin{aligned}
m \cdot n &= (2 \cdot k + 1) \cdot (2 \cdot l + 1) \\
&\quad \text{(reemplazando)} \\
&= (2 \cdot k) \cdot (2 \cdot l + 1) + 1 \cdot (2 \cdot l + 1) \\
&\quad \text{(distributividad de } \cdot \text{ con respecto a } + \\
&\quad \text{y conmutatividad de } \cdot \text{ con respecto a } +) \\
&= 2 \cdot [k \cdot (2 \cdot l + 1)] + 1 \cdot (2 \cdot l + 1) \\
&\quad \text{(asociatividad de } \cdot \text{ en } \mathbb{Z}) \\
&= 2 \cdot [k \cdot (2 \cdot l + 1)] + (2 \cdot l + 1) \\
&\quad \text{(1 es neutro de } \cdot \text{ en } \mathbb{Z}) \\
&= [2 \cdot [k \cdot (2 \cdot l + 1)] + 2 \cdot l] + 1 \\
&\quad \text{(asociatividad de } + \text{ en } \mathbb{Z}) \\
&= 2 \cdot [k \cdot (2 \cdot l + 1) + l] + 1 \\
&\quad \text{(distributividad de } \cdot \text{ con respecto a } + \text{)}
\end{aligned}
$$

Como $k \cdot (2 \cdot l + 1) + l$ es entero (¿por qué?) entonces por definición de número impar tenemos que $m \cdot n$ es impar. ☑

Como consecuencia del anterior hecho, tenemos el siguiente corolario. Dejamos su demostración como ejercicio para el lector.

Corolario 8.1.2. *Sean m, n enteros. $m \cdot n$ es par si y solo si o m es par o n es par.*

8.2. Demostración por casos

Algunas veces tenemos como hipótesis (explícita o implícita) en un enunciado matemático una disyunción; es decir, esa afirmación es de la forma $(\phi \vee \psi) \to \gamma$. No es difícil ver que $(\phi \vee \psi) \to \gamma$ es semánticamente equivalente a la proposición $(\phi \to \gamma) \wedge (\psi \to \gamma)$. Entonces demostrar una afirmación de este tipo es equivalente a tomar primero como hipótesis ϕ y demostrar, a partir de este supuesto, γ y luego suponer ψ como hipótesis y a partir de esto demostrar γ.

Ilustremos esta estrategia de demostración con un ejemplo.

Proposición 8.2.1. *Si n es un entero, entonces $n^2 + n$ es par.*

Análisis previo: nuestra hipótesis inicial es que n es un entero. Gracias al Corolario 6.3.1 sabemos que n es par o n es impar. Esto hace que tengamos como hipótesis implícita que n es par o n es impar. Primero, tomando como hipótesis que n es par, demostraremos que $n^2 + n$ es par; posteriormente tomamos como hipótesis que n es impar e igualmente debemos demostrar que $n^2 + n$ es par también. Esto es suficiente para demostrar lo pedido.

Demostración. Sea n número entero arbitrario pero fijo.

Caso 1: supongamos que n es par, entonces por el Corolario 8.1.2 tenemos que $n^2 := n \cdot n$ es par. Como n es par por hipótesis, por la Proposición 6.4.2 (1) tenemos que $n^2 + n$ es también par.

Caso 2: supongamos que n es impar, entonces por la Proposición 8.1.1 tenemos que $n^2 := n \cdot n$ es impar. Como por hipótesis n es impar, entonces por la Proposición 6.4.2 (2) tenemos que $n^2 + n$ es par.

Como todo entero n es par o impar (por el Corolario 6.3.1), entonces podemos concluir que para todo entero n tenemos que $n^2 + n$ es par.

☑

8.3. Demostración de disyunciones

Algunas veces necesitamos demostrar condicionales que tienen como consecuente una disyunción, es decir, tienen la forma $\phi \to (\psi \vee \gamma)$. Usaremos que estas proposiciones son semánticamente equivalentes a $(\phi \wedge \neg\psi) \to \gamma$ (ejercicio). Esta equivalencia nos muestra que si tenemos que demostrar este tipo de afirmación es suficiente suponer como hipótesis a ϕ y $\neg\psi$ para consecuentemente demostrar γ.

Veamos la demostración de una afirmación que tiene esta forma.

Proposición 8.3.1. *Si x y y son reales tales que $x \cdot y$ es irracional, entonces x es irracional o y es irracional.*

Análisis previo: nótese que en esta afirmación, la conclusión es una disyunción. En este caso, basta tomar como hipótesis que $x \cdot y$ es irracional, pero que x no lo es. Debemos demostrar que y es irracional, lo cual es equivalente a demostrar la afirmación original. Para esto último, podemos utilizar la estrategia de demostración que más nos convenga. En este caso, podemos razonar por *reducción al absurdo*. Para demostrar este hecho, primero debemos demostrar que producto de racionales es racional.

Lema 8.3.2. *Si x y y son racionales, entonces $x \cdot y$ es un número racional.*

Demostración. Supongamos que x y y son racionales. Esto significa que existen a, b, c y d enteros con $b \neq 0$ y $d \neq 0$ tales que $x = \frac{a}{b}$ y $y = \frac{c}{d}$. Por lo tanto, por la definición de multiplicación entre números racionales tenemos que $x \cdot y = \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$. Por la cerradura de la multiplicación en $\mathbb{Z}$ tenemos que $a \cdot c$ y $b \cdot d$ son números enteros. Como los enteros no tienen divisores de cero y $b \neq 0$ y $d \neq 0$, entonces $b \cdot d \neq 0$. Por lo tanto, $x \cdot y = \frac{a \cdot c}{b \cdot d}$ es un racional.

☑

Demostración de la Proposición 8.3.1. Supongamos que x y y son reales, tales que $x \cdot y$ es irracional y x no es irracional. Como x no es irracional, es racional. Razonando por *reducción al absurdo*, supongamos que y no es irracional. Esto significa que y es racional. Como x y y son racionales, entonces por el Lema 8.3.2 tenemos que $x \cdot y$ es racional, por lo tanto, $x \cdot y$ no es irracional. Esto contradice la hipótesis de esta proposición. Por lo tanto, y debe ser irracional. ☑

8.4. Cuantificación múltiple en demostraciones

Muchos teoremas tienen la forma "para todo elemento x en un universo U se satisface una propiedad $P(x)$". Para demostrar este tipo de afirmaciones, tenemos que justificar que para cualquier elemento arbitrario a (que en el argumento será arbitrario pero fijo) en ese universo U se tiene que ese elemento a satisface esa propiedad P. Pero también encontramos teoremas de la forma "existe un elemento x en un universo U que satisface una propiedad $P(x)$", en ese caso para demostrar este tipo de afirmaciones lo que debemos es exhibir un elemento b en U que cumpla esa propiedad. Es usual encontrar afirmaciones que combinen cuantificadores. Vamos a ilustrar con un par de ejemplos cómo proceder en cada caso.

Ejemplo 8.4.1. Veamos una demostración de la siguiente afirmación *universal-existencial*: para todo real a existe un real b tal que $a^2-b^2+4=0$. En este tipo de afirmaciones primero tenemos que fijar a arbitrario en el conjunto de los números reales y para ese elemento fijo pero arbitrario debemos exhibir un elemento b (que en principio podría depender de la escogencia de a) para el cual se cumpla la propiedad pedida (en este caso que $a^2-b^2+4=0$).

En estos casos, al fijar a real arbitrario lo que intentamos es "despejar" b para ver si tal b obtenido de esa manera es un número real. La obtención de dicho elemento b no corresponde realmente a la demostración, corresponde a lo que usualmente llamamos *análisis previo*.

Análisis previo: si tenemos que $a^2 - b^2 + 4 = 0$, tendríamos que $b^2 = a^2 + 4$. Sabemos que como para todo a real se tiene que $a^2 \geq 0$ y que $4 > 0$ entonces $a^2 + 4 > 0$, por lo tanto, sabemos que existe un único número real b tal que $b^2 = a^2 + 4$, el cual denotamos por $\sqrt{a^2+4}$. Entonces si consideramos a real arbitrario pero fijo, debemos hacer las cuentas para verificar que $b := \sqrt{a^2+4}$ es un número real (lo estamos exhibiendo) que cumple la propiedad deseada.

Demostración. Sea a número real arbitrario pero fijo. Como para todo a real se tiene que $a^2 \geq 0$ y $4 > 0$, entonces por monotonía del orden en los reales con respecto a la adición (ver apéndice) tenemos que $a^2 + 4 > a^2 \geq 0$, por lo tanto, existe un único número real $b \geq 0$ tal que $b^2 = a^2 + 4$, el cual denotamos por $b := \sqrt{a^2+4}$. De esta manera:

$$\begin{aligned}
a^2 - b^2 + 4 &= a^2 - \left(\sqrt{a^2+4}\right)^2 + 4 \\
&\quad \text{(reemplazando } b\text{)} \\
&= a^2 - (a^2 + 4) + 4 \\
&\quad \text{(definición de } \sqrt{a^2+4}\text{)} \\
&= (a^2 - a^2) + (-4 + 4) \\
&\quad \text{asociatividad de suma en } \mathbb{R} \\
&= 0 + 0 \\
&\quad (-a^2 \text{ es el opuesto aditivo de } a^2 \text{ y } -4 \text{ es} \\
&\quad \text{el opuesto aditivo de } 4) \\
&= 0 \\
&\quad (0 \text{ es el neutro de la suma en } \mathbb{R}).
\end{aligned}$$

Es así como hemos demostrado que dado cualquier número real a, existe un número real $b := \sqrt{a^2+4}$ tal que $a^2 - b^2 + 4 = 0$. ☑

Ejemplo 8.4.2. Demostremos la siguiente afirmación de tipo *existencial-universal*: existe un número real x tal que para todo número real y se tiene que $(3-x)(y^2+1) > 0$. Lo que hacemos primero es un *análisis previo* de esta afirmación, no es exactamente la demostración misma pero nos da idea de cuál es la elección de ese elemento x que debemos exhibir que cumple la afirmación pedida. Notemos que, en este caso, debemos exhibir un número real fijo x que sin importar cuál reemplazo de y hagamos por cualquier número real la afirmación pedida es verdadera.

En este caso, el mismo real x debe funcionar para cualquier real y, al contrario de lo que ocurrió en el ejemplo anterior (el real b encontrado en dicho ejemplo dependía fuertemente de la elección del real a arbitrario que se consideraba).

Análisis previo: sabemos que para cualquier y real $y^2 \geq 0$ y como $1 > 0$ entonces $y^2 + 1 > y^2 + 0 = y^2 \geq 0$. Luego lo que debemos encontrar es un real x tal que $3 - x > 0$, basta tomar un real x tal que $3 > x$. Por ejemplo, podemos tomar $x = 2$.

Demostración. Tomemos $x := 2$. Nótese que $3 - x = 3 - 2 = 1 > 0$. Sea y real arbitrario pero fijo. Como sabemos que el cuadrado de todo real es no negativo (ver apéndice), en particular esto se tiene para y (es decir, $y^2 \geq 0$). Como $1 > 0$, entonces $y^2 + 1 > y^2 + 0 = y^2 \geq 0$, por lo tanto, $y^2 + 1 > 0$. Como $3 - 2 = 1 > 0$ y $y^2 + 1 > 0$, entonces $(3 - 2)(y^2 + 1) > 0$ (producto de reales positivos es positivo). Por lo que $x := 2$ cumple la propiedad deseada. ☑

8.5. Refutando afirmaciones

Muchas veces debemos decidir si una afirmación es *verdadera* o *falsa*. En el caso de que una afirmación sea falsa, también es necesario justificar por qué lo es. Así que lo que tenemos que hacer es demostrar que la *negación* de dicha afirmación es verdadera. *Refutar* consiste precisamente en justificar que una cierta afirmación es falsa.

8.5.1. Refutando universales

Sabemos que la negación de una afirmación universal de la forma $\forall x \varphi(x)$ es equivalente a $\exists x \neg\varphi(x)$. Esto nos dice que cuando queremos refutar una afirmación universal, basta exhibir al menos un elemento en el universo de referencia donde estamos trabajando para el cual la afirmación dada originalmente falla. Este tipo de refutación de afirmaciones se conoce como *refutación por contraejemplo*, puesto que consiste en mostrar un ejemplo donde la afirmación universal falla.

Ejemplo 8.5.1. Refutemos la siguiente afirmación: "todo entero es par". Su negación es "existe un entero que no es par". Sabemos que esta última afirmación es verdadera, puesto que podemos exhibir un entero que no es par, por ejemplo 5, para el cual la afirmación universal falla (puesto que 5 no es par). Así, hemos refutado mostrando un contraejemplo (5) de la afirmación "todo entero es par".

8.5.2. Refutando existenciales

La negación de una afirmación existencial de la forma $\exists x\varphi(x)$ es equivalente a $\forall x\neg\varphi(x)$. Así, cuando queremos refutar una afirmación existencial, tenemos que mostrar que *ningún* elemento del universo de referencia donde estamos trabajando cumple la afirmación dada originalmente.

Ejemplo 8.5.2. Consideremos la afirmación: "existe un número real tal que su cuadrado es -2". Su negación es equivalente a la afirmación "para todo real se tiene que su cuadrado no es -2". Esta última afirmación es verdadera, puesto que dado cualquier real a, sabemos que $a^2 \geq 0 > -2$ y, por la tricotomía del orden en los números reales, tenemos que, $a^2 \neq -2$. Por lo tanto, ningún real a satisface $a^2 = -2$. Así, hemos refutado la afirmación dada originalmente.

Ejemplo 8.5.3. Refutemos la siguiente afirmación: "para todo real x existe un real y tal que $y^2 = x$". La negación de esta afirmación es equivalente a "existe un real x tal que para todo real y se tiene que $y^2 \neq x$". Esta última afirmación es verdadera, puesto que podemos exhibir un número real , -1 en este caso, tal que para todo real y^2 tenemos que $y^2 \neq -1$. Esto último es válido porque para todo real y se tiene que $y^2 \geq 0 > -1$ y, por la tricotomía del orden de los números reales tenemos que, $y^2 \neq -1$. De esta manera, hemos refutado con un contrajemplo (-1) la afirmación "para todo real x existe un real y tal que $y^2 = x$".

8.6. Ejercicios

Ejercicio 8.6.1. Use casos para demostrar (considerando como universo los números reales):

1. $|xy| = |x|\,|y|$.
2. $|x - y| = |y - x|$.
3. Existen a y b irracionales tales que a^b es racional. (indicación: considere $\sqrt{2}^{\sqrt{2}}$ y argumente por casos dependiendo del resultado de esa exponenciación).

Ejercicio 8.6.2. Encuentre para cada una de las siguientes afirmaciones un contraejemplo que la refute.

1. Si a, b y c son enteros positivos entonces $a^{(b^c)} = \left(a^b\right)^c$.
2. Si n es un entero positivo, entonces $n^2 + n + 41$ es primo.
3. Dos triángulos rectángulos tienen la misma área si y solo si las longitudes de sus hipotenusas son iguales.

Ejercicio 8.6.3. Tomando como universo el conjunto de los números naturales, el conjunto de los números enteros, el conjunto de los números racionales y el conjunto de los números reales, en cada uno de ellos considere cada una de las siguientes afirmaciones, y demuéstrelas o refútelas según sea el caso:

1. Para cada número no negativo s, existe un número no negativo t tal que $s \geq t$.
2. Existe un número no negativo t, tal que para todo número no negativo s se tiene que $s \geq t$.
3. Para cada número no negativo t, existe un número no negativo s tal que $s \geq t$.
4. Existe un número no negativo s, tal que para todo número no negativo t, se tiene $s \geq t$.

Lección *nueve*

Principio de inducción matemática

En esta parte de las notas vamos a suponer que el lector tiene cierta familiaridad con los números naturales. Así que no vamos a entrar en detalle sobre este sistema numérico, cuyo estudio será realizado con mayor profundidad en los cursos de Sistemas Numéricos e Introducción a la Teoría de Conjuntos de la carrera de Matemáticas de la Universidad Nacional de Colombia sede Bogotá.

Aclaramos que para nosotros el cero (0) es un número natural, a pesar de que, de acuerdo con el contexto, no lo es para algunos autores (por ejemplo, para Bloch en su texto [1], 0 no es natural). Sobre esto, haremos la respectiva discusión al abordar el tema de *cardinales finitos* (Lección 25).

Si pretendemos demostrar que una propiedad es verdadera para todos los números naturales, un intento ingenuo sería, primero, demostrar que la propiedad es verdadera para 0, luego para 1, después para 2 y así sucesivamente. El problema es que sabemos (intuitivamente por ahora, más adelante demostraremos este hecho, ver Corolario 25.2.7) que el conjunto de los números naturales $\mathbb{N}$ es *infinito*, por lo tanto, de esta manera nunca acabaremos de comprobar esta propiedad para todos los números naturales (por más que deleguemos esta tarea de generación en generación).

Así que para realizar este tipo de demostración, tenemos que hacerlo de alguna manera que sea aceptable por la comunidad matemática en general, y que además acabemos este proceso en algún momento.

9.1. Principio de inducción matemática forma I

A continuación, presentamos una descripción de este método de demostración por inducción, el cual es crucial para demostrar que una cierta propiedad $P(x)$ sobre los números naturales es verdadera para todo número natural n; es decir, para probar que $P(n)$ es verdadera para todo n número natural.

Lo primero que debemos verificar es que 0 satisface esta propiedad. Esto es, verificar que $P(0)$ es verdadera. Luego, suponemos que para cualquier número natural fijo n tenemos que $P(n)$ es verdadera (es decir, el natural n satisface la propiedad $P(x)$, este supuesto lo denominaremos *hipótesis de inducción*).

Si a partir del hecho de tomar como hipótesis que $P(n)$ es verdadera logramos demostrar que la propiedad $P(x)$ es verdadera para $n + 1$ (esto lo conoceremos como el *paso inductivo* en este tipo de argumento), entonces podemos pensar este argumento general como una "*máquina*" que nos permitirá realizar nuestra prueba requerida.

En efecto, tomando lo anterior y bajo el supuesto de que ya hemos verificado que para $n = 0$ la propiedad $P(x)$ es verdadera, esto implicaría que para $n + 1 = 1$ la propiedad $P(x)$ también es verdadera. Aplicando nuevamente esta "*máquina*" general de demostración a $n = 1$, como la propiedad $P(x)$ es verdadera para $n = 1$, entonces tendríamos que también la propiedad $P(x)$ es verdadera para $n + 1 = 2$. Del mismo modo, del hecho de la propiedad $P(x)$ sea verdadera para $n = 2$ podemos inferir que la propiedad $P(x)$ es también verdadera para $n + 1 = 3$, y así sucesivamente.

De esta manera, habiendo verificado la veracidad de la afirmación $P(x)$ para $n = 0$ y habiendo demostrado en general que si para cualquier natural n fijo suponiendo que $P(n)$ es verdadera (*hipótesis de inducción*) podemos deducir que $P(n + 1)$ es también verdadera (*paso inductivo*), entonces podemos inferir que la propiedad $P(x)$ es satisfecha por todos los números naturales. Esta forma de argumentación sobre los números naturales se conoce como *Principio de inducción matemática*. Más concretamente:

Hecho 9.1.1 (Principio de inducción matemática forma I). *Sea $P(x)$ una propiedad sobre los números naturales. Si se satisface lo siguiente:*

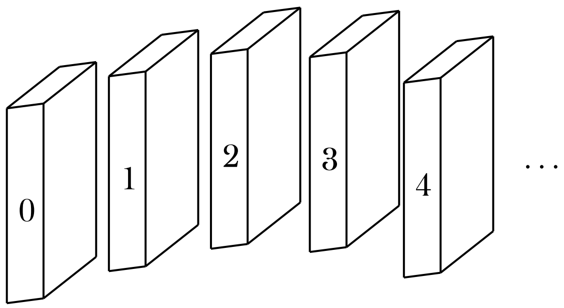
1. $P(0)$, y

2. para todo n natural, $P(n)$ es verdad implica que $P(n + 1)$ es verdad,

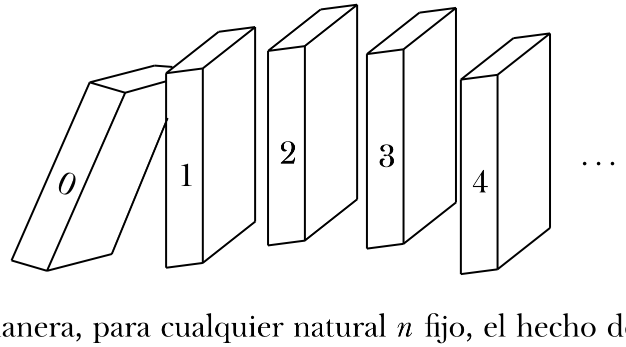
entonces todos los número naturales satisfacen la propiedad $P(x)$.

Este hecho lo presentamos sin demostración, dado que no tenemos aún las herramientas para hacerlo. Esto se verá con detalle cuando se construya el sistema de los números naturales $\mathbb{N}$ a partir de la axiomática de la Teoría de conjuntos de Zermelo-Fraenkel en el curso de Introducción a la Teoría de Conjuntos, ver [6]. Consideramos importante introducir esta forma de argumentación porque es una estrategia bastante utilizada para demostrar propiedades que satisfacen todos los números naturales; además de que, seguramente, varios estudiantes ya habrán utilizado este método en otros cursos como Cálculo Diferencial y la seguirán utilizando en cursos previos a Introducción a la Teoría de Conjuntos como por ejemplo Álgebra Lineal Básica y Sistemas Numéricos.

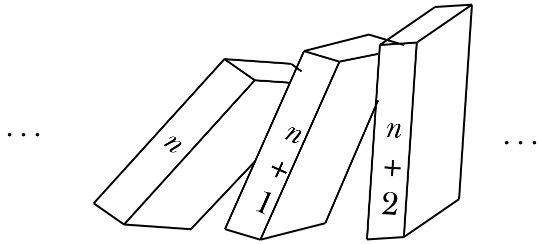
Para ayudar a entender mejor el porqué esta estrategia de demostración es aceptada, utilizamos la siguiente imagen, que consiste en representar cada número natural con una ficha de dominó. Colocamos de manera vertical primero la ficha que corresponde al natural 0, delante de ella la ficha que corresponde al natural 1, luego la ficha que corresponde al natural 2 y así sucesivamente.



Podemos representar el hecho de que n cumple la propiedad $P(x)$ como que la ficha que corresponde n cae. Así, $P(0)$ es verdad significa que la ficha que correspondiente a 0 cae.



De esta manera, para cualquier natural n fijo, el hecho de que la n-ésima ficha caiga implica que esto hace caer la ficha $(n + 1)$-ésima es justamente lo que corresponde al *paso inductivo* en el *Principio de inducción matemática forma I* (Hecho 9.1.1).



Consecuentemente, si la ficha 0 cae y el condicional correspondiente al paso inductivo vale, entonces la ficha 0 hace caer a la ficha que le sigue, la ficha 1. Como la ficha 1 cae, esta hace caer a la ficha 2, y así sucesivamente. De esta manera, podemos *ver* que todas las fichas caen; es decir, la propiedad $P(x)$ es satisfecha por todos los números naturales.

Ejemplo 9.1.2. Demostremos que para todo natural n se tiene que $n = 0$ o $n = k+1$ para algún natural k. Primero aislamos la propiedad a demostrar,

$$P(x)\text{: “}x = 0 \text{ o existe un natural } k \text{ tal que } x = k + 1\text{”.}$$

1. Como $0 = 0$ entonces la propiedad $P(x)$ es satisfecha por 0 (la disyunción $0 = 0$ o existe un natural k tal que $0 = k + 1$ es verdadera porque $0 = 0$).

2. Sea n número natural cualquiera pero fijo. Supongamos que la propiedad a demostrar $P(x)$ es verdadera para n. Esto significa que n es un natural tal que $n = 0$ o existe un natural k tal que $n = k+1$ (*hipótesis de inducción*). Vemos que al considerar $k := n$, que es un número natural, tenemos que $n + 1 = k + 1$. Luego, $P(n + 1)$ es verdadera puesto que la disyunción $n + 1 = 0$ o existe un natural k tal que $n + 1 = k + 1$ es verdadera.

Por el *Principio de inducción matemática forma I* tenemos que para cualquier número natural n, $n = 0$ o existe un natural k tal que $n = k + 1$.

Ejemplo 9.1.3. Demostremos que para todo natural n se tiene que $3 \mid 5^{2n} - 1$. Consideremos la propiedad

$$P(x)\text{: “}3|5^{2x} - 1\text{”.}$$

1. Tomando $n = 0$, notamos que $5^{2(0)} - 1 = 5^0 - 1 = 0 = 3 \cdot 0$, por lo tanto, $3|5^{2(0)} - 1$; es decir, $P(0)$ es verdadera.

2. Sea n cualquier natural fijo. Supongamos que $P(n)$ es verdadera, es decir $3|5^{2n} - 1$ (*hipótesis de inducción*). Así,

$$\begin{aligned}
5^{2(n+1)} - 1 &= 5^{2n+2} - 1\\
&= 5^{2n} \cdot 5^2 - 1\\
&\quad \text{(propiedades de potenciación de naturales)}\\
&= (3k + 1)(24 + 1) - 1\\
&\quad \text{(por hipótesis de inducción, existe}\\
&\quad k \text{ entero tal que } 5^{2n} - 1 = 3k)\\
&= (3(24k) + 24 + 3k + 1) - 1\\
&\quad \text{(distributividad de } \cdot \text{ con respecto a +,}\\
&\quad \text{conmutatividad y asociatividad de } \cdot)\\
&= (3(24k) + 24 + 3k) + (1 - 1)\\
&\quad \text{(asociatividad de +)}\\
&= 3(24k) + 24 + 3k\\
&\quad (1 - 1 = 0 \text{ y } 0 \text{ es neutro de + en } \mathbb{N})\\
&= 3(24k + 8 + k)\\
&\quad \text{(distributividad de } \cdot \text{ con respecto a +)}
\end{aligned}$$

   Puesto que $24k+8+k$ es un entero, tenemos que $3|5^{2(n+1)} - 1$; es decir, $P(n + 1)$ es verdadera.

Por el *Principio de inducción matemática forma I* concluímos que la propiedad $P(x)$ es satisfecha por todos los números naturales; es decir, $3|5^{2n} - 1$ para cualquier n número natural.

9.2. Principio de inducción matemática forma II

Algunas veces, todos salvo un número finito de naturales satisfacen cierta propiedad $P(x)$. Por ejemplo, todo natural $n \geq 2$ es primo o es producto de finitos primos (notemos que ni $n = 0$ ni $n = 1$ satisfacen esta propiedad). Esto corresponde al *Teorema fundamental de la aritmética* (Teorema 7.2.2) pero restringido a los números naturales. Ya habíamos mencionado este hecho cuando empezamos a hacer algunas demostraciones sobre el sistema de los números enteros, aunque no dimos una demostración, ahora tenemos las herramientas para hacerlo. Sin embargo, note que deberíamos empezar nuestro argumento inductivo desde $n = 2$ y no desde $n = 0$. ¿Por qué podemos hacer esto?

Supongamos que dado cualquier número natural $k > 0$ fijo, tenemos que demostrar que cierta propiedad sobre los números naturales $P(x)$ es satisfecha por todo natural $n \geq k$. Consideremos la propiedad auxiliar

$$Q(x)\text{: “}P(x+k) \text{ es verdadera”.}$$

Observamos que demostrar que $Q(n)$ es verdadera para todo n natural es lo mismo que demostrar que para todo n natural $P(n+k)$ es verdadera, equivalentemente que para todo natural $n \geq k$ tenemos que $P(n)$ es verdadera. Consecuentemente, notemos que demostrar $Q(0)$ es lo mismo que demostrar $P(0+k)$, es decir $P(k)$.

Así, si demostramos lo siguiente:

1. $Q(0)$ es verdadera (que ya vimos es equivalente a demostrar que $P(k)$ es verdadera),

2. Para cualquier número natural m fijo se tiene que $Q(m)$ es verdadera (equivalentemente, $P(m+k)$ es verdadera) implica que $Q(m+1)$ es verdadera (equivalentemente, $P(m+1+k)$ es verdadera),

entonces, aplicando el *Principio de inducción matemática forma I* (Hecho 9.1.1) a la propiedad $Q(x)$, todo número natural satisface la propiedad $Q(x)$; es decir, cualquier natural $n \geq k$ satisface la propiedad $P(x)$. De esta manera, hemos demostrado:

Proposición 9.2.1 (Principio de inducción matemática forma II). *Dada una cierta propiedad $P(x)$ sobre los números naturales y cualquier $k \geq 1$ número natural fijo. Si se satisface lo siguiente:*

1. *$P(k)$, y*
2. *Dado cualquier $m \geq k$ número natural, $P(m)$ es verdad implica que $P(m+1)$ es verdad,*

entonces todo número natural $n \geq k$ satisface la propiedad $P(x)$.

Observación 9.2.2. Notemos que el caso particular $k := 1$, en el *Principio de inducción matemática forma II*, corresponde a demostrar que una propiedad sobre los números naturales $P(n)$ es verdadera para todo natural $n \geq 1$. Esto implica que, en lugar de empezar a verificar la propiedad desde $n = 0$, la base de la inducción comienza en $n = 1$.

Esta versión del *Principio de inducción matemática* es utilizada por algunos autores, como Bloch (ver [1]), quienes consideran que los números naturales comienzan en *uno* y no incluyen el *cero* como número natural. Considerar al *cero* como número natural, o no, es una cuestión de conveniencia. Desde la perspectiva del proceso intuitivo de conteo, el cero podría parecer ajeno al conjunto de los números naturales, pues no representa una cantidad tangible de objetos ni está asociado a un proceso concreto de conteo. Sin embargo, si deseamos asignar un número que represente la cantidad de elementos del conjunto vacío, debemos considerar el cero como un número natural.

Ejemplo 9.2.3. Demostremos que para todo número natural $n \geq 1$ tenemos que $1 + \cdots + n = \frac{n(n+1)}{2}$. Aislemos la propiedad que tenemos que demostrar:

$$P(x)\text{: “}1 + \cdots + x = \tfrac{x(x+1)}{2}\text{”.}$$

1. Al tomar $n = 1$, vemos que $1 = \frac{1(2)}{2} = \frac{1(1+1)}{2}$, luego la afirmación $P(1)$ es verdadera.
2. Sea $n \geq 1$ cualquier natural pero fijo. Supongamos que $P(n)$ es verdadera, es decir $1 + \cdots + n = \frac{n(n+1)}{2}$ (*hipótesis de inducción*).

Así,

$$\begin{aligned}
1 + \cdots + n + (n+1) &= (1 + \cdots + n) + (n+1) \\
&\quad \text{(propiedad asociativa de la suma en } \mathbb{N}) \\
&= \frac{n(n+1)}{2} + (n+1) \\
&\quad \text{(hipótesis de inducción)} \\
&= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\
&= \frac{n(n+1) + 2(n+1)}{2} \\
&\quad \text{(suma de racionales con mismo} \\
&\quad \text{denominador)} \\
&= \frac{(n+2)(n+1)}{2} \\
&\quad \text{(factor común } n+1) \\
&= \frac{(n+1)(n+2)}{2} \\
&\quad \text{(conmutatividad del producto en } \mathbb{N}).
\end{aligned}$$

Por lo tanto, $P(n+1)$ es verdadera.

Por el *Principio de inducción matemática forma II*, podemos decir que para todo natural $n \geq 1$ se satisface que $1 + \cdots + n = \frac{n(n+1)}{2}$.

Ejemplo 9.2.4. Demostremos que para todo natural $n \geq 4$ tenemos que $3^n > n^3$. Consideremos la propiedad

$$P(x)\text{: “}3^x > x^3\text{”.}$$

1. Tomemos $n = 4$. Observamos que $3^4 = 81 > 64 = 4^3$, luego la propiedad $P(4)$ es verdadera.

2. Sea $n \geq 4$ cualquier natural pero fijo. Supongamos que $P(n)$ es cierta, es decir $3^n > n^3$ (*hipótesis de inducción*). Por lo tanto, por propiedad distributiva de la multiplicación respecto a la adición de números naturales tenemos que

$$(n+1)^3 = n^3 + 3n^2 + 3n + 1.$$

Como $n \geq 4 > 3$, por monotonía de la multiplicación de números naturales vemos que $3n^2 < n^3$. Similarmente,

$$\begin{aligned}
3n+1 &< 3n+n = 4n \\
&\quad (n \geq 4 > 1 \text{ y monotonía de la adición}) \\
&\leq n^2 < n^3 \\
&\quad (n \geq 4 > 1 \text{ y monotonía de la multiplicación}).
\end{aligned}$$

Teniendo en cuenta el aporte de los términos $3n^2(< n^3)$ y $3n+1(< n^3)$ tenemos que $(n+1)^3 < n^3 + n^3 + n^3 = 3n^3$. Usando la hipótesis de inducción y la monotonía de la multiplicación vemos que:

$$(n+1)^3 < 3 \cdot 3^n = 3^{n+1}.$$

Por el *Principio de inducción matemática* forma II (Proposición 9.2.1), tenemos que para todo natural $n \geq 4$ tenemos que $n^3 < 3^n$.

Observemos que esta propiedad falla en general en el caso de que $n < 4$: por ejemplo, si tomamos $n = 3$, $n^3 = 3^3 = 81 \not< 81 = 3^3 = 3^n$.

9.3. Principio de inducción matemática forma III

Otra manera de demostrar mediante inducción matemática que una cierta propiedad $P(x)$, sobre los números naturales, vale para cualquier natural consiste en suponer que todos los naturales menores estrictos que n, natural fijo, satisfacen $P(x)$ y a partir de este hecho demostrar que n también satisface la propiedad. Veremos que si demostramos lo anterior para cualquier número natural n, la propiedad $P(x)$ es verdadera para todo número natural.

Proposición 9.3.1 (Principio de inducción matemática forma III). *Dada $P(x)$ una cierta propiedad sobre los números naturales y m número natural arbitrario pero fijo. Si se satisface que:*

$(*)_m$ *para todo $k < m$, $P(k)$ es verdad implica que $P(m)$ es verdad,*

entonces la propiedad $P(x)$ es válida para todos los números naturales.

Demostración. Supongamos que la afirmación $(*)_m$ es verdadera para todo natural m. Consideremos la propiedad auxiliar

$$Q(x): \text{"para todo natural } k < x \text{ la afirmación } P(k) \text{ es verdadera".}$$

Veamos que la propiedad $Q(x)$ es satisfecha por todos los números naturales.

1. Razonando por *reducción al absurdo*, si $Q(0)$ fuera falsa existiría $k < 0$ tal que $P(k)$ es falsa. Contradicción, no hay naturales $k < 0$.

2. Sea n cualquier natural fijo tal que $Q(n)$ es verdadera (*hipótesis de inducción*). Esto significa que para todo $k < n$ tenemos que $P(k)$ es verdadera. Como estamos suponiendo que la afirmación $(*)_m$ es verdadera para todo natural m, en particular tenemos que $(*)_n$ es verdadera. Esto implica que $P(n)$ es verdadera. Por lo tanto, la propiedad $P(x)$ es satisfecha por todos los naturales $k \leq n$, más precisamente, por todos los naturales $k < n + 1$. Esto prueba que $Q(n + 1)$ es verdad.

Por el *Principio de inducción matemática forma I* (Hecho 9.1.1) tenemos que la propiedad $Q(x)$ es satisfecha por todos los números naturales.

Sea n cualquier número natural. Como $n < n + 1$ y, en particular, $Q(n + 1)$ es verdadera, esto significa que para todo natural $k < n + 1$ la afirmación $P(k)$ es verdadera. En particular, tomando $k := n$, tenemos que $P(n)$ es verdadera. Como n representa cualquier número natural, hemos probado lo que queríamos. ☑

Ejemplo 9.3.2 (Parte existencial en el Teorema fundamental de la aritmética)**.** Para demostrar que todo número natural $n \geq 2$ es primo o se puede expresar como producto de primos utilizamos el *Principio de inducción matemática forma III*. Esta prueba solo demuestra la existencia de tales números primos en la descomposición de cada natural $n \geq 2$ y no analizaremos la unicidad de dicha descomposición. Aislamos primero la propiedad a la cual aplicaremos el *Principio de inducción matemática forma III*:

$$P(x): \text{"si } x \geq 2, \text{ entonces } x \text{ es primo o es producto de finitos primos".}$$

Sea m cualquier natural fijo. Queremos demostrar la siguiente afirmación:

$(*)_m$ si todo $k < m$ satisface $P(k)$ (*hipótesis de inducción*), entonces $P(m)$ es verdadera (*paso inductivo*).

Si $m \leq 2$, el antecedente del condicional en $(*)_m$ es falso, luego en este caso la propiedad $(*)_m$ es verdadera.

Si $m > 2$, supongamos que todo natural $2 \leq k < m$ es primo o es producto de finitos primos (*hipótesis de inducción*). Tenemos que considerar dos casos:

1. Si m es primo, $P(m)$ es verdadera.
2. Si m no es primo, existen k, j naturales diferentes de m y de 1 tales que $m = k \cdot j$. Como $2 \leq k, j < m$, por la hipótesis de inducción tenemos que, tanto k como j satisfacen la propiedad $P(x)$, es decir, son primos o son producto de finitos primos. Por lo tanto, existen $p_1, \cdots, p_l, q_1, \cdots, q_t$ primos (l, t naturales ≥ 1) tales que $k = p_1 \cdot \ldots \cdot p_l$ y $j = q_1 \cdot \ldots \cdot q_t$. Entonces, $n = k \cdot j = p_1 \cdot \ldots \cdot p_l \cdot q_1 \cdot \ldots \cdot q_t$. Esto prueba que m es producto de primos y así la propiedad $P(m)$ es verdadera.

Consecuentemente, $(*)_m$ es verdadera.

Por el *Principio de inducción matemática forma III* (Proposición 9.3.1) tenemos que $P(n)$ es verdadera para todo natural n; es decir, si n es un natural tal que $n \geq 2$ entonces n es primo o es producto de finitos primos.

9.4. Ejercicios

Ejercicio 9.4.1. Demostrar que para todo número natural n se tiene que $2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$.

Ejercicio 9.4.2. Demuestre que dados reales $a, r, r \neq 1$, para todo natural n tenemos que $a + ar + \cdots + ar^n = \frac{a - ar^{n+1}}{1-r}$.

Ejercicio 9.4.3. Demuestre que si a, b son reales tales que $0 \leq a < b$, entonces para todo natural $n \geq 1$ tenemos que $0 < \frac{1}{(b+1)^n} < \frac{1}{(a+1)^n}$.

Ejercicio 9.4.4. Demuestre que para todo natural $n \geq 1$ tenemos que $1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$.

Ejercicio 9.4.5. Demuestre que para todo natural $n \geq 5$ tenemos que $3^n > (n+1)^3$. Analice qué pasa para los naturales $n \leq 4$.

Ejercicio 9.4.6. Demuestre que para todo natural $n \geq 3$ tenemos que $\left(1 + \frac{1}{n}\right)^n < n$.

Ejercicio 9.4.7. Determine dónde está el error en el siguiente razonamiento y justifique su respuesta. Supongamos que para cierto número natural $n \geq 2$, en cualquier conjunto de $k < n$ automóviles, todos ellos son blancos (*hipótesis de inducción*). Al tomar un conjunto de n automóviles, si al ordenarlos tomamos los $n - 1$ primeros tenemos por la *hipótesis de inducción* que esos $n - 1$ primeros automóviles son blancos, quedando solo el último automóvil por verificar que sea blanco; si tomamos los $n - 1$ últimos (que incluye el único automóvil que no hemos verificado su color) por la *hipótesis de inducción* todos ellos también son blancos, por lo tanto, todos los n automóviles son blancos. Por el *Principio de inducción matemática forma III* tenemos entonces que en todos los posibles conjuntos finitos de dos o más automóviles, todos ellos son blancos.

Parte III

Teoría intuitiva de conjuntos

Lección

diez

Nociones básicas

10.1. ¿Qué es un conjunto?

La noción de *conjunto* es la base de buena parte de lo que se conoce como *matemáticas modernas*. Desde tiempos antiguos, se considera la noción de *conjunto*, intuitivamente, como una colección de objetos. Basados en esta idea, podemos pensar por ejemplo en el conjunto de seres humanos, el conjunto de libros clásicos de la literatura en lengua española, el conjunto de estudiantes del curso Fundamentos de Matemáticas, el conjunto de ingredientes para elaborar una paella, entre otros. Sin embargo, al tomar los conjuntos como objetos matemáticos, debemos ser mucho más precisos.

Es hasta finales del siglo XIX, en los trabajos de Georg Cantor sobre series trigonométricas, que se empieza a considerar la *Teoría de conjuntos* como un área de estudio de las matemáticas. En los trabajos iniciales de Georg Cantor y Richard Dedekind, un conjunto era simplemente descrito por una propiedad común que tuvieran los objetos que se estaban agrupando. De manera más concreta, dada una propiedad $P(x)$, se podía considerar la colección de objetos x que cumplen dicha propiedad $P(x)$ (la cual se denotaba por $\{x : P(x)\}$). Diremos que, desde ese punto de vista, un objeto y pertenece al conjunto $\{x : P(x)\}$ si y solo si $P(y)$ es verdadera (i.e., y cumple la propiedad $P(x)$), lo cual denotaremos por $y \in \{x : P(x)\}$. Sin embargo, esta aproximación llevó a problemas. Si tomamos el "conjunto" $Y := \{x : x \notin x\}$, hay dos posibilidades: que Y sea elemento de sí mismo o que no. En el primer caso, si $Y \in Y$, el objeto Y debe cumplir la propiedad descrita para los elementos de Y, es decir, $Y \notin Y$. Por otro lado, si $Y \notin Y$, entonces el objeto Y cumple la propiedad que satisfacen los elementos del "conjunto" Y por lo que $Y \in Y$. Una situación contradictoria de este tipo es lo que se conoce como *paradoja*. Esta paradoja es debida a Bertrand Russell. Este es el motivo por el cual fue necesario introducir una mejor manera de determinar conjuntos, lo que llevó a la aproximación conocida como *Teoría axiomática de conjuntos*. Desde este punto de vista, el término conjunto *no está definido*. En efecto, un objeto se puede denominar *conjunto* si se puede garantizar su existencia por medio de algún axioma o teorema demostrado, por lo tanto, no es necesario dar una definición precisa de la noción de conjunto, de manera similar ocurre con las nociones de punto, recta y plano en *geometría euclidiana*.

Algunos de los sistemas axiomáticos de la Teoría de conjuntos más utilizados actualmente son los debidos a E. Zermelo y A. Fraenkel, denominado simplemente como ZF, el cual es tal vez el sistema más aceptado por la comunidad matemática en la actualidad. Hay otros sistemas axiomáticos para la Teoría de conjuntos que permiten estratificar objetos de estudio (conjuntos en un primer nivel, tomando colecciones de conjuntos que no son conjuntos –que se denominan *clases*–, y colecciones de clases que no son clases –que se denominan *conglomerados*– y así sucesivamente), como por ejemplo el sistema propuesto por Gödel, Bernays y von Neumann (conocido como GBN).

En estas notas no pretendemos abordar el punto de vista axiomático, dado que no es el objetivo central del curso y en la Universidad Nacional de Colombia, sede Bogotá, en el curso Introducción a la Teoría de conjuntos se estudia a profundidad esta aproximación. Aquí abordaremos el punto de vista conocido como *Teoría intuitiva de conjuntos*. Esto no quiere decir que no vayamos a hacer con cierta rigurosidad el estudio de los temas que trataremos en esta parte de las presentes Notas, lo que quiere decir es que no pretendemos profundizar en ninguna de estas axiomatizaciones. En esta parte pretendemos introducir el lenguaje básico conjuntista (e.g., contenencia entre conjuntos, igualdad entre conjuntos, operaciones básicas entre conjuntos, pareja ordenada, producto cartesiano, familias indexadas de conjuntos, entre otros) sin perder rigurosidad al momento de abordar estas nociones, presentando algunas demostraciones de propiedades fundamentales.

Intuitivamente, entenderemos *conjunto* como cualquier colección de objetos, no necesariamente matemáticos. Por ejemplo, podemos considerar como conjuntos la colección de seres humanos, la colección de estudiantes del curso Fundamentos de Matemáticas, la colección de letras del alfabeto español, entre otros. También, entenderemos como conjuntos la colección de los números naturales (denotado por $\mathbb{N}$), la colección de los números enteros (denotado por $\mathbb{Z}$), la colección de los números racionales (denotado por $\mathbb{Q}$), la colección de los números reales (denotado por $\mathbb{R}$) y la colección de los números complejos (denotado por $\mathbb{C}$). En textos de *Teoría axiomática de con-*

juntos (como por ejemplo [6]) se puede demostrar que a la luz de la axiomática ZF que dichas colecciones son conjuntos. Como lo mencionamos, no profundizaremos en puntos de vista axiomáticos, por lo que en estas notas no nos preocuparemos por garantizar su existencia como conjuntos.

Por otro lado, también consideraremos como conjunto una colección especial que no tiene elementos (el conocido *conjunto vacío*), que denotaremos por $\varnothing$ o por $\{\}$.

Un conjunto estará plenamente determinado por sus elementos. Desde el punto de vista intuitivo, consideramos dos maneras de determinar los elementos de un conjunto:

1. *Por extensión*: determinamos los elementos de un conjunto dando una lista explícita y exhaustiva de *todos* los elementos de un conjunto. En este caso, los elementos se delimitan por medio de los corchetes { y } y separando sus elementos por medio de comas (,).

2. *Por comprensión*: dado un conjunto de referencia U, tomamos aquellos elementos de U que cumplen una propiedad común $P(x)$, denotando este conjunto por $\{x \in U : P(x)\}$.

Observación 10.1.1. Al determinar un conjunto por comprensión, necesitamos obligatoriamente tomar un conjunto de referencia por varias razones: la primera es para evitar paradojas como la de Russell, y la segunda es para evitar ambigüedades; por ejemplo, si tomáramos como conjunto la colección $\{x : x \text{ es perfecto}\}$ y no determinamos el contexto, habría ambigüedad en el sentido de que no sabemos si estamos hablando de números naturales ("ser un número perfecto" como propiedad numérica, en el que un número natural se dice perfecto si y solo si es igual a la suma de sus divisores positivos propios) o de cosas o situaciones que tienen el grado máximo de una determinada cualidad.

Ejemplo 10.1.2. Los siguientes conjuntos están determinados por extensión, puesto que estamos listando explícitamente los elementos del conjunto:

1. $A := \{1, 2, 3, 4, 5\}$.

2. $B := \{a, e, i, o, u\}$.
3. $C := \{1, a, 2, b\}$.
4. $D := \{Pepe, Juana, Carlos\}$.
5. $E :=$ {auto, avión, tren}.

Observación 10.1.3. Un error muy común cometido por los estudiantes de primeros semestres es denotar al conjunto vacío por $\{\varnothing\}$ en vez de $\varnothing$ o $\{\}$. Notemos que $\{\varnothing\}$ tiene un elemento (precisamente $\varnothing$), por lo que *no* puede ser el conjunto vacío que describimos anteriormente.

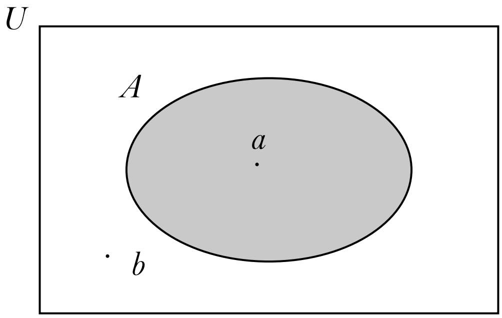
Ejemplo 10.1.4. Los siguientes conjuntos están determinados por comprensión:

1. Tomando como conjunto de referencia el conjunto de números naturales $\mathbb{N}$, el conjunto $A := \{x \in \mathbb{N} : x \text{ es primo}\}$ está determinado tomando del conjunto de referencia $\mathbb{N}$ aquellos números que sean primos.
2. Tomando como conjunto de referencia al conjunto U de estudiantes del curso Fundamentos de Matemáticas, el conjunto $B := \{x \in U : x \text{ es estudiante de matemáticas}\}$ está determinado por la propiedad $P(x)$: "x es estudiante de matemáticas".

10.1.1. Relación de pertenencia $\in$

La relación más básica y simple considerada en la teoría de conjuntos es la relación de *pertenencia*; la cual permite afirmar si un elemento forma parte de un conjunto. Si un conjunto A está determinado por extensión, decimos que un objeto *a pertenece* al conjunto A cuando el elemento a aparece explícitamente en la lista de elementos de A. En caso de que el conjunto A esté determinado por comprensión de la forma $A := \{x \in U : P(x)\}$, decimos que a es *elemento* de A si a está en el conjunto de referencia U y además a cumple la propiedad $P(x)$.

En cualquier caso, denotaremos el hecho de que a pertenezca a A por $a \in A$. En caso de que $a \in A$, también diremos que *a es elemento de A*. En caso de que un objeto b no pertenezca a un conjunto A, denotamos este hecho por $b \notin A$.



Representación de $a \in A$ y $b \notin A$.

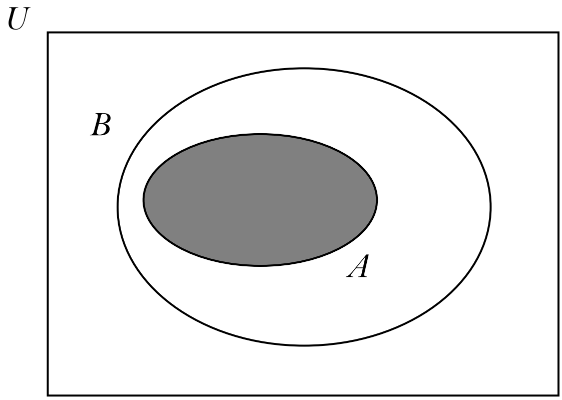
Ejemplo 10.1.5. Consideremos el conjunto $A := \{1, 2, 3, 4\}$. Como el elemento 2 aparece explícitamente en la lista de elementos de A, decimos que 2 pertenece a A (lo que denotamos por $2 \in A$). Nótese que 5 no aparece explícitamente en dicha lista, luego 5 no pertenece a A (este hecho lo denotamos por $5 \notin A$).

Ejemplo 10.1.6. Consideremos $B := \{x \in \mathbb{Z} : x \text{ es primo y par}\}$. Obsérvese que como 2 es un número entero, pertenece al conjunto de referencia $\mathbb{Z}$. Adicionalmente 2 es primo y par, entonces satisface la propiedad que describe los elementos del conjunto B. Por lo tanto, como 2 está en el conjunto de referencia del que tomamos los elementos de B y adicionalmente cumple la propiedad que describe los elementos de B, entonces $2 \in B$. Por otro lado, a pesar de que $5 \in \mathbb{Z}$ y 5 es primo, no es par. Como 5 no cumple la propiedad que describe los elementos de B, entonces $5 \notin B$. Consideremos $\frac{1}{2}$, como este objeto no está en el conjunto de referencia $\mathbb{Z}$, entonces inmediatamente podemos decir que $\frac{1}{2} \notin B$.

10.2. Contenencia entre conjuntos

A continuación, estudiaremos una relación entre conjuntos que, aunque no es la más básica por derivarse de la noción de pertenencia, es de las más importantes que consideraremos: la relación de *contenencia* entre conjuntos.

Definición 10.2.1. Sean A y B conjuntos cuyos elementos están dentro de un conjunto de referencia U. Decimos que *A está contenido en B* (o también que A es *subconjunto* de B) si y solo si todo elemento de A es elemento de B. Este hecho lo denoteremos por $A \subseteq B$.

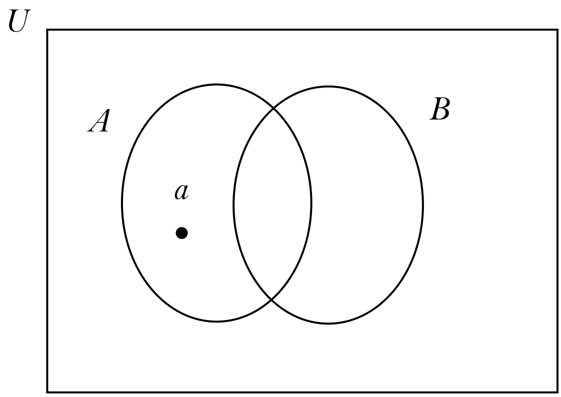


Representación de $A \subseteq B$.

Observación 10.2.2. Sean A y B conjuntos. Tomando los predicados $A(x)$: "$x \in A$" y $B(x)$: "$x \in B$", el hecho de que $A \subseteq B$ se escribe en lenguaje lógico de la siguiente manera:

$$\forall x\,(A(x) \to B(x)).$$

Analizando el caso de que A *no esté contenido en* B, vemos que en lenguaje lógico la negación de $\forall x\,(A(x) \to B(x))$ es equivalente semánticamente a $\exists x\,(A(x) \wedge \neg B(x))$, por lo tanto, tenemos que A *no está contenido en* B (lo que denotamos por $A \nsubseteq B$) si y solo si existe un elemento de A que no pertenece a B.



Representación de $A \nsubseteq B$.

Ejemplo 10.2.3. Considere los suguientes conjuntos $A := \{1, 2, 3, 4\}$ y $B := \{2, 4\}$. Notemos que $B \subseteq A$ puesto que todos los elementos de B (2 y 4) son elementos de A. Por otro lado, $A \nsubseteq B$ puesto que podemos exhibir al menos un elemento de A que no pertenece a B (por ejemplo, 3).

Observación 10.2.4. Un error frecuente cuando se empieza a estudiar estos conceptos es confundir las nociones *pertenencia* y *contenencia*. Cuando un objeto a pertenece a un conjunto A, algunas veces se cae en la tentación de afirmar que A contiene a a. En este caso la relación correcta es *pertenencia* y no *contenencia*. Recordemos que la relación de contenencia es una relación entre dos conjuntos, donde tenemos que todos los elementos de uno de ellos pertenecen al otro.

A continuación, demostraremos algunas propiedades básicas que tiene la relación de contenencia entre conjuntos.

Proposición 10.2.5. *Sean A, B y C conjuntos con elementos dentro de un conjunto de referencia U.*

1. $\varnothing \subseteq A$.

2. $A \subseteq A$.

3. *Si $A \subseteq B$ y $B \subseteq C$ entonces $A \subseteq C$.*

Demostración.

1. Por reducción al absurdo, supongamos que $\varnothing \nsubseteq A$. Por definición de contenencia entre conjuntos existiría un elemento x tal que $x \in \varnothing$ y $x \notin A$ (el hecho de que $x \in \varnothing$ contradice que $\varnothing$ no tiene elementos). Por lo tanto, $\varnothing \subseteq A$.

2. Por reducción al absurdo, si $A \nsubseteq A$, por definición de contenencia entre conjuntos existiría un elemento x tal que $x \in A$ pero $x \notin A$ (contradicción). Por lo tanto, $A \subseteq A$.

3. Sean A, B y C conjuntos tales que $A \subseteq B$ y $B \subseteq C$. Para demostrar que $A \subseteq C$ tomemos un elemento arbitrario de A y veamos que pertecene a C. Sea $x \in A$ cualquiera. Por hipótesis $A \subseteq B$ y puesto que $x \in A$, por definición de contenencia entre conjuntos, tenemos que $x \in B$. Por hipótesis tenemos también que $B \subseteq C$ y como $x \in B$, por definición de contenencia entre conjuntos, obtenemos que $x \in C$. Como hemos visto que todo elemento de A es elemento de C, por definición de contenencia entre conjuntos, concluimos que $A \subseteq C$.

☑

10.3. Igualdad entre conjuntos

Desde el punto de vista intuitivo, un conjunto está unívocamente determinado por sus elementos. De esta manera, decimos que dos conjuntos son iguales en caso de que tengan exactamente los mismos elementos. En otras palabras, dados dos conjuntos A y B, contenidos en un conjuntos de referencia U, decimos que A es igual a B (como conjuntos), en símbolos $A = B$, si y solo si $A \subseteq B$ (es decir, todo elemento de A es elemento de B) y adicionalmente $B \subseteq A$ (es decir, todo elemento de B es elemento de A). Con base en la Observación 10.2.2, en la que tomamos los predicados $A(x)$: "$x \in A$" y $B(x)$: "$x \in B$", el hecho de que $A = B$ se escribe en lenguaje lógico de la siguiente manera:

$$\forall x\,(A(x) \leftrightarrow B(x)).$$

A continuación, enunciaremos algunas propiedades básicas sobre la igualdad entre conjuntos.

Proposición 10.3.1. *Sean A, B y C conjuntos.*

1. *$A = A$.*
2. *Si $A = B$, entonces $B = A$.*
3. *Si $A = B$ y $B = C$, entonces $A = C$.*

Demostración.

1. Sea A conjunto. Por la Proposición 10.2.5 (2.), $A \subseteq A$. Como $A \subseteq A$, por la definición de igualdad entre conjuntos tenemos que $A = A$.

2. Sean A y B conjuntos tales que $A = B$. Por definición de igualdad entre conjuntos tenemos que $A \subseteq B$ y $B \subseteq A$. Por la conmutatividad de la conjunción, esto es lo mismo que decir que $B \subseteq A$ y $A \subseteq B$. Así, por definición de igualdad entre conjuntos tenemos que $B = A$.

3. Sean A, B y C conjuntos tales que $A = B$ y $B = C$. Por definición de igualdad entre conjuntos tenemos que $A \subseteq B$, $B \subseteq A$, $B \subseteq C$ y $C \subseteq B$; en particular tenemos que $A \subseteq B$ y $B \subseteq C$, luego por la Proposición 10.2.5 (3.) tenemos que $A \subseteq C$. También, en particular $C \subseteq B$ y $B \subseteq A$. Por la Proposición 10.2.5

(3.) tenemos que $C \subseteq A$. Como $A \subseteq C$ y $C \subseteq A$, por la definición de igualdad entre conjuntos concluimos que $A = C$. ☑

10.4. Conjunto potencia o conjunto de partes

Definición 10.4.1. Dado un conjunto A, la colección de todos los subconjuntos de A es un conjunto y lo denominamos *conjunto potencia* de A, el cual denotamos por $\mathscr{P}(A) := \{B : B \subseteq A\}$. Este conjunto es también conocido como *conjunto de partes* de A.

Observación 10.4.2. Dado cualquier conjunto A, como $\varnothing \subseteq A$ entonces $\varnothing \in \mathscr{P}(A)$. Por lo tanto, como $\mathscr{P}(A)$ tiene al menos un elemento ($\varnothing$) entonces $\mathscr{P}(A) \neq \varnothing$.

Proposición 10.4.3. *Si $A \neq \varnothing$ es conjunto, entonces $A \nsubseteq \varnothing$.*

Demostración. Sea $A \neq \varnothing$ conjunto. Luego existe $x \in A$. Puesto que por definición $\varnothing$ no tiene elementos, entonces $x \notin \varnothing$. Por la negación de la definición de continencia de conjuntos, $A \nsubseteq \varnothing$. ☑

Corolario 10.4.4. *Sea A conjunto. Si $A \subseteq \varnothing$ entonces $A = \varnothing$.*

Demostración. Corresponde a la afirmación contrarrecíproca de la proposición anterior. ☑

Ejemplos 10.4.5.

1. Del corolario anterior, podemos decir que $\mathscr{P}(\varnothing) = \{\varnothing\}$.

2. Si $A := \{a\}$, nótese que $\mathscr{P}(A) = \{\varnothing, \{a\}\}$.

3. Si $A := \{a, b\}$, con $a \neq b$, no es difícil observar que el conjunto potencia de A es: $\mathscr{P}(A) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$.

4. Si $A := \{a, b, c\}$ con a, b, c diferentes dos a dos, se ve que $\mathscr{P}(A) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$.

Proposición 10.4.6. *Si A y B son conjuntos tales que $A \subseteq B$, entonces $\mathscr{P}(A) \subseteq \mathscr{P}(B)$.*

Demostración. Sea $X \in \mathcal{P}(A)$ cualquiera. Por definición de conjunto potencia tenemos que $X \subseteq A$. Como por hipótesis tenemos que $A \subseteq B$ entonces por la Proposición 10.2.5 (3) tenemos que $X \subseteq B$. Por definición de conjunto potencia tenemos que $X \in \mathcal{P}(B)$. Como todo elemento de $\mathcal{P}(A)$ es elemento de $\mathcal{P}(B)$, por definición de contenencia entre conjuntos tenemos que $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. ☑

10.5. Ejercicios

Ejercicio 10.5.1. ¿Cuál es el número de elementos que tiene el conjunto $\{a, b, c, \{b, c\}\}$?

Ejercicio 10.5.2. Dé ejemplos de conjuntos A y B para los cuales es válido que $A \in B$ y $A \subseteq B$.

Ejercicio 10.5.3. Sea $A = \{a, b, c, d\}$. Liste todos los elementos de $\mathcal{P}(A)$.

Ejercicio 10.5.4. Vimos que $\mathcal{P}(\varnothing) = \{\varnothing\}$ y $\{\varnothing\} \neq \varnothing$. Determine $\mathcal{P}(\{\varnothing\})$.

Ejercicio 10.5.5. Liste todos los elementos de $\mathcal{P}(\mathcal{P}(\mathcal{P}(\varnothing)))$ y también los de $\mathcal{P}(\mathcal{P}(\mathcal{P}(\{\varnothing\})))$.

Ejercicio 10.5.6. Considere los conjuntos $A = \{0, \{0\}, \{0, 1\}\}$ y $B = \{0, 1, \{0\}, \{0, 1\}, A\}$. Llene el espacio vacío con los símbolos $\in$ o $\notin$, $\subseteq$ o $\nsubseteq$, de manera que se obtenga una proposición verdadera. Justifique su respuesta.

(a) $\{0, 1\}$ ___ A.	(b) $\{0, 1\}$ ___ A.	(c) A ___ B.
(d) A ___ B.	(e) $\{1\}$ ___ A.	(f) $\{1\}$ ___ B.
(g) $\{0, 1\}$ ___ B.	(h) B ___ A.	(i) 1 ___ B.
(j) B ___ A.	(k) 0 ___ A.	(l) $\{0\}$ ___ A.

Lección

once

Operaciones entre conjuntos

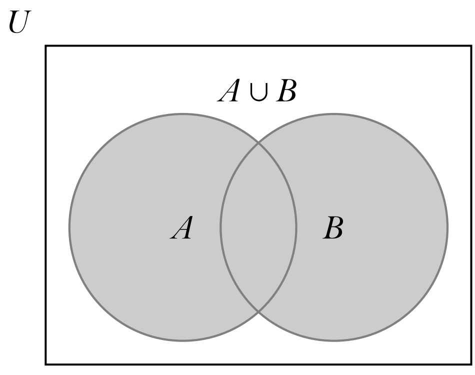
En esta lección estudiaremos algunas manera de obtener (posiblemente) nuevos conjuntos a partir de otros dados previamente. Primero, estudiaremos algunas de las operaciones elementales entre conjuntos: uniones e intersecciones de dos conjuntos. Posteriormente, hablaremos sobre la diferencia entre conjuntos (teniendo como caso particular el complemento de un conjunto).

11.1. Unión e intersección entre conjuntos

Definición 11.1.1 (Unión entre conjuntos). Sean U conjunto de referencia y $A, B \subseteq U$ conjuntos. Definimos la *unión* entre A y B como el conjunto conformado por todos los elementos de U que pertenecen a A o que pertenecen a B. Dicho conjunto lo denotamos por

$$A \cup B := \{x \in U : x \in A \text{ o } x \in B\}.$$

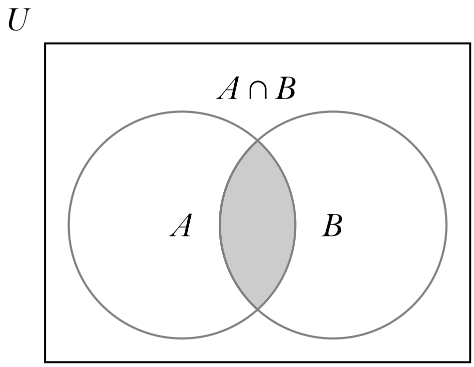
En otras palabras, para cualquier $x \in U$, $x \in A \cup B$ si y solo si $x \in A$ o $x \in B$.



Definición 11.1.2 (Intersección entre conjuntos). Sean U conjunto de referencia y $A, B \subseteq U$ conjuntos. Definimos la *intersección* entre A y B como el conjunto conformado por todos los elementos de U que pertenecen a A y que pertenecen a B simultáneamente. Dicho conjunto lo denotamos por

$$A \cap B := \{x \in U : x \in A \text{ y } x \in B\}.$$

En otras palabras, para cualquier $x \in U$, $x \in A \cap B$ si y solo si $x \in A$ y $x \in B$.



Ejemplo 11.1.3. Considere el conjunto de referencia $U := \mathbb{N}$ el conjunto de los números naturales, $A := \{1, 2, 3\}$ y $B := \{3, 4, 5\}$. Nótese que la unión de A y B corresponde al conjunto conformado por los elementos de $\mathbb{N}$ que están en alguno de esos dos conjuntos, es decir $A \cup B := \{1, 2, 3, 4, 5\}$. La intersección de A y B corresponde al conjunto cuyos elementos son los del conjunto de referencia $\mathbb{N}$ comunes a A y a B, es decir $A \cap B = \{3\}$.

Proposición 11.1.4. *Sean U conjunto de referencia y $A, B, C, X, Y \subseteq U$ conjuntos.*

1. *$A \cap B \subseteq A$ y $A \cap B \subseteq B$.*
2. *Si $X \subseteq A$ y $X \subseteq B$, entonces $X \subseteq A \cap B$.*
3. *$A \subseteq A \cup B$ y $B \subseteq A \cup B$.*
4. *Si $A \subseteq Y$ y $B \subseteq Y$, entonces $A \cup B \subseteq Y$.*
5. *$A \cup B = B \cup A$ y $A \cap B = B \cap A$.*
6. *$(A \cup B) \cup C = A \cup (B \cup C)$ y $(A \cap B) \cap C = A \cap (B \cap C)$.*
7. *$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ y $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.*
8. *$A \cup \varnothing = A$ y $A \cap \varnothing = \varnothing$.*

9. $A \cup A = A$ *y* $A \cap A = A$.

10. $(A \cap B) \cup A = A$ *y* $A \cap (A \cup B) = A$.

11. *Si* $A \subseteq B$, *entonces* $A \cap C \subseteq B \cap C$ *y* $A \cup C \subseteq B \cup C$.

Demostración. Sean U conjunto de referencia y $A, B, C, X, Y \subseteq U$ conjuntos.

1. Veamos que $A \cap B \subseteq A$. Sea $x \in A \cap B$ cualquiera pero fijo. Por definición de interesección entre conjuntos tenemos que $x \in A$ y $x \in B$, en particular $x \in A$. Como todo elemento de $A \cap B$ es elemento de A, por definición de contenencia entre conjuntos tenemos que, $A \cap B \subseteq A$. De manera análoga podemos demostrar que $A \cap B \subseteq B$ (ejercicio).

2. Supongamos que $X \subseteq A$ y $X \subseteq B$. Sea $x \in X$ cualquiera pero fijo. Como por hipótesis $X \subseteq A$, entonces, por definición de contenencia entre conjuntos tenemos que, $x \in A$. Como también por hipótesis $X \subseteq B$ entonces, por definición de contenencia entre conjuntos vale que, $x \in B$. Vemos que $x \in A$ y $x \in B$, entonces, por definición de intersección entre conjuntos tenemos que, $x \in A \cap B$. Hemos probado que todo elemento de X es también elemento de $A \cap B$, por lo tanto, por definición de contenencia entre conjuntos tenemos que, $X \subseteq A \cap B$.

   Dejamos como ejercicio para el lector los numerales 3, 4, 5, 6 y 7.

8. Veamos primero que $A \cup \varnothing = A$. Por la Proposición 11.1.4 (3), tenemos que $A \subseteq A \cup \varnothing$. Para completar nuestra demostración basta probar que $A \cup \varnothing \subseteq A$. Sea $x \in A \cup \varnothing$ cualquiera. Por definición de unión entre conjuntos tenemos que $x \in A$ o $x \in \varnothing$. Por definición de $\varnothing$ tenemos que $x \notin \varnothing$, entonces $x \in A$. Luego, todo elemento de $A \cup \varnothing$ es elemento de A, entonces, por definición de contenencia entre conjuntos tenemos que, $A \cup \varnothing \subseteq A$. Como tenemos que $A \cup \varnothing \subseteq A$ y $A \subseteq A \cup \varnothing$, entonces, por definición de igualdad entre conjuntos tenemos que, $A \cup \varnothing = A$.

Veamos ahora que $A \cap \emptyset = \emptyset$. Por la Proposición 11.1.4 (1) tenemos que $A \cap \emptyset \subseteq \emptyset$. Por la Proposición 10.2.5 (3) sabemos que $\emptyset$ es subconjunto de cualquier conjunto, en particular tenemos que $\emptyset \subseteq A \cap \emptyset$. Como $A \cap \emptyset \subseteq \emptyset$ y $\emptyset \subseteq A \cap \emptyset$, por la definición de igualdad entre conjuntos tenemos que $A \cap \emptyset = \emptyset$.

9. Demostraremos que $A \cup A = A$. Por la Proposición 11.1.4 (2) tenemos que $A \subseteq A \cup A$. Veamos que $A \cup A \subseteq A$. Sea $x \in A \cup A$ cualquiera. Por definición de unión entre conjuntos tenemos que $x \in A$ o $x \in A$, en cualquier caso tenemos que $x \in A$. Como cualquier elemento de $A \cup A$ es elemento de A, por la definición de contenencia entre conjuntos tenemos que, $A \cup A \subseteq A$. Como $A \cup A \subseteq A$ y $A \subseteq A \cup A$, por definición de igualdad entre conjuntos tenemos que, $A \cup A = A$.

Dejamos como ejercicio los numerales 10 y 11.

☑

11.2. Diferencia entre conjuntos

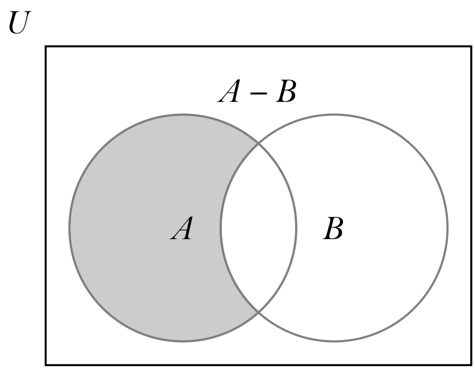
Dada la importancia de comparar conjuntos en diversos contextos matemáticos, la diferencia es una operación clave que nos ayuda a identificar los elementos exclusivos de un conjunto con respecto a otro. Si A y B son dos conjuntos, la diferencia $A - B$ está compuesta por todos los elementos que pertenecen a A pero no a B.

Definición 11.2.1 (Diferencia entre conjuntos)**.** Sea U conjunto de referencia y $A, B \subseteq U$ conjuntos. La *diferencia* entre A y B es el conjunto

$$A - B := \{x \in U : x \in A \text{ y } x \notin B\}.$$

Es decir, $A - B$ es el conjunto conformado por todos los elementos de U que pertenecen a A y no pertenecen a B. En otras palabras, para cualquier $x \in U$, $x \in A - B$ si y solo si $x \in A$ y $x \notin B$.

Notación 11.2.2. En otros textos la diferencia entre A y B se denota también como $A \setminus B$. En estas notas lo denotaremos por $A - B$.



Ejemplos 11.2.3.

1. Considere como conjunto de referencia $U := \mathbb{N}$.
   Si $A := \{1, 2, 3, 4\}$ y $B := \{3, 4, 5\}$, note que los elementos de A que están en B, son 3 y 4. Luego, los demás elementos de A, que son 1 y 2, corresponden a los elementos de la diferencia $A-B$, es decir, $A-B = \{1, 2\}$. La diferencia $B-A$ corresponde al conjunto formado por los elementos de B que no están en A, en este caso $B - A = \{5\}$.

2. Considere como conjunto de referencia U el conjunto de las letras del alfabeto español, $A := \{a, b, c, d, e, f\}$ y $B := \{f, g, h\}$. $A-B$ y $B-A$ en este caso corresponden a los conjuntos $A-B = \{a, b, c, d, e\}$ y $B - A = \{g, h\}$.

Proposición 11.2.4. *Sean U conjunto de referencia y $A, B, C \subseteq U$ conjuntos.*

1. $A - B \subseteq A$.
2. $(A - B) \cap B = \emptyset$.
3. $A - B = \emptyset$ *si y solo si* $A \subseteq B$.
4. $B - (B - A) = A$ *si y solo si* $A \subseteq B$.
5. *Si* $A \subseteq B$*, entonces* $A - C = A \cap (B - C)$.
6. *Si* $A \subseteq B$*, entonces* $C - B \subseteq C - A$.
7. *(Ley de De Morgan I)* $C - (A \cap B) = (C - A) \cup (C - B)$.

8. *(Ley de De Morgan II)* $C - (A \cup B) = (C - A) \cap (C - B)$.

Demostración. Sean U conjunto de referencia y $A, B, C \subseteq U$ conjuntos.

1. Sea $x \in A - B$ cualquiera. Por definición de diferencia entre conjuntos $x \in A$ y $x \notin B$. En particular, tenemos que $x \in A$. Como todo elemento de $A - B$ es elemento de A, entonces por la definición de contenencia entre conjuntos tenemos que $A - B \subseteq A$.

2. Supongamos por reducción al absurdo que $(A - B) \cap B \neq \varnothing$. Esto significa que existe $x \in (A-B) \cap B$. Por definición de intersección entre conjuntos, $x \in A-B$ y $x \in B$. Como $x \in A-B$, por definición de diferencia entre conjuntos tenemos que, $x \in A$ y $x \notin B$. En particular, $x \notin B$. Pero, $x \in B$ (contradicción). Por lo tanto, $(A - B) \cap B = \varnothing$.

3. $(\rightarrow)$ Supongamos que $A - B = \varnothing$. Razonando por reducción al absurdo, supongamos que $A \nsubseteq B$. Por negación de la definición de contenencia entre conjuntos tenemos que existe $x \in A$ tal que $x \notin B$. Por definición de diferencia entre conjuntos se tiene que $x \in A - B$, es decir, $A - B \neq \varnothing$ (contradicción). Luego $A \subseteq B$.
   $(\leftarrow)$ Supongamos que $A \subseteq B$ es verdad. Razonando por reducción al absurdo suponemos que $A - B \neq \varnothing$. Esto significa que existe $x \in A-B$. Por definición de diferencia entre conjuntos se tiene que tal $x \in A$ y $x \notin B$, pero por negación de contenencia entre conjuntos, $A \nsubseteq B$ (contradicción). Luego $A - B = \varnothing$.

   Dejamos los numerales 4 y 5 como ejercicio para el lector.

6. Supongamos que $A \subseteq B$. Sea $x \in C - B$ cualquiera. Por definición de diferencia entre conjuntos tenemos que $x \in C$ y $x \notin B$. Como por hipótesis $A \subseteq B$ y $x \notin B$, entonces $x \notin A$ (por reducción al absurdo, si $x \in A$, entonces, como $A \subseteq B$, tendríamos que $x \in B$, contradicción). Por lo tanto, $x \in C$ y $x \notin A$, es decir, $x \in C - A$, por definición de diferencia de conjuntos. Así, todo elemento de $C - B$ es elemento de $C - A$. Por definición de

contenencia entre conjuntos concluímos que $C - B \subseteq C - A$.

Dejamos también los numerales 7 y 8 como ejercicio para el lector. ☑

Observación 11.2.5. Es importante resaltar que el recíproco de la Proposición 11.2.4 (6.) no es cierto. Si tomamos como conjunto de referencia $U := \mathbb{N}$, $A := \{4, 5, 7\}$, $B := \{4, 5, 6\}$ y $C := \{1, 2, 3, 4, 5\}$, observemos que $C - A = \{1, 2, 3\} = C - B$ pero $A \nsubseteq B$ ($7 \in A$ pero $7 \notin B$) y $B \nsubseteq A$ ($6 \in B$ pero $6 \notin A$).

11.3. Complemento de un conjunto

A continuación, presentamos el *complemento* de un conjunto en términos de la diferencia entre conjuntos.

Definición 11.3.1. Dado un conjunto A con elementos en un conjunto de referencia U, definimos el *complemento* de A (con respecto a U), denotado por A', como el conjunto

$$A' := \{x \in U : x \notin A\} = U - A.$$

Más precisamente, A' es el conjunto de todos los elementos del conjunto de referencia U que no son elementos de A. En otras palabras, para cualquier $x \in U$, $x \in A'$ si y solo si $x \notin A$.

A continuación, presentamos algunas propiedades del *complemento* de un conjunto que son consecuencia directa de los resultados en la Proposición 11.2.4.

Proposición 11.3.2. *Sean U conjunto de referencia y $A, B \subseteq U$ conjuntos.*

1. *$A' \subseteq U$.*

2. *$A \cap A' = \varnothing$.*

3. *$A' = \varnothing$ si y solo si $A = U$.*

4. $(A')' = A$.

5. $A - B = A \cap B'$.

6. *Si* $A \subseteq B$, *entonces* $B' \subseteq A'$.

7. *(Ley de De Morgan I)* $(A \cap B)' = A' \cup B'$.

8. *(Ley de De Morgan II)* $(A \cup B)' = A' \cap B'$.

Presentamos a continuación demostraciones alternativas de estas afirmaciones sin usar la Proposición 11.2.4.

Demostración. Sean U conjunto de referencia y $A, B \subseteq U$ conjuntos.

1. Es inmediato de la definición de A'.

2. Sabemos que $\varnothing$ está contenido en cualquier conjunto, en particular $\varnothing \subseteq A \cap A'$. Por otro lado, si $A \cap A' \nsubseteq \varnothing$, existiría $x \in A \cap A'$ tal que $x \notin \varnothing$. Por definición de intersección de conjuntos, como $x \in A \cap A'$, tenemos que $x \in A$ y $x \in A'$. Por definición de complemento de un conjunto, esto nos dice que $x \in A$ y $x \notin A$ (contradicción). Por lo tanto, $A \cap A' \subseteq \varnothing$. Puesto que $\varnothing \subseteq A \cap A'$ y $A \cap A' \subseteq \varnothing$, por definición de igualdad entre conjuntos tenemos que, $A \cap A' = \varnothing$.

   Dejamos como ejercicio para el lector los numerales 3 y 4.

5. Sea $x \in U$ cualquiera. Por definición de diferencia entre conjuntos, $x \in A - B$ es equivalente a que $x \in A$ y $x \notin B$. Por definición de complemento de un conjunto, $x \notin B$ significa que $x \in B'$. Por lo tanto, $x \in A - B$ si y solo si $x \in A$ y $x \in B'$. Finalmente, por la definición de intersección de conjuntos, $x \in A - B$ si y solo si $x \in A \cap B'$. Así, por definición de igualdad entre conjuntos, hemos probado que $A - B = A \cap B'$.

   Dejamos como ejercicio para el lector el numeral 6.

7. Sea $x \in U$ cualquiera. Por definición de intersección entre conjuntos, sabemos que $x \notin A \cap B$ es equivalente a que $x \notin A$ o $x \notin B$ (¿por qué?). Por las definiciones de complemento de un conjunto y unión entre conjuntos tenemos que, $x \in (A \cap B)'$

si y solo si $x \in A' \cup B'$. Así, por definición de igualdad entre conjuntos, hemos probado que $(A \cap B)' = A' \cup B'$.

Dejamos como ejercicio para el lector el numeral 8.

☑

11.4. Ejercicios

Ejercicio 11.4.1. Demuestre los numerales 3., 4., 5., 6., 7., 10 y 11. de la Proposición 11.1.4.

Ejercicio 11.4.2. Demuestre los numerales 4., 5., 7. y 8. de la Proposición 11.2.4.

Ejercicio 11.4.3. Demuestre los numerales 1., 3., 4., 6. y 8. de la Proposición 11.3.2.

Ejercicio 11.4.4. Sean A, B y C conjuntos. Demuestre que

$$(A - B) \cap C = (A \cap C) - B = (A \cap C) - (B \cap C).$$

Ejercicio 11.4.5. Sea X un conjunto arbitrario, y sean $A, B, C \subseteq X$. Suponga que $A \cap B = A \cap C$, y que $(X - A) \cap B = (X - A) \cap C$. Demuestre que $B = C$.

Ejercicio 11.4.6. Sean U conjunto de referencia y A, B, $C \subseteq U$ conjuntos. Suponga que $A \cap B = A \cap C$, y que $A' \cap B = A' \cap C$. Demuestre que $B = C$.

Ejercicio 11.4.7. Sean A, B y C conjuntos. La *diferencia simétrica* de A y B, denotada por $A \triangle B$, es el conjunto $A \triangle B = (A - B) \cup (B - A)$. Demuestre las siguientes afirmaciones:

1. $A \triangle \varnothing = A$.
2. $A \triangle A = \varnothing$.
3. $A \triangle B = B \triangle A$.
4. $(A \triangle B) \triangle C = A \triangle (B \triangle C)$.

5. $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.
6. $A \triangle B = (A \cup B) - (A \cap B)$.

Ejercicio 11.4.8. Considere los conjuntos A, B y C subconjuntos arbitrarios de un conjunto de referencia U y determine si las siguientes proposiciones son verdaderas o falsas. Demuestre o exhiba un contraejemplo según el caso.

1. Si $A \cup B = C \cup B$, entonces $A = C$.
2. $A \cap (B - C) = (A \cap B) - (A \cap C)$.
3. $(A - B) \cup B = A$.
4. Si $A \cap B = \varnothing$, entonces $A = \varnothing$ o $B = \varnothing$.
5. Existen conjuntos A y B tales que $(A - B)^c = (B - A)^c$.
6. $A \cup B = \varnothing$ implica que $A = \varnothing$ o $B = \varnothing$.
7. $A - B = \varnothing$ si y solo si $A = B$.
8. $A \subseteq B$ si y solo si $A' \cup B = U$.
9. Para todo par de conjuntos A y B se cumple que $(A - B) \cup (B - A) = A$.
10. $A \subseteq B$ si y solo si $A \cap B' = \varnothing$.
11. Si $A \cup B = U$, entonces $B = A'$.
12. $B' \subseteq A'$ implica que $B \subseteq A$.
13. Existen conjuntos A, B y C tales que $A - (B - C) = (A - B) - C$.
14. Si A, B y C son conjuntos entonces se cumple que
$$A - (B - C) = (A - B) - C.$$
15. Si $A \cup B = A$, entonces $B = \varnothing$.

16. $A - (B \cup C) = (A - B) \cup (A - C)$.

17. Existen conjuntos A y B tales que $A \triangle B = A \cup B$.

18. Hay conjuntos A y B para los cuales $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$.

19. Dados dos conjuntos A y B existe un conjunto C para el cual $A \cup C = B$.

20. $A \triangle B \triangle C = (A \cup B \cup C) - (A \cap B \cap C)$.

Ejercicio 11.4.9. En cada uno de los siguientes casos encuentre, si es posible, condiciones *necesarias* (pero no suficientes), *suficientes* (pero no necesarias), y *necesarias y suficientes* para que se cumpla la igualdad.

1. $A \cap B = A$. 2. $A \cup B = A$.

3. $A' \cap U = \varnothing$. 4. $(A \cap B)' = B'$.

Ejercicio 11.4.10. Consideremos $U := \{x \in \mathbb{N} : 0 \leq x \leq 10\}$, $A := \{x \in U : x \text{ es primo}\}$ y $B = \{x \in U : x \text{ es impar}\}$. Describa por extensión y por comprensión los conjuntos:

$$A', \qquad B - A, \qquad (A \cap B)', \qquad A - (B \cup A'), \qquad A \triangle B.$$

Ejercicio 11.4.11. Si $A = \{1, 2, \{1, 2\}\}$ $B = \{1, \{2\}, 3\}$ y $C = \{2\}$.

a) Determine por extensión:

1. $\mathcal{P}(A)$.
2. $\mathcal{P}(B)$.
3. $\mathcal{P}(A \cap B)$.
4. $\mathcal{P}(A) \cap \mathcal{P}(B)$.
5. $\mathcal{P}(A \cup B)$.

6. $\mathscr{P}(A) \cup \mathscr{P}(B)$.
7. $\mathscr{P}(A - C)$.
8. $\mathscr{P}(A) - \mathscr{P}(C)$.

b) Llene el espacio vacío con los símbolos $\in$ o $\notin$, $\subseteq$ o $\not\subseteq$, de manera que se obtenga una proposición verdadera. Justifique su respuesta.

1. $\{1, 2\} \underline{\hspace{2em}} A$.
2. $\{1, 2\} \underline{\hspace{2em}} B$.
3. $\{\{\{\}\}\} \underline{\hspace{2em}} \mathscr{P}(\mathscr{P}(\mathscr{P}(A)))$.
4. $\{\{2\}\} \underline{\hspace{2em}} \mathscr{P}(A)$.
5. $\{\{2\}\} \underline{\hspace{2em}} \mathscr{P}(B)$.

Lección

doce

Familias indexadas de conjuntos

Es muy usual en matemáticas enfrentarnos a problemas en los que se involucran muchos conjuntos, y pueden ser tantos que las letras del alfabeto no son suficientes para nombrarlos. Por lo tanto, en lugar de denotar todos esos conjuntos por A, B, C, etc., será conveniente usar subíndices en su notación, de tal manera que los denotaremos por A_1, A_2, A_3, etc. Conjuntos como estos son llamados conjuntos con subíndices en su notación o, más simplemente, *cojuntos indexados*. Un conjunto para el que todos sus elementos son conjuntos es llamado *colección* o *familia* de conjuntos.

Las operaciones elementales básicas (unión e intersección) que hemos definido entre conjuntos solo tienen sentido cuando se realizan entre dos conjuntos pero, de manera natural, debido a la asociatividad y conmutatividad de dichas operaciones (ver Proposición 11.1.4 en sus numerales 3 y 4), se pueden extender a una colección finita de conjuntos.

Por ejemplo, dados tres conjuntos A_1, A_2, A_3, podemos definir la intersección de dichos conjuntos $A_1 \cap A_2 \cap A_3$ como $(A_1 \cap A_2) \cap A_3$; es decir, por la definición dada anteriormente, $x \in A_1 \cap A_2 \cap A_3$ si y solo si $x \in A_1 \cap A_2$ y $x \in A_3$, que es lo mismo que decir que $x \in A_1$ y $x \in A_2$ y $x \in A_3$; en otras palabras, x pertenece simultáneamente a todos los conjuntos que estamos intersectando. Esto también lo podemos escribir de la siguiente manera: $x \in A_1 \cap A_2 \cap A_3$ si y solo si $x \in A_j$ para todo $j \in \{1, 2, 3\}$. Esta misma idea la podemos extender si intersectamos una familia finita de conjuntos $A_1, A_2, \cdots, A_n$.

De manera análoga, podemos definir la unión $A_1 \cup A_2 \cup A_3 := (A_1 \cup A_2) \cup A_3$, donde $x \in A_1 \cup A_2 \cup A_3$ si y solo si $x \in (A_1 \cup A_2)$ o $x \in A_3$, luego $x \in A_1$ o $x \in A_2$ o $x \in A_3$; en otras palabras, x pertenece a la unión de dichos conjuntos si y solo si x está en alguno de ellos. Esto también lo podemos escribir de la siguiente manera: $x \in A_1 \cup A_2 \cup A_3$ si y solo si $x \in A_j$ para algún $j \in \{1, 2, 3\}$. Así mismo, tal idea la podemos extender si unimos una familia finita de conjuntos $A_1, A_2, \cdots, A_n$.

En esta lección extendemos estas ideas a una familia arbitraria (no necesariamente finita) de conjuntos.

12.1. Familias indexadas de conjuntos

Una *familia indexada de conjuntos* es una colección de conjuntos que está organizada o etiquetada mediante un conjunto de índices. Las familias indexadas son útiles para agrupar conjuntos en una colección donde el conjunto de índices ayuda a organizar o identificar a cada conjunto.

Definición 12.1.1. Sean $I \neq \emptyset$ un conjunto, U un conjunto de referencia y $\mathcal{F}$ una familia de conjuntos contenidos en U. Diremos que $\mathcal{F}$ es una *familia de conjuntos indexada por I* si y solo si para cada $i \in I$ existe un único elemento de $\mathcal{F}$ tal que i aparece como subíndice en la notación del elemento de $\mathcal{F}$. De este modo $\mathcal{F} = \{A_i : i \in I\} = \{A_i\}_{i \in I}$. La colección $\mathcal{F}$ es denominada *familia indexada de conjuntos*. El conjunto I se denomina *conjunto de índices*.

Ejemplos 12.1.2.

1. Considere $I := \{5, 6, 7, 8\}$. Para cada $k \in I$ se define el conjunto $A_k = \{2^j : 2 \leq j \leq k\}$. Así,

$$\begin{aligned} A_5 &= \{4, 8, 16, 32\}, \\ A_6 &= \{4, 8, 16, 32, 64\}, \\ A_7 &= \{4, 8, 16, 32, 64, 128\}, \\ A_8 &= \{4, 8, 16, 32, 64, 128, 256\}. \end{aligned}$$

   En este caso la familia indexada de conjuntos es $\mathcal{F} := \{A_5, A_6, A_7, A_8\}$.

2. Considere $I := \mathbb{N}$. Para cada $n \in \mathbb{N}$ defina el conjunto $B_n := \{k \in \mathbb{N} : 0 \leq k \leq 3n\}$ (nótese que en este conjunto, la definición de cada conjunto B_n depende del índice n). De este modo, $B_0 = \{0\}, B_1 = \{0, 1, 2, 3\}, B_2 := \{0, 1, 2, 3, 4, 5, 6\}$ y así sucesivamente. Luego, la familia indexada de conjuntos es $\mathcal{F} := \{B_0, B_1, B_2, \cdots\} = \{B_n\}_{n \in \mathbb{N}}$.

3. Considere $I := \mathbb{N}^* := \mathbb{N} - \{0\}$. Para cada $k \in \mathbb{N}^*$ defina $B_k := \left(\frac{1}{k}, 8 + \frac{3}{k}\right)$ (el intervalo real $\left\{x \in \mathbb{R} : \frac{1}{k} < x < 8 + \frac{3}{k}\right\}$). Siguien-

do esta definición, encontramos que, por ejemplo:

$$
\begin{aligned}
B_1 &= \left(\frac{1}{1}, 8+\frac{3}{1}\right) = (1, 11),\\
B_2 &= \left(\frac{1}{2}, 8+\frac{3}{2}\right) = \left(\frac{1}{2}, \frac{19}{2}\right),\\
B_3 &= \left(\frac{1}{3}, 8+\frac{3}{3}\right) = \left(\frac{1}{3}, 9\right),
\end{aligned}
$$

y así sucesivamente. La familia indexada de conjuntos es en este caso $\mathscr{F} := \{B_k\}_{k\in\mathbb{N}^*}$.

12.2. Intersección de una familia indexada de conjuntos

En la Definición 11.1.2 de la Lección 11 vimos que dados conjuntos A y B, subconjuntos de un conjunto de referencia U, un elemento x está en la intersección entre A y B cuando x es simultáneamente elemento de A y de B. En otras palabras, si consideramos la familia de conjuntos $\mathcal{S} := \{A, B\}$, que dicho elemento x esté tanto en A como en B es lo mismo que decir que x es elemento de *todos* los elementos de la familia $\mathcal{S}$. Dada una familia indexada de conjuntos $\mathscr{A} = \{A_i : i \in I\}$, basada en las ideas expuestas, definiremos a continuación la intersección de todos los conjuntos que están en esta familia.

Definición 12.2.1 (Intersección de una familia indexada de conjuntos). Sea $\mathscr{A} := \{A_i : i \in I\}$ una familia indexada de conjuntos, en la que para cada $i \in I$ tenemos que A_i es un subconjunto de un conjunto de referencia U. La *intersección* de dicha familia es el conjunto

$$\bigcap_{i\in I} A_i := \{x \in U : x \in A_i \text{ para todo } i \in I\}.$$

En otras palabras, $x \in \bigcap_{i\in I} A_i$ si y solo si $x \in A_i$ para todo $i \in I$.

Otra manera de denotar dicha intersección es $\bigcap \mathscr{A}$.

Ejemplos 12.2.2.

1. En el Ejemplo 12.1.2 (1) vemos que $\bigcap_{i\in I} A_i = A_5 \cap A_6 \cap A_7 \cap A_8 = \{4, 8, 16, 32\}$.

2. En el Ejemplo 12.1.2 (2), no es difícil ver que $\bigcap_{n\in\mathbb{N}} B_n = \{0\}$. Para verificar que se tiene esta igualdad, debemos ver que $\bigcap_{n\in\mathbb{N}} B_n \subseteq \{0\}$ y que $\{0\} \subseteq \bigcap_{n\in\mathbb{N}} B_n$ (ejercicio para el lector).

3. En el Ejemplo 12.1.2 (3), no es difícil ver que $\bigcap_{k\in\mathbb{N}^*} B_k = (1, 8]$ (ejercicio para el lector).

Observación 12.2.3. Dada una familia indexada de conjuntos $\mathcal{A} := \{A_i : i \in I\}$ en la que todo A_i es subconjunto de un conjunto de referencia U para todo $i \in I$ tenemos que, $x \notin \bigcap_{i\in I} A_i$ si y solo si *existe* $j \in I$ tal que $x \notin A_j$ (nótese que $x \notin \bigcap_{i\in I} A_i$ corresponde a negar una afirmación *universal*).

12.3. Unión de una familia indexada de conjuntos

En la Definición 11.1.1 de la Lección 11 vimos que para cualesquiera dos conjuntos A, B, subconjuntos de un conjunto de referencia U, un elemento x está en la unión entre A y B cuando x es elemento de A o es elemento de B. En otras palabras, si consideramos la familia de conjuntos $\mathcal{S} := \{A, B\}$, que dicho elemento x esté en A o en B es lo mismo que decir que x es elemento de *algún* elemento de la familia $\mathcal{S}$. Dada una familia indexada de conjuntos $\mathcal{A} := \{A_i : i \in I\}$ arbitraria y basados en las ideas presentadas, vamos a definir a continuación la unión de todos los conjuntos de esta familia de conjuntos.

Definición 12.3.1 (unión de una familia indexada de conjuntos). Dada una familia indexada de conjuntos $\{A_i : i \in I\}$, en la que para cada $i \in I$ tenemos que A_i es un subconjunto de un conjunto de referencia U, definimos la *unión* de esta familia como el conjunto

$$\bigcup_{i\in I} A_i := \{x \in U : x \in A_j \text{ para algún } j \in I\}.$$

En otras palabras, $x \in \bigcup_{i \in I} A_i$ si y solo si $x \in A_j$ para algún $j \in I$.

Otra manera de denotar dicha unión es $\bigcup \mathscr{A}$.

Ejemplos 12.3.2.

1. En el ejemplo 12.1.2 (1) vemos que $\bigcup_{i \in I} A_i = A_5 \cup A_6 \cup A_7 \cup A_8 = \{4, 8, 16, 32, 64, 128, 256\}$.

2. En el ejemplo 12.1.2 (2), no es difícil ver que $\bigcup_{n \in \mathbb{N}} B_n = \mathbb{N}$ (ejercicio para el lector).

3. En el ejemplo 12.1.2 (3), no es difícil ver que $\bigcup_{k \in \mathbb{N}^*} B_k = (0, 11)$. (ejercicio para el lector).

Observación 12.3.3. Dada una familia indexada de conjuntos $\mathscr{A} := \{A_i : i \in I\}$ en la que cada A_i es subconjunto de un conjunto de referencia U para todo $i \in I$ tenemos que, $x \notin \bigcup_{i \in I} A_i$ si y solo si *para todo* $j \in I$ se tiene que $x \notin A_j$ (nótese que $x \notin \bigcup_{i \in I} A_i$ corresponde a negar una afirmación *existencial*).

12.4. Algunas propiedades

A continuación, mostraremos algunas propiedades relacionadas con intersecciones y uniones de familias indexadas de conjuntos, análogas a las propiedades vistas en la proposición 11.1.4.

Proposición 12.4.1. *Sean $\mathscr{A} := \{A_i : i \in I\}$ una familia indexada de subconjuntos de un conjunto de referencia U y $B \subseteq U$.*

1. *Para todo $k \in I$ se tiene que $\bigcap_{i \in I} A_i \subseteq A_k$.*

2. *Si $B \subseteq A_k$ para todo $k \in I$, entonces $B \subseteq \bigcap_{i \in I} A_i$.*

3. *Para todo $k \in I$ se tiene que $A_k \subseteq \bigcup_{i \in I} A_i$.*

4. *Si $A_k \subseteq B$ para todo $k \in I$, entonces $\bigcup_{i \in I} A_i \subseteq B$.*

5. *$B \cap (\bigcup_{i \in I} A_i) = \bigcup_{i \in I} (B \cap A_i)$ (distributividad de $\cap$ con respecto a $\cup$).*

6. $B \cup (\bigcap_{i\in I} A_i) = \bigcap_{i\in I} (B \cup A_i)$ *(distributividad de $\cup$ con respecto a $\cap$).*

7. $B - (\bigcup_{i\in I} A_i) = \bigcap_{i\in I} (B - A_i)$ *(leyes de De Morgan (I)).*

8. $B - (\bigcap_{i\in I} A_i) = \bigcup_{i\in I} (B - A_i)$ *(leyes de De Morgan (II)).*

Demostración. Probaremos $1, 4$ y 7. Las otras proposiciones quedarán como ejercicio para el lector.

1. Sean $k \in I$ y $y \in \bigcap_{i\in I} A_i$ cualesquiera. Como $y \in \bigcap_{i\in I} A_i$, entonces por definición de interesección de una familia indexada de conjuntos tenemos que $y \in A_i$ para todo $i \in I$. En particular, $y \in A_k$. Por lo tanto, cualquier elemento de $\bigcap_{i\in I} A_i$ es también elemento de A_k para cualquier $k \in I$, y por definición de contenencia entre conjuntos tenemos que $\bigcap_{i\in I} A_i \subseteq A_k$.

4. Supongamos que $A_k \subseteq B$ para todo $k \in I$. Sea $y \in \bigcup_{i\in I} A_i$ cualquiera, lo que por definición de unión de una familia indexada de conjuntos nos dice que $y \in A_i$ para algún $i \in I$. Como por hipótesis $A_k \subseteq B$ para todo $k \in I$, en particular $A_i \subseteq B$. Así, $y \in A_i \subseteq B$ y por definición de contenencia entre conjuntos tenemos que $y \in B$. Por lo tanto, $\bigcup_{i\in I} A_i \subseteq B$.

7. En este caso debemos probar una igualdad entre conjuntos. Basados en la definición de la igualdad de conjuntos, probaremos la doble contenencia entre estos conjuntos.
   Sea $y \in B - (\bigcup_{i\in I} A_i)$ arbitrario. Esto significa que $y \in B$ y $y \notin \bigcup_{i\in I} A_i$ (definición de diferencia entre conjuntos). Como $y \notin \bigcup_{i\in I} A_i$, entonces, por la observación $12.3.3$, $y \notin A_i$ para todo $i \in I$. Así que $y \in B$ y $y \notin A_i$ para todo $i \in I$. Es decir, $y \in B - A_i$ para todo $i \in I$. Por lo tanto, por definición de intersección de una familia indexada de conjuntos tenemos que $y \in \bigcap_{i\in I} (B - A_i)$. Hemos probado que $B - (\bigcup_{i\in I} A_i) \subseteq \bigcap_{i\in I} (B - A_i)$.
   Ahora sea $z \in \bigcap_{i\in I} (B - A_i)$ cualquiera. Esto significa que $z \in B - A_i$ para todo $i \in I$. Sea $k \in I$ arbitrario pero fijo, luego $z \in B - A_k$ y, por definición de diferencia entre conjuntos,

$z \in B$ y $z \notin A_k$; por consiguiente, en particular, $z \notin A_k$. Como $k \in I$ es arbitrario, $z \notin A_i$ para todo $i \in I$. Por lo tanto, de la observación 12.3.3 podemos decir que, $z \notin \bigcup_{i\in I} A_i$. Así, $z \in B$ y $z \notin \bigcup_{i\in I} A_i$, luego de la definición de diferencia entre conjuntos tenemos que $z \in B - (\bigcup_{i\in I} A_i)$, es decir $B - (\bigcup_{i\in I} A_i) \subseteq \bigcap_{i\in I} (B - A_i)$.

Puesto que

$$B - \left(\bigcup_{i\in I} A_i\right) \subseteq \bigcap_{i\in I} (B - A_i) \text{ y } B - \left(\bigcup_{i\in I} A_i\right) \subseteq \bigcap_{i\in I} (B - A_i),$$

por la definición de igualdad entre conjuntos tenemos que $B - (\bigcup_{i\in I} A_i) = \bigcap_{i\in I} (B - A_i)$.

☑

Ejemplo 12.4.2. Veamos que $\bigcup\limits_{k\in\mathbb{Z}^+} \left(\frac{3k-1}{k}, \frac{6k+2}{k}\right] = (2, 8]$. Llamemos $A_k = \left(\frac{3k-1}{k}, \frac{6k+2}{k}\right]$ para todo $k \in \mathbb{Z}^+$. Vemos que $A_1 = (2, 8]$ y aplicando la Proposición 12.4.1 (3.) se tiene que $A_1 = (2, 8] \subseteq \bigcup\limits_{k\in\mathbb{Z}^+} A_k$. Nótese que para todo $k \in \mathbb{Z}^+$ se tiene que $k = 3k - 2k \geq 1$, esto es, $2k \leq 3k - 1$. Es decir, $2 \leq \frac{3k-1}{k}$ para todo $k \in \mathbb{Z}^+$. También, para todo $k \in \mathbb{Z}^+$ se tiene que $2 \leq 2k = 8k - 6k$, esto es, $6k + 2 \leq 8k$. Es decir, $\frac{6k+2}{k} \leq 8$ para todo $k \in \mathbb{Z}^+$. En resumen, $A_k = \left(\frac{3k-1}{k}, \frac{6k+2}{k}\right] \subseteq (2, 8]$ para todo $k \in \mathbb{Z}^+$. Aplicando la Proposición 12.4.1 (4.) se tiene que $\bigcup\limits_{k\in\mathbb{Z}^+} A_k \subseteq (2, 8]$. Esto prueba lo que se quería mostrar.

Ejemplo 12.4.3. Veamos ahora que $\bigcap\limits_{k\in\mathbb{Z}^+} \left(\frac{3k-1}{k}, \frac{6k+2}{k}\right] = [3, 6]$. Es simple ver que $\frac{3k-1}{k} = 3 - \frac{1}{k} < 3$ y $\frac{6k+2}{k} = 6 + \frac{2}{k} > 6$ para cualquier $k \in \mathbb{Z}^+$. Por lo tanto, $[3, 6] \subseteq A_k$ para todo $k \in \mathbb{Z}^+$. Aplicando la Proposición 12.4.1 (2.) se tiene que $[3, 6] \subseteq \bigcap\limits_{k\in\mathbb{Z}^+} A_k$. Para mostrar la otra contenencia $\bigcap\limits_{k\in\mathbb{Z}^+} A_k \subseteq [3, 6]$, veremos que ningún real que está fuera del intervalo $[3, 6]$ puede estar en $\bigcap\limits_{k\in\mathbb{Z}^+} A_k$. Note que basta ver que cualquier real $x < 3$, muy cercano a 3, no está en $\bigcap\limits_{k\in\mathbb{Z}^+} A_k$ y que ningún real $x > 6$, muy cercano a 6, tampoco está en $\bigcap_{k\in\mathbb{Z}^+} A_k$. La clave para esta prueba es aplicar la *Propiedad arquimediana de los números reales*, vea el Teorema A.4.1 (4.) en el Apéndice A. Consideremos $\epsilon = 3-x$ positivo y muy, muy pequeño. Por la *Propiedad arquimediana*, sabemos que existe $n \in \mathbb{Z}^+$ tal que $n\epsilon > 1$, es decir, $3 - x > \frac{1}{n}$. Esto prueba que $x \notin \left(\frac{3n-1}{n}, \frac{6n+2}{n}\right] = A_n$ para algún $n \in \mathbb{Z}^+$ porque existe $n \in \mathbb{Z}^+$ tal que $x < \frac{3n-1}{n}$, es decir, $x \notin \bigcap_{k\in\mathbb{Z}^+} A_k$. La prueba de que cualquier $x > 6$ tampoco está en $\bigcap_{k\in\mathbb{Z}^+} A_k$ es dejada como ejercicio para el lector.

12.5. Ejercicios

Ejercicio 12.5.1. Pruebe la Proposición 12.4.1 numerales 2, 3, 5, 6, 8.

Ejercicio 12.5.2. Sean $A_1 = \{1, 3, 5, 7, 9\}$, $A_2 = \{1, 2, 3, 4, 5, 6\}$, $A_3 = \{4, 5, 6, 7, 8, 9\}$ y $A_4 = \{0, 5, 10\}$ conjuntos. Halle

$$\bigcap_{k=1}^{4} A_k \qquad \text{y} \qquad \bigcup_{k=1}^{4} A_k$$

Ejercicio 12.5.3. Pruebe que ningún $x > 6$ está en $\bigcap_{k\in\mathbb{Z}^+}\left(\frac{3k-1}{k}, \frac{6k+2}{k}\right]$.

Ejercicio 12.5.4. Determine

1. $\bigcap_{k\in\mathbb{N}} [k, k+1]$ y $\bigcup_{k\in\mathbb{N}} [k, k+1]$.
2. $\bigcap_{k\in\mathbb{N}} [0, k+1)$ y $\bigcup_{k\in\mathbb{N}} [0, k+1)$.
3. $\bigcap_{k\in\mathbb{N}} [-k, k]$ y $\bigcup_{k\in\mathbb{N}} [-k, k]$.
4. $\bigcap_{k\in\mathbb{N}} \{-1, 0, 1, \cdots, 2k\}$ y $\bigcup_{k\in\mathbb{N}} \{-1, 0, 1, \cdots, 2k\}$.

5. $\bigcap_{k\in\mathbb{Z}^+} \{1, 2, 4, \cdots, 2^k\}$ y $\bigcup_{k\in\mathbb{Z}^+} \{1, 2, 4, \cdots, 2^k\}$.

6. $\bigcap_{k\in\mathbb{Z}^+} \left[\frac{-5k+4}{k}, \frac{7}{k}\right)$ y $\bigcup_{k\in\mathbb{Z}^+} \left[\frac{-5k+4}{k}, \frac{7}{k}\right)$.

Ejercicio 12.5.5. Sean I un conjunto no vacío, $\mathscr{A} = \{A_j\}_{j\in I}$ y $\mathscr{B} = \{B_j\}_{j\in I}$ familias de conjuntos indexados por I tales que $A_j \subseteq B_j$ para todo $j \in I$. Para las siguientes afirmaciones diga si son falsas o verdaderas. Justifique completamente su respuesta.

1. $\bigcup_{j\in I} A_j \subseteq \bigcup_{j\in I} B_j$.
2. $\bigcup_{j\in I} B_j \subseteq \bigcup_{j\in I} A_j$.
3. $\bigcap_{j\in I} B_j \subseteq \bigcap_{j\in I} A_j$.
4. $\bigcap_{j\in I} A_j \subseteq \bigcap_{j\in I} B_j$.

Ejercicio 12.5.6. Dada $\mathscr{A}$ una familia de conjuntos con elementos en un conjunto de referencia U, definimos la *unión* de $\mathscr{A}$ como

$$\bigcup \mathscr{A} := \{x \in U : \text{ existe } X \in \mathscr{A} \text{ tal que } x \in X\}$$

y la *intersección* de $\mathscr{A}$ como

$$\bigcap \mathscr{A} := \{x \in U : \text{ para todo } X \in \mathscr{A} \text{ se tiene que } x \in X\}.$$

Demuestre:

1. Para todo $X \in \mathscr{A}$ se tiene que $\bigcap \mathscr{A} \subseteq X$.
2. Si $B \subseteq X$ para todo $X \in \mathscr{A}$, entonces $B \subseteq \bigcap \mathscr{A}$.
3. Para todo $X \in \mathscr{A}$ se tiene que $X \subseteq \bigcup \mathscr{A}$.
4. Si $X \subseteq B$ para todo $X \in \mathscr{A}$, entonces $\bigcup \mathscr{A} \subseteq B$.
5. $B - (\bigcup \mathscr{A}) = \bigcap_{X\in\mathscr{A}} (B - X)$ (leyes de De Morgan (I)).
6. $B - (\bigcap \mathscr{A}) = \bigcup_{X\in\mathscr{A}} (B - X)$ (leyes de De Morgan (II)).

Lección

trece

Parejas ordenadas y producto cartesiano

13.1. Parejas ordenadas

Sean U un conjunto de referencia y a, b elementos de U. Muchas veces queremos distinguir el orden en que tomamos dichos elementos. Cuando pensamos en el conjunto $\{a, b\}$, no se tiene en cuenta el orden en que escribimos sus elementos, puesto que como conjuntos $\{a, b\}$ es igual al conjunto $\{b, a\}$ (¿por qué?). Al intentar definir el concepto de pareja ordenada (a, b), queremos hacerlo de manera que el orden importe si $a \neq b$; es decir, considerar la pareja ordenada (a, b) no es lo mismo que la pareja ordenada (b, a). Usando conjuntos, podemos definir formalmente el concepto de pareja ordenada como se sigue a continuación:

Definición 13.1.1. Dados dos elementos $a, b \in U$, donde U es el conjunto de referencia. Definimos la *pareja ordenada* (a, b) como el conjunto $\{\{a\}, \{a, b\}\}$.

El principal objetivo al definir una pareja ordenada (a, b) es distinguir este objeto de la pareja ordenada (b, a) en el caso de que $a \neq b$. De la manera como hemos definido la pareja ordenada (a, b), esto puede ser demostrado, como veremos a continuación.

Proposición 13.1.2. *Dados a, $b \in U$ tales que $a \neq b$, entonces* $(a, b) \neq (b, a)$.

Demostración. Como por hipótesis $a \neq b$, entonces $a \notin \{b\}$ (de lo contrario, como el único elemento de $\{b\}$ es b, entonces $a = b$. Absurdo). Por lo tanto, por definición de contenencia entre conjuntos tenemos que $\{a\} \nsubseteq \{b\}$ ($a \in \{a\}$ y $a \notin \{b\}$) y por definición de igualdad entre conjuntos tenemos que $\{a\} \neq \{b\}$. Veamos ahora que $\{a\} \neq \{a, b\}$. De lo contrario, si $\{a\} = \{a, b\}$, como $b \in \{a, b\}$, entonces $b \in \{a\}$, por lo tanto, $b = a$ (contradicción). Como $\{a\} \notin (b, a) = \{\{b\}, \{b, a\}\}$ (puesto que $\{a\} \neq \{b\}$ y $\{a\} \neq \{b, a\}$ –ejercicio para el lector–) y $\{a\} \in (a, b) := \{\{a\}, \{a, b\}\}$, por definición de contenencia entre conjuntos, tenemos que $(a, b) \nsubseteq (b, a)$ y, por definición de igualdad entre conjuntos, concluímos que $(a, b) \neq (b, a)$. ☑

A continuación, demostraremos una equivalencia de la igualdad de dos parejas ordenadas. Básicamente, mostraremos que dos parejas ordenadas son iguales si y solo si son iguales componente a componente.

Proposición 13.1.3. *Sea U un conjunto de referencia y $a, b, c, d \in U$. $(a, b) = (c, d)$ si y solo si $a = c$ y $b = d$.*

Demostración. Para demostrar la dirección directa de esta equivalencia, razonaremos por contrarrecíproca. Supongamos que $a \neq c$ o $b \neq d$. Sin pérdida de generalidad supongamos que $a \neq c$. En este caso, tenemos que $\{a\} \neq \{c\}$ (de lo contrario, si $\{a\} = \{c\}$, como $a \in \{a\} = \{c\}$ entonces $a \in \{c\}$, por consiguiente $a = c$; contradicción). Adicionalmente, $\{a\} \neq \{c, d\}$ (de lo contrario, si $\{c, d\} = \{a\}$, puesto que $c \in \{c, d\} = \{a\}$ entonces $c \in \{a\}$, por consiguiente $c = a$; contradicción). Por lo tanto, $\{a\} \notin (c, d) := \{\{c\}, \{c, d\}\}$. Como $\{a\} \in (a, b) := \{\{a\}, \{a, b\}\}$ y $\{a\} \notin (c, d)$, por definición de contenencia entre conjuntos tenemos que $(a, b) \nsubseteq (c, d)$ y por definición de igualdad entre conjuntos tenemos que $(a, b) \neq (c, d)$. Argumentamos de manera análoga en el caso de que $b \neq d$.

Recíprocamente, supongamos que $a = c$ y $b = d$. Como $a = c$, se tiene que $\{a\} = \{c\}$ (sea $x \in \{a\}$, luego por definición de conjunto unitario tenemos que $x = a$. Como $a = c$, entonces por la transitividad de la igualdad tenemos que $x = c$; por lo tanto, $x \in \{c\}$, y así por la definición de contenencia entre conjuntos tenemos que $\{a\} \subseteq \{c\}$. De manera análoga se demuestra que $\{c\} \subseteq \{a\}$. Luego por la definición de igualdad entre conjuntos tenemos que $\{a\} = \{c\}$). Veamos ahora que $a = c$ y $b = d$ implica $\{a, b\} = \{c, d\}$: sea $x \in \{a, b\}$, luego $x = a$ o $x = b$; si $x = a$, puesto que $a = c$, por transitividad de la igualdad tenemos que $x = c$. Por lo tanto, $x = c \in \{c, d\}$. En el caso de que $x = b$, puesto que $b = d$, entonces $x = d$. Por consiguiente $x = d \in \{c, d\}$. Luego, en cualquier caso tenemos que $x \in \{c, d\}$ y, por definición de contenencia entre conjuntos tenemos que $\{a, b\} \subseteq \{c, d\}$. De manera análoga demostramos que $\{c, d\} \subseteq \{a, b\}$. Por la definición de igualdad entre conjuntos, concluimos que $\{a, b\} = \{c, d\}$. Ahora, dado $X \in (a, b) := \{\{a\}, \{a, b\}\}$, entonces $X = \{a\}$ o $X = \{a, b\}$. Si $X = \{a\}$, como $\{a\} = \{c\}$, entonces $X = \{c\} \in (c, d) := \{\{c\}, \{c, d\}\}$. Si en cambio $X = \{a, b\}$, puesto que $\{a, b\} = \{c, d\}$, entonces $X =$

$\{c, d\} \in (c, d) := \{\{c\}, \{c, d\}\}$; así pues, por la definición de contenencia entre conjuntos tenemos que $(a, b) \subseteq (c, d)$. De manera análoga podemos demostrar que $(c, d) \subseteq (a, b)$. Por la definición de igualdad entre conjuntos tenemos que $(a, b) = (c, d)$. ☑

13.2. Producto cartesiano de conjuntos

Sean a, b elementos de un conjunto de referencia U. Notemos que en general el conjunto $(a, b) := \{\{a\}, \{a, b\}\}$ no necesariamente es elemento de U (por ejemplo, tomemos $U := \mathbb{N}$ donde vemos que $(0, 1) := \{\{0\}, \{0, 1\}\}$ no es un número natural). Hasta ahora hemos definido lo que es una pareja ordenada. Pero para hacer más coherente nuestro desarrollo, estos elementos deberíamos tomarlos de un objeto matemático que sea conjunto, para definir bien este conjunto por *comprensión*. Este objeto, que definiremos en las próximas líneas, se conoce como *producto cartesiano*.

Seguramente, desde primaria y secundaria (especialmente en cálculo infinitesimal y diferencial) los estudiantes han trabajado con lo que conocemos como *plano cartesiano*, que consiste en la representación gráfica del conjunto de parejas ordenadas (a, b) donde tanto a como b son números reales. En esta lección pretendemos trabajar con una generalización de este concepto, ya no trabajando solamente con el conjunto de los números reales sino con conjuntos arbitrarios.

Definición 13.2.1. Sean A y B subconjuntos de un conjunto de referencia U. Definimos el *producto cartesiano* de A y B como el conjunto

$$A \times B := \{(a, b) : a \in A \text{ y } b \in B\}.$$

De la manera como hemos definido el producto cartesiano de A y B, no podemos garantizar que el producto cartesiano $A \times B$ sea de hecho un conjunto. Sin embargo, recordemos que si A y B son conjuntos (no vacíos, por ahora) con $a \in A$ y $b \in B$, definimos la pareja ordenada (a, b) como el conjunto $\{\{a\}, \{a, b\}\}$. Como $\{a\}$ y $\{a, b\}$ son subconjuntos de $A \cup B$, entonces $\{a\}, \{a, b\} \in \mathcal{P}(A \cup B)$ (pertenecen al conjunto potencia de $A \cup B$) y de esta manera $(a, b) = \{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$, porque $\{\{a\}, \{a, b\}\} \subseteq A \cup B$. Luego, podemos separar del conjunto $\mathcal{P}(\mathcal{P}(A \cup B))$ solo aquellos elementos que sean de la forma $\{\{a\}, \{a, b\}\}$, con $a \in A$ y $b \in B$. Así, es fácil ver que

$$A \times B = \{X \in \mathcal{P}(\mathcal{P}(A \cup B)) : \text{ existen } a \in A, b \in B \text{ con } X = (a, b)\}.$$

De esta forma garantizamos la construcción del producto cartesiano $A \times B$ como conjunto, aunque para efectos prácticos utilizaremos la manera como lo hemos definido en 13.2.1.

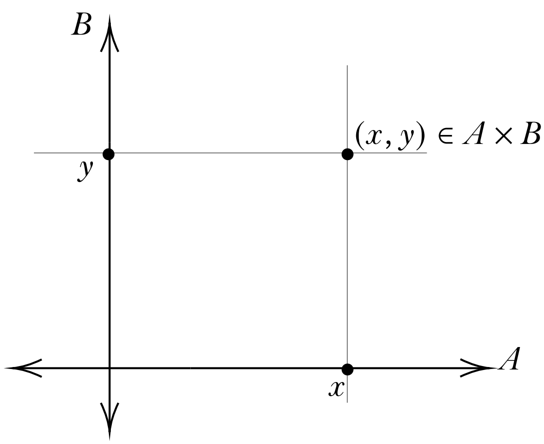
Ejemplos 13.2.2.

1. Si $A := \{1, 2\}$ y $B := \{a, b\}$, entonces
$$A \times B := \{(1, a), (1, b), (2, a), (2, b)\}$$
y
$$B \times A := \{(a, 1), (a, 2), (b, 1), (b, 2)\}.$$
2. Considerando $\mathbb{R}$ el conjunto de los números reales, $\mathbb{R} \times \mathbb{R}$ es el conjunto de las parejas ordenadas (x, y) donde $x, y \in \mathbb{R}$. Este conjunto es denotado también como $\mathbb{R}^2$, y se conoce como el *plano cartesiano*.

13.3. Representación de productos cartesianos

Sean A y B conjuntos con elementos en un conjunto de referencia U. Según la RAE, *representar* significa "hacer presente algo con palabras o figuras que la imaginación retiene". Esto no implica que la palabra o figura usada en la representación sea ese algo que deseamos representar; así como, por ejemplo, tampoco el actor en una obra de teatro es el personaje al que interpreta o representa. El propósito de esta sección es hacer una gráfica que nos permita representar el producto cartesiano $A \times B$, y para esto usaremos algunas nociones geométricas en las que no entraremos en detalle.

Inicialmente, representamos los elementos del conjunto A como puntos de una recta o de un segmento de recta, según la necesidad, y del mismo modo los elementos del conjunto B como puntos de otra recta u otro segmento de recta. Luego, ubicamos estas rectas o segmentos de tal modo que sean perpendiculares –vale la pena aclarar que para esta representación no es necesario que las rectas o segmentos sean perpendiculares– dejando la recta o segmento en el que representamos los elementos de A de modo horizontal y la recta o segmento en el que se representan los elementos de B de manera vertical. Para representar un elemento (x, y) del producto cartesiano $A \times B$ trazamos una recta vertical que sea paralela al segmento o recta en el que representamos los elementos de B y que intersecte al segmento horizontal en el punto x que está en A. Así mismo, trazamos otra recta paralela al segmento o recta horizontal en el que representamos los elementos de A y que pase por el punto $y \in B$. Estas dos rectas, que son solamente de apoyo, se intersectan en único punto que representará a la pareja ordenada (x, y). Procediendo del mismo modo podemos representar cada uno de los elementos del producto cartesiano $A \times B$.

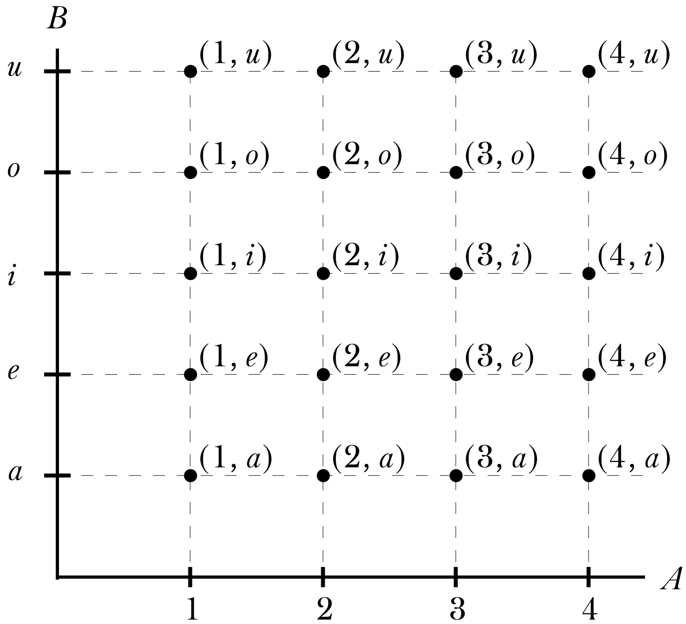


Para ver mejor esto, consideremos el siguiente ejemplo:

Ejemplo 13.3.1. Consideremos los conjuntos $A = \{1, 2, 3, 4\}$ y $B = \{a, e, i, o, u\}$. En este caso, necesitamos apenas segmentos de recta para representar los conjuntos A y B. Vemos que

$$\begin{aligned} A \times B = \{ & (1, a), (1, e), (1, i), (1, o), (1, u), (2, a), (2, e), \\ & (2, i), (2, o), (2, u), (3, a), (3, e), (3, i), (3, o), \\ & (3, u), (4, a), (4, e), (4, i), (4, o), (4, u) \}. \end{aligned}$$

La representación del conjunto $A \times B$ basada en la anterior descripción es la siguiente:



13.4. Propiedades

Proposición 13.4.1. *Sean U conjunto de referencia y $A, B, C, D \subseteq U$ conjuntos.*

1. *Si $A \subseteq B$ y $C \subseteq D$, entonces $A \times C \subseteq B \times D$.*
2. *$A \times (B \cup C) = (A \times B) \cup (A \times C)$ y $(B \cup C) \times A = (B \times A) \cup (C \times A)$.*

3. $A\times(B\cap C) = (A\times B)\cap(A\times C)$ y $(B\cap C)\times A = (B\times A)\cap(C\times A)$.

4. $A \times \varnothing = \varnothing$ y $\varnothing \times A = \varnothing$.

5. $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$.

Demostración.

1. Supongamos que $A \subseteq B$ y $C \subseteq D$. Sea $x \in A\times C$. Por definición de producto cartesiano, existen $a \in A$ y $c \in C$ tales que $x = (a, c)$. Puesto que $a \in A$ y como por hipótesis $A \subseteq B$, por la definición de contenencia entre conjuntos, tenemos que $a \in B$. Como $c \in C$ y, por hipótesis, $C \subseteq D$, por la definición de contenencia entre conjuntos, tenemos que $c \in D$. Como $a \in B$ y $c \in D$, por definición de producto cartesiano tenemos que $x = (a, c) \in B \times D$. Como vimos que todo elemento de $A \times C$ es elemento de $B \times D$, por definición de contenencia entre conjuntos tenemos que $A \times C \subseteq B \times D$.

2 y 3. Ejercicios.

4. Por reducción al absurdo, supongamos que $A \times \varnothing \neq \varnothing$. Por lo tanto, existiría $x \in A \times \varnothing$, luego por definición de producto cartesiano de conjuntos tenemos que existirían $a \in A$ y $b \in \varnothing$ tales que $x = (a, b)$ (contradice que $\varnothing$ no tiene elementos). Por consiguiente $A \times \varnothing = \varnothing$. De manera análoga podemos ver que $\varnothing \times A = \varnothing$ (ejercicio).

5. Ejercicio.

☑

13.5. Ejercicios

Ejercicio 13.5.1. Considere los conjuntos $A = \{a, e, i\}$ y $B = \{i, o, u\}$. Determine:

1. $(A \times B) \cap B$.
2. $(A \times A) \cup (B \times B)$.
3. $A \times (B \cap A)$.
4. $\mathscr{P}(A \times B)$.

Ejercicio 13.5.2. Determine

1. $\bigcap_{k\in\mathbb{N}} [k, k+1] \times \mathbb{R}$ y $\bigcup_{k\in\mathbb{N}} [k, k+1] \times \mathbb{R}$.
2. $\bigcap_{k\in\mathbb{N}} [0, k+1) \times \{k\}$ y $\bigcup_{k\in\mathbb{N}} [0, k+1) \times \{k\}$.
3. $\bigcap_{k\in\mathbb{N}} [-k, k] \times \{0\}$ y $\bigcup_{k\in\mathbb{N}} [-k, k] \times \{0\}$.
4. $\bigcap_{x\in[0,1]} [x, 1) \times [x^2, 1)$ y $\bigcup_{k\in\mathbb{N}} [x, 1) \times [x^2, 1)$.
5. $\bigcap_{x\in\mathbb{R}} \{x\} \times (2, 3]$ y $\bigcup_{x\in\mathbb{R}} \{x\} \times (2, 3]$.

Ejercicio 13.5.3. Sean A, B y C conjuntos arbitrarios. Diga de las siguientes afirmaciones si son verdaderas o falsas. Justifique su respuesta, es decir, demuestre o dé un contraejemplo según el caso.

1. $A \times (B - C) = (A \times B) - (A \times C)$.
2. Si $B \subseteq A$, entonces $(A \times A) - (B \times B) = [(A - B) \times A] \cup [A \times (A - B)]$.

Ejercicio 13.5.4. Demostrar los numerales 2, 3 y 5 de la Proposición 13.4.1.

Parte IV

Relaciones

Lección *catorce*

Nociones básicas

Según la Real Academia Española (RAE), la palabra *relación* significa “conexión, correspondencia de algo con otra cosa”. Mas coloquialmente, entendemos por relación algo como el vínculo que existe, por ejemplo, entre los miembros de una pareja sentimental, entre padres e hijos, entre empresas, entre naciones, etc. Un ejemplo de relación entre personas podría ser haber nacido en la misma ciudad. En matemáticas también se estudian relaciones entre objetos, pero, como frecuentemente ocurre, el significado de la palabra *relación* es muy técnico y no coincide totalmente con su uso coloquial, aunque se puede entender en un sentido más amplio como una conexión (posiblemente implícita) entre objetos matemáticos. Algunos ejemplos de relaciones entre objetos matemáticos, digamos los números enteros, que son muy comunes son las relaciones $=$ o $<$. Desde este punto de vista, una relación es una manera de *comparar* dos números, que de todas maneras es un tipo de conexión que podemos encontrar entre ellos.

Por ejemplo, podemos definir otra *relación* entre números enteros mediante la siguiente condición: dos números enteros a y b están relacionados si y solo si a divide a b. De esta manera, por ejemplo vemos que, mediante esta relación “divide a”, 2 no está relacionado con 3 (¿por qué?) y 4 sí lo está con 8. Esta es otra manera de *conectar* números enteros diferente a compararlos mediante la igualdad ($=$) o la relación de orden usual ($<$) en los enteros.

Por otro lado, consideremos la relación de una persona de ser progenitor (padre o madre) biológico de otra. Si tomamos dos personas aleatoriamente, digamos *Sutana* y *Perencejo*, entonces Sutana puede ser la madre biológica de Perencejo, o no. Podemos responder a la pregunta: ¿Sutana es madre biológica de Perencejo? porque sabemos el significado de la palabra “madre biológica”, y sabemos verificar si la condición de alguien ser madre biológica se satisface. En caso de que Sutana sea la madre biológica de Perencejo, sabemos que Perencejo no puede ser madre biológica de Sutana, así que es importante el orden en que tomemos los objetos (en este caso, personas) que vamos a relacionar. Como vimos anteriormente, los objetos matemáticos que nos permiten distinguir el orden en que tomamos dos objetos son los que denominamos *parejas ordenadas*.

De esta manera, podemos hacer un listado de todas las parejas *ordenadas* de personas (X, Y) para las cuales X es progenitor biológico de Y. De este modo, si una persona no sabe el significado de ser progenitor biológico y se ve en la tarea de decidir si una pareja de personas (X, Y) está conformada por su progenitor biológico e hijo, bastaría simplemente con revisar la lista y verificar si (X, Y) está en la lista, o no. En este ejemplo la relación que consideramos muestra una conexión entre dos personas, sin embargo, las relaciones no necesariamente ocurren entre objetos que estén en el mismo conjunto. En el ejemplo que estamos considerando, la pareja $(Sutana, Perencejo)$ estaría en la lista que tomamos anteriormente para definir la relación "ser progenitor biológico de". Más concretamente, tomando A como el conjunto de seres humanos, esta relación puede ser descrita por el siguiente conjunto:

$$\mathscr{P} := \{(X, Y) \in A \times A : \ X \text{ es progenitor biológico de } Y\},$$

en donde tenemos que $(Sutana, Perencejo) \in \mathscr{P}$.

Veamos un ejemplo de relación más general que nos permita introducir algunas nociones de este concepto. Consideremos por ejemplo la relación X leyó la obra Y. Esta relación no conecta objetos del mismo tipo, en efecto, conecta lectores con obras literarias. Es decir, X representa elementos del conjunto A de personas, mientras Y representa elementos del conjunto B de títulos de obras literarias. De este modo, esta relación nos permite formar parejas ordenadas tomando como primera componente una persona de A, que es un lector, y como segunda componente uno de los títulos de obras de B, que ha sido leída por él. En otras palabras, podemos separar de $A \times B$ aquellas parejas ordenadas cuya primera componente está relacionada mediante esta relación descrita con la segunda, es decir, consideremos el conjunto

$$\mathscr{R} = \{(X, Y) \in A \times B \mid X \text{ leyó } Y\}.$$

Consecuentemente, a toda *relación* dada entre los elementos de dos conjuntos se le hace corresponder un único conjunto de parejas ordenadas. Por este motivo podemos considerar que una *relación* es el conjunto de parejas ordenadas correspondiente. Además, nótese que del conjunto $\mathscr{R}$ se puede intuir el significado de la relación entre lector y obra.

14.1. Concepto de relación

Intuitivamente, una relación es un conjunto de parejas ordenadas que establece una conexión o correspondencia entre las componentes de tales parejas ordenadas.

Definición 14.1.1. Sean A y B conjuntos. Una *relación* $\mathscr{R}$ de A en B es un subconjunto de $A \times B$, es decir, $\mathscr{R} \subseteq A \times B$. Si $a \in A$ y $b \in B$, escribimos $a\mathscr{R}b$ cuando $(a, b) \in \mathscr{R}$, y $a\not\mathscr{R}b$ cuando $(a, b) \notin \mathscr{R}$. Si $A = B$, diremos simplemente que $\mathscr{R}$ es una relación en A.

Denotaremos las relaciones por las letras cursivas mayúsculas $\mathscr{R}$, $\mathscr{S}$, o $\mathscr{T}$.

Ejemplo 14.1.2. Dados A y B conjuntos, $\varnothing \subseteq A \times B$ es una relación de A en B que denomimamos *relación vacía*.

Ejemplo 14.1.3. Sean $A = \{2, 3, 4, 5\}$ y $B = \{a, b, c, d\}$. Existen muchas posibles relaciones de A en B. Por ejemplo, consideremos la relación $\mathscr{R}$ definida por el conjunto $\{(2, b), (3, c), (4, c)\}$. Entonces $(2, b) \in \mathscr{R}$, $(3, c) \in \mathscr{R}$ y $(4, c) \in \mathscr{R}$, pero $(4, d) \notin \mathscr{R}$ y $(2, a) \notin \mathscr{R}$.

Ejemplo 14.1.4. Sean X conjunto y $A := \mathscr{P}(X)$. Definimos la siguente relación en A:

$$\subseteq := \{(Y, Z) \in A \times A : Y \text{ es subconjunto de } Z\}.$$

Esta relación la denominamos *ser subconjunto de*.

Ejemplo 14.1.5. La relación en $\mathbb{R}$,

$$\leq := \{(x.y) \in \mathbb{R} \times \mathbb{R} : x \text{ es menor o igual que } y\},$$

es la que denominamos *orden usual de los números reales*.

Ejemplo 14.1.6. En $\mathbb{Z}^+ := \{n \in \mathbb{Z} : n > 0\}$, definimos la relación de *divide a* de la siguiente manera:

$$| := \{(m, n) \in \mathbb{Z} \times \mathbb{Z} : m \text{ divide a } n\}.$$

Esta relación fue introducida en la Lección 6.

Ejemplo 14.1.7. Dado $k \in \mathbb{Z}^+$, definimos la siguiente relación:

$$\equiv_k := \{(m, n) \in \mathbb{Z} \times \mathbb{Z} : k \text{ divide a } m - n\}.$$

Esta relación se denomina *congruencia módulo k* en $\mathbb{Z}$. En el caso de que dados $a, b \in \mathbb{Z}$ se tenga que $a \equiv_k b$, también es muy usual denotar esto por $a \equiv b \pmod{k}$. Esta relación será estudiada con más cuidado en la siguiente lección.

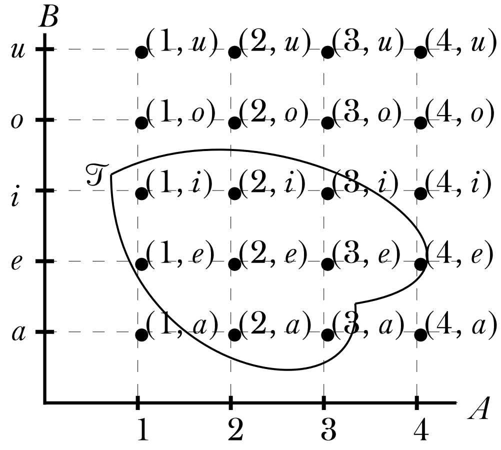
14.2. Representación de relaciones

Hay por lo menos dos maneras reconocidas de representar relaciones. Una está apoyada en la representación que presentamos en la Lección 13 para el producto cartesiano de dos conjuntos. La otra se hace mediante diagramas de flechas. En los siguientes ejemplos mostramos estas formas de representar relaciones.

Ejemplo 14.2.1. Consideremos $A = \{1, 2, 3, 4\}$ y $B = \{a, e, i, o, u\}$. Consideremos la relación

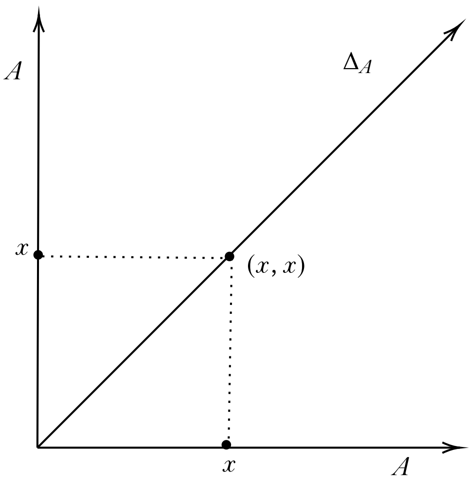
$$\begin{aligned}\mathcal{T} = \{\, &(1, e), (1, i), (2, a), (2, e), (2, i),\\ &(3, a), (3, e), (3, i), (4, e)\,\}.\end{aligned}$$

La siguiente es una representación de esta relación $\mathcal{T} \subseteq A \times B$, basada en el gráfico de $A \times B$ del Ejemplo 13.3.1.



Este tipo de representación es llamado *gráfico* de una relación.

Ejemplo 14.2.2. Sea A un conjunto. El conjunto $\{(x, y) \in A \times A \mid x = y\}$ es denotado usualmente por Δ_A y se denomina la *relación diagonal* de A. A continuación presentamos el gráfico de una relación Δ_A. En este gráfico usamos una semirrecta para representar los elementos del conjunto A.

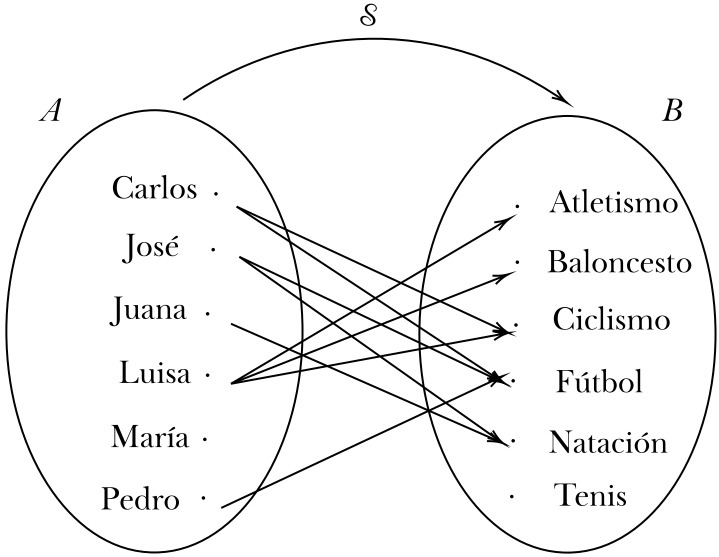


Ejemplo 14.2.3. Otra manera de representar las relaciones es usando diagramas de flechas. Para mostrar esto consideremos una relación $\mathcal{S}$ de A en B, donde A = {Carlos, José, Juana, Luisa, María, Pedro} y B = {Atletismo, Baloncesto, Ciclismo, Fútbol, Natación, Tenis}.

Diremos que la pareja $(X, Y) \in \mathcal{S}$ donde $X \in A$ y $Y \in B$ si y solo si X practica el deporte Y. Supongamos que

$$\begin{aligned}\mathcal{S} = \Big\{&(\text{Carlos, Ciclismo}), (\text{Carlos, Fútbol}), (\text{José, Fútbol}),\\ &(\text{José, Natación}),(\text{Juana, Natación}), (\text{Luisa, Atletismo}),\\ &(\text{Luisa, Baloncesto}),(\text{Luisa, Ciclismo}), (\text{Pedro, Fútbol})\Big\}.\end{aligned}$$

La representación de esta relación $\mathcal{S}$ mediante el diagrama de flechas es la siguiente:

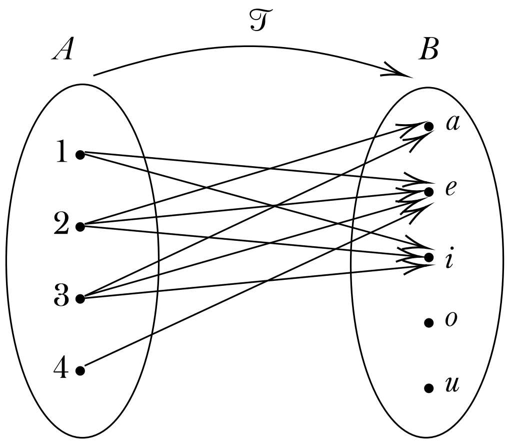


Esta imagen está compuesto por la representación de los conjuntos A y B como diagramas de Venn, en los que se resalta cada uno de sus elementos, y por las flechas que salen de elementos de A y llegan a elementos de B. Cada una de estas flechas representa a cada pareja ordenada que está en $\mathcal{S}$. Así por ejemplo, vemos que (*Juana, Natación*)$\in \mathcal{S}$ y en correspondencia en el gráfico de arriba hay una flecha que sale de *Juana* y llega a *Natación*. De manera semejante vemos que de *Carlos* sale una flecha que llega a *Ciclismo* esto significa que la pareja (*Carlos, Ciclismo*)$\in \mathcal{S}$, es decir, Carlos practica Ciclismo. Notamos de esta representación que *María* no practica deporte alguno y que ninguno de este grupo de amigos A practica *Tenis*. También podemos ver que *Luisa* es una gran deportista pues practica tres deportes que son *Atletismo*, *Baloncesto* y *Ciclismo*; el *Fútbol* es practicado por los tres hombres de este grupo y ninguna de las mujeres lo practica. Como acabamos de ver, este diagrama de flechas nos brinda información rápida de la relación $\mathcal{S}$.

Ejemplo 14.2.4. La siguiente es la representación de la relación

$$\mathcal{T} = \{(1,e),(1,i),(2,a),(2,e),(2,i),(3,a),(3,e),(3,i),(4,e)\}$$

de $A = \{1,2,3,4\}$ en $B = \{a,e,i,o,u\}$ del Ejemplo 14.2.1, mediante diagrama de flechas.



Podemos notar que de todos los elementos de A salen flechas pero no a todos los elementos de B llegan flechas.

En la siguiente subsección vemos que los diagramas de flechas inspiran nombres para los conjuntos A y B, y se resaltan los subconjuntos de A y de B de los cuales salen y llegan flechas, respectivamente.

14.3. Dominio y rango

Definición 14.3.1. Sea $\mathcal{R}$ una relación de A en B. El conjunto A será llamado *conjunto de salida* y el conjunto B será llamado *conjunto* *de llegada*. Definimos el *dominio* de $\mathcal{R}$, denotado por $dom(\mathcal{R})$, como el conjunto de todos los elementos $x \in A$ para los cuales *existe* $y \in B$ tales que $x\mathcal{R}y$ o lo que es lo mismo $(x, y) \in \mathcal{R}$; es decir

$$dom(\mathcal{R}) = \{x \in A \mid x\mathcal{R}y \quad \text{para algún } y \in B\}.$$

Definimos el *rango* de la relación $\mathcal{R}$, denotado por $rango(\mathcal{R})$, como el conjunto de todos los elementos $y \in B$ para los cuales *existe* $x \in A$ tales que $x\mathcal{R}y$ o lo que es lo mismo $(x, y) \in \mathcal{R}$; es decir

$$rango(\mathcal{R}) = \{y \in B \mid x\mathcal{R}y \quad \text{para algún } x \in A\}.$$

Nótese que de la anterior definición podemos decir que el dominio de la relación $\mathcal{R}$ coincide con el conjunto de las primeras componentes de las parejas ordenadas que pertenecen a $\mathcal{R}$, y el rango de la relación $\mathcal{R}$ coincide con el conjunto de las segundas componentes de las parejas ordenadas que pertenecen $\mathcal{R}$; en otras palabras, si tuvieramos un diagrama de flechas de la relación $\mathcal{R}$, $dom(\mathcal{R})$ coincide con el conjunto de todos los elementos de A de donde salen flechas y $rango(\mathcal{R})$ coincide con el conjunto de todos los elementos de B a donde llegan flechas.

Ejemplo 14.3.2. Aquí se tienen en cuenta las relaciones consideradas en los Ejemplos 14.1.2, 14.1.3, 14.1.4, 14.2.1, 14.2.2 y 14.2.3, respectivamente.
$dom(\emptyset) = rango(\emptyset) = \emptyset$,
$dom(\mathcal{R}) = \{2, 3, 4\}$ y $rango(\mathcal{R}) = \{b, c\}$,
$dom(\subseteq) = rango(\subseteq) = \mathcal{P}(X)$,
$dom(\mathcal{T}) = \{1, 2, 3, 4\} = A$ y $rango(\mathcal{T}) = \{a, e, i\}$,
$dom(\Delta_A) = rango(\Delta_A) = A$,
$dom(\mathcal{S}) = \{$*Carlos, José, Juana, Luisa, Pedro*$\}$ y
$rango(\mathcal{S}) = \{$*Atletismo, Baloncesto, Ciclismo, Fútbol, Natación*$\}$.

Como hemos observado en el anterior ejemplo, el dominio de una relación no necesariamente coincide con el conjunto de salida. Similarmente, el rango de una relación no necesariamente coincide con el conjunto de llegada. Lo que siempre es verdad para una relación $\mathcal{R}$ de A en B es lo siguiente:

$$dom(\mathcal{R}) \subseteq A, \quad rango(\mathcal{R}) \subseteq B \quad \text{y} \quad \mathcal{R} \subseteq dom(\mathcal{R}) \times rango(\mathcal{R}).$$

14.4. Relación inversa

Consideremos nuestro ejemplo coloquial de relación "ser progenitor biológico de", definido de manera matemática como

$$\mathscr{P} := \{(X, Y) \in A \times A : \ X \text{ es progenitor biológico de } Y\},$$

donde A es el conjunto de seres humanos. En dicho ejemplo tomamos que Sutana es progenitora biológica (es decir, es la madre biológica) de Perencejo, es decir $(Sutana, Perencejo) \in \mathscr{P}$. Si analizamos este vínculo en el sentido contrario, vemos que Perencejo es hijo biológico de Sutana. Esta relación "ser hijo biológico de" está estrechamente relacionada con la relación original "ser progenitor biológico de" en el sentido de que simplemente es tomar el vínculo que la define pero en el sentido contrario. Esto nos lleva al concepto de *relación inversa*.

Definición 14.4.1. Sea $\mathscr{R}$ una relación de un conjunto A en un conjunto B. La *relación inversa* de $\mathscr{R}$, denotada por $\mathscr{R}^{-1}$, se define como

$$\mathscr{R}^{-1} := \{(b, a) \in B \times A : (a, b) \in \mathscr{R}\}.$$

Observación 14.4.2. Dada $\mathscr{R}$ una relación de un conjunto A en un conjunto B,

$$dom(\mathscr{R}^{-1}) = rango(\mathscr{R}) \qquad \text{y} \qquad rango(\mathscr{R}^{-1}) = dom(\mathscr{R}).$$

Ejemplo 14.4.3. En el ejemplo coloquial

$$\mathscr{P} := \{(X, Y) \in A \times A : \ X \text{ es progenitor biológico de } Y\},$$

nótese que

$$\begin{aligned}\mathscr{P}^{-1} &= \{(X, Y) \in A \times A : Y \text{ es progenitor biológico de } X\}\\ &= \{(X, Y) \in A \times A : X \text{ es hijo biológico de } Y\}.\end{aligned}$$

Ejemplo 14.4.4. Consideremos $\mathscr{R}$ como en el Ejemplo 14.1.3. Notamos que $\mathscr{R}^{-1} = \{(b, 2), (c, 3), (c, 4)\}$, $dom(\mathscr{R}^{-1}) = \{b, c\}$ y $rango(\mathscr{R}^{-1}) = \{2, 3, 4\}$.

Definición 14.4.5. Sean A y B conjuntos cualesquiera y sean $\mathcal{R}$ y $\mathcal{S}$ dos relaciones de A en B. Decimos que $\mathcal{R} = \mathcal{S}$ cuando ambas relaciones están definidas por el mismo subconjunto de $A \times B$. En otras palabras, $\mathcal{R} = \mathcal{S}$ cuando para cualesquiera $x \in A$ y $y \in B$ se tiene que $x\mathcal{R}y$ si y solo si $x\mathcal{S}y$.

Una demostración de que una relación $\mathcal{R}$ es igual a otra relación $\mathcal{S}$ es típicamente una demostración de igualdad entre conjuntos.

Ejemplo 14.4.6. Consideremos el conjunto $A := \{1, 2, 4\}$ y las relaciones $\mathcal{R} := \{(x, y) \in A \times A : x \leq y\}$ y $\mathcal{S} := \{(x, y) \in A \times A : x \text{ divide a } y\}$. Nótese que

$$\mathcal{R} = \{(1, 1), (1, 2), (1, 4), (2, 2), (2, 4), (4, 4)\} = \mathcal{S}.$$

14.5. Clases de una relación

Pensemos nuevamente en nuestra relación coloquial "ser progenitor biológico de". Tomando X :=Sutana, nos podemos preguntar quiénes están relacionados con Sutana por medio de esta relación (es decir, quiénes son hijos biológicos de Sutana). Este conjunto lo denominamos la *clase* de Sutana relativa a la relación "ser progenitor biológico de".

Este concepto lo podemos formalizar para relaciones arbitrarias, como veremos a continuación.

Definición 14.5.1. Sean A y B conjuntos no vacíos, sea $\mathcal{R}$ una relación de A en B, y sea $x \in A$. La *clase* de x con respecto a $\mathcal{R}$, denotada por $[x]_{\mathcal{R}}$, es el conjunto de todos los elementos de B tales que x se relaciona con ellos mediante $\mathcal{R}$, es decir,

$$[x]_{\mathcal{R}} = \{y \in B \mid x \,\mathcal{R}\, y\}.$$

Si no hay riesgo de confusión con alguna otra relación, la clase de x respecto a $\mathcal{R}$ será denotada simplemente por $[x]$ en lugar de $[x]_{\mathcal{R}}$.

Ejemplo 14.5.2. Continuamos con las relaciones dadas en los Ejemplos 14.1.3, 14.1.4 y 14.2.2.

1. Observamos que $[2]_{\mathcal{R}} = \{b\}$ (puesto que $(2, b) \in \mathcal{R}$ y ningún otro elemento $x \in B$ satisface que $(2, x) \in \mathcal{R}$), $[3]_{\mathcal{R}} = [4]_{\mathcal{R}} = \{c\}$ (dado que $(3, c), (4, c) \in \mathcal{R}$ y ningún otro elemento $x \in B$ satisface que $(3, x) \in \mathcal{R}$ ni $(4, c) \in \mathcal{R}$) y $[5]_{\mathcal{R}} = \phi$ (ya que para ningún $x \in B$ tenemos que $(5, x) \in \mathcal{R}$).

2. $[P]_{\subseteq} = \{Q \in \mathcal{P}(A) \,|\, P \subseteq Q\}$ para cualquier $P \in \mathcal{P}(A)$ fijo, puesto que para todo $Q \in \mathcal{P}(A)$ tenemos que $(P, Q) \in \subseteq$ si y solo si $P \subseteq Q$.

3. $[x]_{\Delta_A} = \{x\}$ para $x \in A$ fijo, puesto que dado $y \in A$ tenemos que $(x, y) \in \Delta_A$ si y solo si $x = y$.

14.6. Composición de relaciones

Volvamos nuevamente a nuestra relación coloquial "ser progenitor biológico". Si Sutana es abuela (biológica) de Fulano, es porque Sutana es la madre (biológica) de alguno de los padres de Fulano, es decir, existe una persona (la madre o el padre biológico de Fulano, llamémosla X) tal que Sutana es progenitora biológica de X y X es progenitor biológico de Fulano. Vemos que la relación "ser abuelo de" puede ser obtenida de esta manera a partir de la relación (*a priori* más primitiva) "ser progenitor biológico de". Esto lo podemos formalizar matemáticamente por medio de lo que conocemos como *composición de relaciones*.

Definición 14.6.1. Sean A, B y C conjuntos, $\mathcal{S}$ una relación de A en B y $\mathcal{R}$ una relación de B en C. Entonces, se define una nueva relación $\mathcal{R} \circ \mathcal{S}$ de A en C llamada *relación compuesta* de $\mathcal{R}$ y $\mathcal{S}$ cuyos elementos son las parejas $(a, c) \in A \times C$ para las cuales existe $b \in rango(\mathcal{S}) \cap dom(\mathcal{R}) \subseteq B$ tal que $(a, b) \in \mathcal{S}$ y $(b, c) \in \mathcal{R}$. Es decir,

$$\mathcal{R} \circ \mathcal{S} = \{(a, c) \in A \times C \,|\, (a, b) \in \mathcal{S} \text{ y } (b, c) \in \mathcal{R} \text{ para algún } b \in B\}.$$

Observación 14.6.2. Dados A, B y C conjuntos, $\mathcal{S}$ una relación de A en B y $\mathcal{R}$ una relación de B en C, tenemos que

$$dom(\mathcal{R} \circ \mathcal{S}) = \{a \in dom(\mathcal{S}) \,|\, a\mathcal{S}b \text{ para algún } b \in dom(\mathcal{R})\}.$$

Ejemplo 14.6.3. Sean $A := \{a, b, c, d\}$, $\mathcal{S} := \{(a, b), (a, c), (b, c)\}$ y $\mathcal{R} := \{(a, a), (b, c), (c, d)\}$.

1. Puesto que $(a, b) \in \mathcal{S}$ y $(b, c) \in \mathcal{R}$, entonces podemos decir que $(a, c) \in \mathcal{R} \circ \mathcal{S}$.

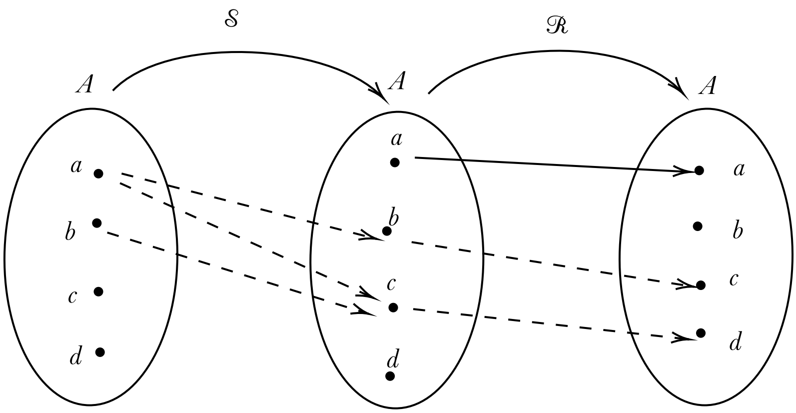
2. Puesto que $(a, c) \in \mathcal{S}$ y $(c, d) \in \mathcal{R}$, entonces podemos decir que $(a, d) \in \mathcal{R} \circ \mathcal{S}$.

3. Puesto que $(b, c) \in \mathcal{S}$ y $(c, d) \in \mathcal{R}$, entonces podemos decir que $(b, d) \in \mathcal{R} \circ \mathcal{S}$.

   No hay más posibilidades donde $(x, y) \in \mathcal{S}$ y $(y, z) \in \mathcal{R}$, entonces podemos decir que

$$\mathcal{R} \circ \mathcal{S} = \{(a, c), (a, d), (b, d)\}.$$

El diagrama de flechas de estas relaciones es el siguiente:



Basados en este diagrama de flechas, podemos ver que las parejas ordenadas (x, z) que pertenecen a la relación $\mathcal{R} \circ \mathcal{S}$ son aquellas que satisfacen que a partir de $x \in A$ sale una flecha, por medio de la relación $\mathcal{S}$, que llega a algún elemento $y \in A$, y que después se conecta con otra flecha que sale de y y, vía $\mathcal{R}$, llega a $z \in A$. Vemos que de esta manera salen flechas conectadas de a hacia c y hacia d y de b hacia d. Concluimos igualmente que $\mathcal{R} \circ \mathcal{S} = \{(a, c), (a, d), (b, d)\}$.

14.7. Ejercicios

Ejercicio 14.7.1. Considere las siguientes relaciones definidas en $A := \{1, 2, 3, 4\}$:

1. $\mathcal{R}_1 := \{(1, 1), (2, 2), (3, 3), (2, 1), (1, 2)\}$.
2. $\mathcal{R}_2 := \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 3), (1, 3)\}$.
3. $\mathcal{R}_3 := \varnothing$.
4. $\mathcal{R}_4 := A \times B$ como relación definida en un conjunto arbitrario B, y donde $A \subseteq B$.
5. $\mathcal{R}_5 := \{(a, b) \in A \times A : a + b = 6\}$.

Determine:

a) $\mathcal{R}_2 \circ \mathcal{R}_1$ b) $\mathcal{R}_4^{-1}$ c) $\mathcal{R}_4 \circ \mathcal{R}_5$ d) $(\mathcal{R}_3 \circ \mathcal{R}_5)^{-1}$

Ejercicio 14.7.2. Consideremos U como el conjunto de divisiones político-administrativas de Colombia y de personas nacidas en Colombia. Dados

$$D = \{x \in U : x \text{ es un departamento de Colombia}\},$$
$$C = \{y \in U : y \text{ es una ciudad de Colombia}\} \text{ y}$$
$$A = \{t \in U : t \text{ es un alumno del curso de fundamentos}\},$$

considere las siguientes relaciones:

1. $\mathcal{R}_1 \subseteq D \times C$ definida como sigue: $x\mathcal{R}_1 y$ si y solo si y es la capital de x.
2. $\mathcal{R}_2 \subseteq A \times D$ definida como sigue: $t\mathcal{R}_2 x$ si y solo si t es oriundo de x.
3. $\mathcal{R}_3 \subseteq A \times D$ definida como sigue: $t\mathcal{R}_3 x$ si y solo si el nombre de t y x empiezan por la misma letra.

Definir por comprensión $\mathscr{R}_1 \cap \mathscr{R}_2$, $\mathscr{R}_2'$, $\mathscr{R}_1^{-1}$, $\mathscr{R}_3 \cap \mathscr{R}_2$, $\mathscr{R}_1 \circ \mathscr{R}_2$ y dar ejemplos de por lo menos dos parejas que estén y dos parejas que no estén en cada relacion.

*** Recuerde que dada una relación $\mathscr{R} \subseteq A \times B$ se define $\mathscr{R}' := (A \times B) - \mathscr{R}$.

Ejercicio 14.7.3. Considere las siguientes relaciones definidas en el conjunto de los números naturales:

i) $m \mathscr{R}_1 n$ si y solo si $m < n$.

ii) $m \mathscr{R}_2 n$ si y solo si m divide a n.

iii) $m \mathscr{R}_3 n$ si y solo si $n = 3m + 1$.

iv) $m \mathscr{R}_4 n$ si y solo si n y m tienen el mismo número de divisores.

1. Encuentre, si es posible, por lo menos cinco parejas que pertenezcan a cada relación.
2. Determine las relaciones $\mathscr{R}_1 \cap \mathscr{R}_2$, $\mathscr{R}_2'$, $\mathscr{R}_3^{-1}$, $\mathscr{R}_3 \cup \mathscr{R}_2$, $\mathscr{R}_1 \cap \mathscr{R}_3$, $\mathscr{R}_1 \circ \mathscr{R}_2$, $\mathscr{R}_3 \circ \mathscr{R}_2$, $\mathscr{R}_2 \circ \mathscr{R}_3$ y dé, si es posible, por lo menos dos parejas que estén y dos parejas que no estén en cada relación.

Ejercicio 14.7.4. Sea $D := \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Para cada una de las siguientes relaciones, determine el dominio y el rango.

i) $\mathscr{R}_1 = \{(x, y) \in D \times D \mid x < y + 1\}$.

ii) $\mathscr{R}_2 = \{(x, y) \in D \times D \mid y = x^2\}$.

iii) $\mathscr{R}_3 = \{(s, t) \in D \times D \mid s + t \text{ es par}\}$.

iv) $\mathscr{R}_2 \cap \mathscr{R}_3$.

v) $(\mathscr{R}_1)'$.

vi) $\mathscr{R}_4 \subseteq (D \times D) \times (D \times D)$, definida por $(a, b)\mathscr{R}_4(c, d)$ si y solo si $a + c = b + d$.

vii) $\mathscr{R}_5 \subseteq \mathbb{N} \times \mathbb{N}$, definida por: $x\,\mathscr{R}_5\, y$ si y solo si x y y tienen el mismo residuo al dividirlos por 5.

viii) $\mathscr{R}_6 \subseteq \mathscr{P}(D) \times \mathscr{P}(D)$, definida por $X\,\mathscr{R}_6\,Y$ si y solo si $X \subseteq Y$.

Ejercicio 14.7.5. Teniendo en cuenta las relaciones dadas en el Ejercicio 14.7.4, determine cuáles de las siguientes afirmaciones son verdaderas y cuáles falsas. Justifique su respuesta.

1. Para todo elemento x de D existe y en D tal que (x, y) no está en $\mathscr{R}_1$.
2. Si una pareja (x, y) está en $\mathscr{R}_1$, la pareja (y, x) no está en $\mathscr{R}_1$.
3. Si una pareja (x, y) está en $\mathscr{R}_3$, la pareja (y, x) también está en $\mathscr{R}_3$.
4. Si (x, y) y (x, z) están en $\mathscr{R}_5$ entonces $y = z$.
5. Para $\mathscr{R}_3$ y $\mathscr{R}_5$ se tiene que todo elemento está relacionado con sí mismo.
6. Si (x, y) y (y, z) están en $\mathscr{R}_5$, entonces (x, z) también estará en $\mathscr{R}_5$.
7. Existen parejas de elementos de $\mathscr{P}(D)$ que no están relacionados según $\mathscr{R}_6$.
8. Existe un elemento X en $\mathscr{P}(D)$ tal que para todo elemento Y de $\mathscr{P}(D)$ se tiene $X\,\mathscr{R}_6\,Y$

Ejercicio 14.7.6. Si F es un clan familiar y en $F \times F$ se consideran las relaciones $\mathscr{P}$, $\mathscr{H}$ y $\mathscr{C}$ definidas así:

$$x\mathscr{P}y \text{ si y solo si } y \text{ es padre de } x,$$
$$x\mathscr{H}y \text{ si y solo si } y \text{ es hermano de } x,$$
$$x\mathscr{C}y \text{ si y solo si } y \text{ es conyuge de } x.$$

Exprese en términos de $\mathscr{P}$, $\mathscr{H}$ y $\mathscr{C}$, si es posible, las siguientes relaciones:

1. Ser tío.

2. Ser cuñado.

3. Ser primo.

4. Ser nieto.

5. Ser yerno.

Ejercicio 14.7.7. De los siguientes enunciados, determine si son verdaderos o si son falsos, justificando completamente su respuesta (demuestre o refute según el caso).

1. Dada $\mathcal{R}$ una relación en un conjunto A, entonces $\mathcal{R} = dom(\mathcal{R}) \times rango(\mathcal{R})$.

2. Dado A conjunto, demuestre que $\Delta_A^{-1} = \Delta_A$.

3. Dado A conjunto, demuestre que $\Delta_A \circ \Delta_A = \Delta_A$.

En esta última parte de la lección estudiaremos una relación muy importante que está definida sobre el conjunto de los números enteros. Esta relación no solo sirve como ejemplo para ilustrar las relaciones de equivalencia, que son nuestro objeto de estudio en la siguiente lección, sino que también es una herramienta valiosa en las matemáticas y sus aplicaciones, por ejemplo en teoría de números.

14.8. * Congruencias módulo n en $\mathbb{Z}$

Volvemos a citar el teorema conocido como el *Algoritmo de la división* de números enteros (el cual ya fue mencionado –Teorema 6.2.2–).

Teorema 14.8.1 (Algoritmo de la división)**.** *Sean $a, b \in \mathbb{Z}$ con $b > 0$. Existen enteros únicos $q, r \in \mathbb{Z}$ tales que $a = bq + r$ donde $0 \leq r < b$.*

Para definir la relación anunciada entre números enteros, fijamos un entero positivo n. Por el *Algoritmo de la división* sabemos que al dividir cada entero entre n obtendremos residuos que solo pueden ser enteros no negativos menores estrictamente a n. Con esto, diremos que dos números enteros a y b están relacionados si y solo si el residuo de dividir a entre n es el mismo residuo de dividir b entre n. En otras palabras, dados a y b enteros, aplicando el Teorema 14.8.1, sabemos que existen enteros únicos q_1, r_1 y q_2, r_2 tales que $a = nq_1 + r_1$ y $b = nq_2 + r_2$ donde $0 \leq r_1,\ r_2 < n$. Entonces, a estará relacionado con b si y solo si $r_1 = r_2$. Cuando $r_1 = r_2$ tenemos que $a - b = n(q_1 - q_2)$, es decir, $n \mid a - b$ puesto que $q_1 - q_2$ es un entero. Nótese que esta relación que estamos definiendo entre números enteros depende del entero positivo n.

Definición 14.8.2. Ver Ejemplo 14.1.7. Sea $n \in \mathbb{Z}^+$ y sean $a, b \in \mathbb{Z}$. Diremos que el número a es *congruente* al número b *módulo* n, lo que es denotado por $a \equiv b \pmod{n}$, cuando $n \mid a - b$. Si no es verdad que $a \equiv b \pmod{n}$, como es costumbre, escribiremos: $a \not\equiv b \pmod{n}$.

Ejemplo 14.8.3.

1. $12 \equiv 5 \pmod{7}$ porque $7 \mid 12 - 5 = 7$.
2. $19 \equiv 31 \pmod{6}$ porque $19 - 31 = -12 = 6(-2)$, por lo que $6 \mid 19 - 31$.
3. $8 \equiv -5 \pmod{13}$ porque $8 - (-5) = 13 = 13(1)$, luego $13 \mid 8 - (-5)$.
4. $6 \not\equiv 9 \pmod{5}$ porque $6 - 9 = -3$ y -3 no es múltiplo de 5 (¿por qué?).
5. A diario usamos esta relación para calcular la hora del día en la que estamos. Por ejemplo, si un reloj marca las 18 horas del día, usando la relación de congruencia módulo 12, sabremos que son las 6 de la tarde puesto que $18 \equiv 6 \pmod{12}$ (¿por qué?).
6. Supóngase que son las 9 de la mañana en punto y que se quiere saber qué horas serán dentro de 59 horas. Lo primero que se hace es calcular $9+59 = 68$ y luego de 68 se sustrae venticuatro veces el número de veces que cabe 24 en 68, es decir, $68-48 =$

20 (nótese que $68 \equiv 20 \pmod{24}$ puesto que $24 \mid 68 - 20 = 48 = 24(2)$). Este número que se obtiene es un número en el rango de 1 a 24. Finalmente, como $20 \equiv 8 \pmod{12}$ (¿por qué?), concluimos que en 59 horas serán las 8 p.m.

Para cada $n \in \mathbb{Z}^+$, tenemos una relación en $\mathbb{Z}$ que es dada por congruencia módulo n. El siguiente lema nos muestra que para cada n entero positivo, la relación de congruencia módulo n satisface algunas propiedades que estudiaremos en la siguiente lección.

Lema 14.8.4. *Sea $n \in \mathbb{Z}^+$ y sean a, b y $c \in \mathbb{Z}$.*

1. *$a \equiv a \pmod{n}$.*
2. *Si $a \equiv b \pmod{n}$ entonces $b \equiv a \pmod{n}$.*
3. *Si $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n}$, entonces $a \equiv c \pmod{n}$.*

Demostración. Sea $n \in \mathbb{Z}^+$ fijo.

1. Sean $a \in \mathbb{Z}$ cualquiera. Como $a - a = 0 = 0 \cdot n$, entonces $a \equiv a \pmod{n}$.
2. Sean $a, b \in \mathbb{Z}$ cualesquiera. Supóngase que $a \equiv b \pmod{n}$. Así, $a - b = kn$ para algún $k \in \mathbb{Z}$. Luego, $b - a = (-k)n$ (¿por qué?). Como $-k \in \mathbb{Z}$, se concluye que $b \equiv a \pmod{n}$.
3. Sean $a, b, c \in \mathbb{Z}$ cualesquiera. Supongamos que $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n}$. Esto significa que existen $k, j \in \mathbb{Z}$ tales que $a - b = kn$ y $b - c = jn$. Luego, $a - c = (a - b) + (b - c) = kn + jn = (k + j)n$ (¿por qué?). Como $k + j \in \mathbb{Z}$, podemos concluir que $a \equiv c \pmod{n}$.

☑

El siguiente teorema nos da información muy valiosa acerca de la relación de congruencia módulo n. La demostración de este resultado es consecuencia directa del *Algoritmo de la división* mencionado en el Teorema 14.8.1.

Teorema 14.8.5. *Sea $n \in \mathbb{Z}^+$ fijo y sea $a \in \mathbb{Z}$ cualquiera. Entonces, existe un único $r \in \{0, 1, \ldots, n-1\}$ tal que $a \equiv r \pmod{n}$.*

Demostración. Por aplicación del *Algoritmo de la división* 14.8.1 podemos decir que existen enteros únicos q y $r \in \mathbb{Z}$ tales que $a = nq + r$ y $0 \leq r < n$. Entonces $a - r = qn$, es decir, $a \equiv r \pmod{n}$. Esto prueba el resultado de existencia del teorema.

Para probar la unicidad, supongamos que existen enteros $x, y \in \{0, 1, \ldots, n-1\}$ tales que $a \equiv x \pmod{n}$ y $a \equiv y \pmod{n}$. Por el Lema 14.8.4 parte 2, tenemos que $x \equiv a \pmod{n}$, y por el Lema 14.8.4 parte 3, $x \equiv y \pmod{n}$. Esto último equivale a afirmar que existe $p \in \mathbb{Z}$ tal que $x - y = pn$. Así, $x - y$ es un múltiplo de n. Denotemos el conjunto $\{k \in \mathbb{Z} : \text{ existe } p \in \mathbb{Z} \text{ tal que } k = pn\}$ de todos los múltiplos de n por $n\mathbb{Z}$.

Puesto que $x, y \in \{0, 1, \ldots, n-1\}$, tenemos que

$$-y \in \{-(n-1), -(n-2), \ldots, -2, -1, 0\}.$$

Esto significa que x y y son enteros tales que

$$0 \leq x \leq n - 1$$

y

$$-(n-1) \leq -y \leq 0.$$

Entonces $x - y \in \{m \in \mathbb{Z} \mid -(n-1) \leq m \leq n-1\}$. Denotemos este conjunto por A_n. Es decir,

$$x - y \in \{-(n-1), -(n-2), \ldots, -2, -1, 0, 1, 2, \ldots, n-1\} = A_n.$$

Por lo tanto, $x - y \in n\mathbb{Z}$ y $x - y \in A_n$, esto es

$$x - y \in n\mathbb{Z} \cap A_n = \{0\}.$$

Entonces $x - y = 0$ y, por lo tanto, $x = y$. ☑

Podemos reescribir el Teorema 14.8.5 sin hacer referencia a la relación de congruencia módulo n de la siguiente manera.

Corolario 14.8.6. *Sea $n \in \mathbb{Z}^+$ fijo y sea $a \in \mathbb{Z}$ cualquiera. Entonces, una y solo una de las siguientes afirmaciones es verdad: $a = nk$ para algún*

$k \in \mathbb{Z}$ o $a = nk + 1$ para algún $k \in \mathbb{Z}$ o $a = nk + 2$ para algún $k \in \mathbb{Z}$, ..., o $a = nk + (n - 1)$ para algún $k \in \mathbb{Z}$.

14.9. * Clases Residuales

Para entender mejor el resultado del Teorema 14.8.5 fijemos $n \in \mathbb{Z}^+$, por ejemplo tomemos $n = 5$. En este caso particular, determinemos las diferentes clases respecto a la relación congruencia módulo 5 y notemos que cada entero se encuentra en una y solo una de las clases [0], [1], [2], [3], o [4]. Veamos:

$$\begin{aligned}
&\vdots\\
[-1] &= \{\ldots, -11, -6, -1, 4, 9, \ldots\}\\
[0] &= \{\ldots, -10, -5, 0, 5, 10, \ldots\}\\
[1] &= \{\ldots, -9, -4, 1, 6, 11, \ldots\}\\
[2] &= \{\ldots, -8, -3, 2, 7, 12, \ldots\}\\
[3] &= \{\ldots, -7, -2, 3, 8, 13, \ldots\}\\
[4] &= \{\ldots, -6, -1, 4, 9, 14, \ldots\}\\
[5] &= \{\ldots, -5, 0, 5, 10, 15, \ldots\}\\
&\vdots
\end{aligned}$$

Además, vemos que estas clases, también llamadas *clases residuales*, se repiten cada cinco enteros, es decir:

$$\begin{aligned}
\cdots = [-10] = [-5] = [0] = [5] = [10] = \cdots\\
\cdots = [-9] = [-4] = [1] = [6] = [11] = \cdots\\
\cdots = [-8] = [-3] = [2] = [7] = [12] = \cdots\\
\cdots = [-7] = [-2] = [3] = [8] = [13] = \cdots\\
\cdots = [-6] = [-1] = [4] = [9] = [14] = \cdots
\end{aligned}$$

A pesar de que a cada entero le corresponde una clase, en efecto, hay apenas cinco clases residuales distintas respecto a la relación congruencia módulo 5, las cuales son: [0], [1], [2], [3] y [4]. Además, estas clases son disyuntas dos a dos y su unión es todo $\mathbb{Z}$. Lo mismo ocurre para cualquier valor de n como se enuncia en el siguiente teorema.

Teorema 14.9.1. *Sea $n \in \mathbb{Z}^+$ fijo y sean a, $b \in \mathbb{Z}$ cualesquiera.*

1. *Si $a \equiv b \pmod n$, entonces $[a] = [b]$.*
2. *Si $a \not\equiv b \pmod n$, entonces $[a] \cap [b] = \emptyset$.*
3. $[0] \cup [1] \cup [2] \cup \cdots \cup [n-1] = \mathbb{Z}$.

Demostración. Sea $n \in \mathbb{Z}^+$ fijo y sean a y b enteros cualesquiera.

1. Supongamos que $a \equiv b \pmod n$. Probemos la igualdad entre conjuntos $[a] = [b]$. Así, sea $x \in [a]$ cualquiera. Por definición de clases sabemos que $a \equiv x \pmod n$. Como la relación de congruencia módulo n satisface la parte 2 del Lema 14.8.4, se sigue que $b \equiv a \pmod n$ y, por la parte 3 del Lema 14.8.4 tenemos que, $b \equiv x \pmod n$. Esto significa que $x \in [b]$, por lo tanto, $[a] \subseteq [b]$. El mismo argumento, pero cambiando la letra a por la letra b, nos permite concluir que $[b] \subseteq [a]$. Entonces, $[a] = [b]$.

2. Razonamos por reducción al absurdo para concluir 2. Supongamos que $a \not\equiv b \pmod n$ y que $[a] \cap [b] \neq \emptyset$. Entonces, existe al menos un $y \in [a] \cap [b]$, es decir, $y \in [a]$ y también $y \in [b]$. De nuevo, por la definición de clases sabemos que, $a \equiv y \pmod n$ y $b \equiv y \pmod n$. Luego, por la parte 2 del Lema 14.8.4 tenemos que $y \equiv b \pmod n$ y por la la parte 3 del Lema 14.8.4 concluimos que $a \equiv b \pmod n$, lo cual es absurdo. Esto prueba lo que queríamos.

3. La afirmación en 3 es una igualdad entre conjuntos, así que debemos probar la doble contenencia. Por definición de las clases tenemos que dado cualquier $z \in \mathbb{Z}$, vale que $[z] \subseteq \mathbb{Z}$. Por lo tanto, por Proposición 12.4.1 (4), $[0] \cup [1] \cup [2] \cup \cdots \cup [n-1] \subseteq \mathbb{Z}$.
   Ahora, sea $x \in \mathbb{Z}$ cualquiera. Por aplicación del Teorema 14.8.5, existe un único $r \in \{0, 1, \cdots, n-1\}$ tal que $x \equiv r \pmod n$.

Como la relación de congruencia satisface la parte 2 del Lema 14.8.4 también es válido que $r \equiv x \pmod{n}$, así que, $x \in [r]$ donde r es alguno de los elementos del conjunto $\{0, 1, \cdots, n-1\}$, entonces, $x \in [0] \cup [1] \cup [2] \cup \cdots \cup [n-1]$. Esto prueba que $\mathbb{Z} \subseteq [0] \cup [1] \cup [2] \cup \cdots \cup [n-1]$. Luego, $[0] \cup [1] \cup [2] \cup \cdots \cup [n-1] = \mathbb{Z}$.

☑

El Teorema 14.9.1 nos permite ver que las clases para las relaciones de congruencia módulo n cumplen propiedades muy particulares, comparadas con las clases respecto a relaciones arbitrarias; estas propiedades nos permitirán caracterizar las relaciones de equivalencia y serán estudiadas en el Teorema 16.2.1 de la Lección 16.

Definición 14.9.2. Sea $n \in \mathbb{Z}^+$ fijo. El conjunto de todas las clases respecto a la relación de congruencia módulo n, denotado por $\mathbb{Z}_n$, es la familia definida por

$$\mathbb{Z}_n = \{[m] \, : \, m \in \mathbb{Z}\} = \{[0], [1], \cdots, [n-1]\},$$

donde los elementos son llamados *clases residuales* determinadas por la relación de congruencia módulo n.

Ejemplo 14.9.3. La familia de las clases residuales respecto a la relación congruencia módulo 9 es el conjunto $\mathbb{Z}_9 = \{[0], [1], \cdots, [8]\}$. Este conjunto tiene 9 elementos y cada uno de estos 9 elementos es a su vez un conjunto, los cuales serán vistos en este contexto como simples elementos. Así, escribiremos por ejemplo que: $[6] \in \mathbb{Z}_9$.

14.10. * Ejercicios

Ejercicio 14.10.1. Sean $m, n \in \mathbb{Z}^+$ y $a, b \in \mathbb{Z}$. Demuestre que si $m \mid n$ y $a \equiv b \pmod{n}$, entonces $a \equiv b \pmod{m}$.

Ejercicio 14.10.2. Sean $n \in \mathbb{Z}^+$ y $a, b \in \mathbb{Z}$. Demuestre que si $a \equiv b \pmod{n}$, entonces $n \mid a$ si y solo si $n \mid b$.

Ejercicio 14.10.3. Sea $n \in \mathbb{Z}$. ¿Es $n^3 \equiv n \pmod{6}$? Justifique su respuesta.

Ejercicio 14.10.4. Demuestre o dé un contraejemplo para cada una de las siguientes afirmaciones según el caso.

1. Sean $n \in \mathbb{Z}^+$ y $a, b, c \in \mathbb{Z}$. Si $a + c \equiv b + c \pmod{n}$, entonces $a \equiv b \pmod{n}$.
2. Sean $n \in \mathbb{Z}^+$ y $a, b, c \in \mathbb{Z} - \{0\}$. Si c no es múltiplo de n y $ac \equiv bc \pmod{n}$, entonces $a \equiv b \pmod{n}$.

Ejercicio 14.10.5. Demuestre que para todo natural n solo una de las siguientes afirmaciones se cumple: $n \equiv 0(mod\ 4)$, $n \equiv 1(mod\ 4)$, $n \equiv 2(mod\ 4)$ o $n \equiv 3(mod\ 4)$.

Lección *quince*

Algunos tipos especiales de relaciones

Las relaciones que presentaremos aquí son fundamentales en diversos contextos de las matemáticas y otras disciplinas, como la informática, la lógica, la economía e incluso las ciencias sociales. A lo largo de las siguientes lecciones solo consideraremos relaciones en un conjunto A. Es decir, relaciones de A en A; o mejor, relaciones contenidas en $A \times A$.

15.1. Relaciones reflexivas

La palabra *reflexivo* viene del latín *reflexus*, que es el participio pasado del verbo *reflectĕre* que significa "volver hacia atrás". Esto explica el nombre de este tipo de relaciones; puesto que si dibujáramos una flecha para mostrar el vínculo entre un elemento $x \in A$ arbitrario y él mismo, esa flecha volvería hacia el mismo elemento.

Definición 15.1.1. Una relación $\mathcal{R}$ en A se dice *reflexiva* en A cuando *todo* elemento $x \in A$ está relacionado mediante $\mathcal{R}$ consigo mismo. Es decir, $\mathcal{R}$ es reflexiva en A si y solo si $x\mathcal{R}x$ *para todo* $x \in A$.

Observación 15.1.2. Una relación $\mathcal{R}$ en A *no* es *reflexiva* en A si y solo si *existe* al menos un elemento $x \in A$ tal que $x\not{\mathcal{R}}x$.

A continuación, mostramos algunos ejemplos refiriéndonos a las relaciones que se presentaron en los Ejemplos 14.1.2, 14.1.3, 14.1.4, 14.1.5, 14.1.6, 14.1.7 y 14.2.2.

Ejemplo 15.1.3. Consideremos la relación vacía $\mathcal{R} := \varnothing$ dada en el Ejemplo 14.1.2, en el caso particular de que $A = B = \varnothing$. Notemos que $\mathcal{R} = \varnothing$ como relación en $A = \varnothing$ es reflexiva; de lo contrario, existiría $x \in A = \varnothing$ (contradicción) tal que $(x, x) \notin \mathcal{R} = \varnothing$. Como relación sobre un conjunto $A \neq \varnothing$, observemos que $\mathcal{R} = \varnothing$ no es una relación reflexiva. Como A es no vacío, tiene por lo menos un elemento $x \in A$. Claramente, por definición del conjunto vacío, tenemos que $(x, x) \notin \varnothing = \mathcal{R}$.

Ejemplo 15.1.4. En la relación dada en el ejemplo 14.1.3, tomando $A = \{2, 3, 4, 5\}$ y $B = \{a, b, c, d\}$, no tiene sentido examinar si la relación $\mathscr{R} := \{(2, b), (3, c), (4, c)\}$ es reflexiva porque el conjunto de llegada no es el mismo conjunto de salida.

Ejemplo 15.1.5. La relación *ser subconjunto de* presentada en el Ejemplo 14.1.4, $\subseteq := \{(Y, Z) \in \mathscr{P}(X) \times \mathscr{P}(X) : Y$ es subconjunto de $Z\}$, es una relación reflexiva en $\mathscr{P}(X)$ porque dado $Y \in \mathscr{P}(X)$ tenemos que Y es subconjunto de Y, en símbolos, $Y \subseteq Y$.

Ejemplo 15.1.6. La relación dada en el Ejemplo 14.2.2, Δ_A, la diagonal de A, es reflexiva en A puesto que, dado $x \in A$ tenemos que $x = x$, luego $(x, x) \in \Delta_A$.

Ejemplo 15.1.7. La relación

$$\leq := \{(x.y) \in \mathbb{R} \times \mathbb{R} : x \text{ es menor o igual que } y\}$$

dada en el ejemplo 14.1.5 es reflexiva en $\mathbb{R}$ porque todo $x \in \mathbb{R}$ satisface $x = x$, por lo tanto, x es menor o igual que x.

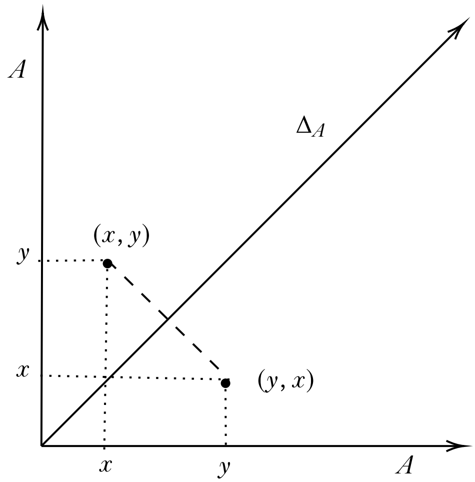
Ejemplo 15.1.8. La relación $| := \{(m, n) \in \mathbb{Z}^+ \times \mathbb{Z}^+ : m$ divide a $n\}$ definida en el Ejemplo 14.1.6 es reflexiva en $\mathbb{Z}^+$: en efecto, sea $m \in \mathbb{Z}^+$ cualquiera. Como $m \cdot 1 = m$ (1 es el neutro del producto en $\mathbb{Z}$), por definición de divisibilidad en $\mathbb{Z}$, tenemos que m divide a m, por lo tanto, $(m, m) \in |$.

Ejemplo 15.1.9. Dado $n \in \mathbb{Z}^+$. La relación $\equiv_n$ definida en el Ejemplo 14.1.7 (congruencia módulo n en $\mathbb{Z}$), es reflexiva tal como se vió en la parte 1 de la Proposición 14.8.4.

15.2. Relaciones simétricas

Informalmente, la *simetría* se refiere a una propiedad que describe la correspondencia exacta entre dos partes de un objeto o figura cuando se las compara a través de un punto, una recta o un plano. En nuestro caso, compararemos las relaciones contenidas en $A \times A$ con respecto a la diagonal Δ_A.

Definición 15.2.1. Una relación $\mathscr{R}$ en A se dice *simétrica* cuando para cualesquiera $x, y \in A$, si $x\mathscr{R}y$ entonces $y\mathscr{R}x$.



Este gráfico justifica el nombre de este tipo de relaciones debido al hecho de presentar una simetría con respecto a la diagonal de A, Δ_A. Más coloquialmente, si una pareja (x, y) está en la relación $\mathcal{R}$ y Δ_A fuera un espejo, su reflejo con respecto a Δ_A –la pareja (y, x)– también debería estar en la relación $\mathcal{R}$).

Observación 15.2.2. Una relación $\mathcal{R}$ en A *no* es *simétrica* si *existen* x, $y \in A$ tales que $x\mathcal{R}y$ pero $y\not{\mathcal{R}}x$.

A continuación, mostramos algunos ejemplos refiriéndonos a las relaciones que se presentaron en los Ejemplos 14.1.2, 14.1.3, 14.1.4, 14.1.5, 14.1.6, 14.1.7 y 14.2.2.

Ejemplo 15.2.3. Consideremos $B = A = \varnothing$. La relación vacía $\mathcal{R} = \varnothing$ definida en $A = \varnothing$ (Ejemplo 14.1.2) es simétrica, pues de lo contrario existirían $x, y \in A = \varnothing$ (contradicción) tales que $(x, y) \in \mathcal{R} = \varnothing$ y $(y, x) \notin \mathcal{R} = \varnothing$). $\mathcal{R} = \varnothing$ como relación sobre un conjunto $A \neq \varnothing$ continúa siendo una relación simétrica (¿por qué?).

Ejemplo 15.2.4. En la relación dada en el Ejemplo 14.1.3 donde tomamos $A = \{2, 3, 4, 5\}$ y $B = \{a, b, c, d\}$, no tiene sentido examinar si la relación $\mathcal{R} := \{(2, b), (3, c), (4, c)\}$ es simétrica porque el conjunto de llegada no es el mismo conjunto de salida.

Ejemplo 15.2.5. La relación $\subseteq$ del Ejemplo 14.1.4 *ser subconjunto de* en $\mathcal{P}(X)$ en general no es una relación simétrica. Considere $X \neq \varnothing$, $a \in X$, $P := \varnothing$ y $Q := \{a\}$. Notemos que $P \subseteq Q$ pero $Q \nsubseteq P$ (¿por qué?). Dejamos como ejercicio analizar qué pasaría si $X = \varnothing$.

Ejemplo 15.2.6. La relación Δ_A, la diagonal de A, (Ejemplo 14.2.2) es simétrica. En efecto, sean $x, y \in A$ tales que $(x, y) \in \Delta_A$, luego por la definición de Δ_A tenemos que $x = y$. De esto podemos decir que $y = x$, por lo tanto, $(y, x) \in \Delta_A$.

Ejemplo 15.2.7. La relación $\leq$ denominada *orden usual de los números reales* **no** es simétrica en $\mathbb{R}$ porque por ejemplo -3 es menor o igual que 5 pero 5 no es menor o igual a -3.

Ejemplo 15.2.8. La relación $| := \{(m, n) \in \mathbb{Z}^+ \times \mathbb{Z}^+ : m \text{ divide a } n\}$ (Ejemplo 14.1.6) *no* es simétrica. Notemos que 1 divide a 2 (puesto que $1 \cdot 2 = 2$) por lo que $1 \mid 2$, pero 2 no divide a 1 (¿por qué?) por lo que $2 \nmid 1$.

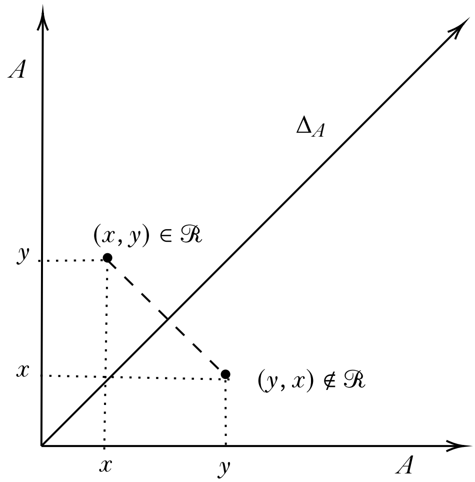
Ejemplo 15.2.9. Dado $n \in \mathbb{Z}^+$. La relación $\equiv_n$ denominada *congruencia* módulo n en $\mathbb{Z}$ (Ejemplo 14.1.7) es simétrica tal como se vió en la parte 2. de la Proposición 14.8.4.

15.3. Relaciones antisimétricas

El concepto de *antisimetría* impone una condición importante: dos elementos pueden estar relacionados en ambos sentidos (es decir, dados $a, b \in A$, a está relacionado con b y b con a) únicamente si son iguales. Es importante destacar que los conceptos de relación simétrica y antisimétrica no se excluyen mutuamente, ni son opuestos, ya que una relación puede cumplir con una de estas propiedades, con ambas, o con ninguna.

Definición 15.3.1. Una relación $\mathcal{R}$ en A se dice *antisimétrica* cuando para cualesquiera $x, y \in A$, si $x\mathcal{R}y$ y $y\mathcal{R}x$, entonces $x = y$.

Observación 15.3.2. Otra manera equivalente de definir que una relación $\mathcal{R}$ en A es *antisimétrica* es la siguiente: dados $x, y \in A$ con $x \neq y$, si $x\mathcal{R}y$, entonces $y\not\mathcal{R}x$.



La única posiblidad para que un par de parejas (x, y) y (y, x) estén simultáneamente en este tipo de relaciones es que estas parejas se encuentren dentro de la diagonal de A; es decir, que $x = y$.

Observación 15.3.3. Una relación $\mathcal{R}$ en A **no** es *antisimétrica* si y solo si *existen* $x, y \in A$ tales que $x\mathcal{R}y$, $y\mathcal{R}x$ *pero* $x \neq y$.

Ejemplo 15.3.4. Observaremos que *antisimetría* **no** significa la negación de simetría. Consideremos la relación Δ_A en un conjunto $A \neq \emptyset$ (la diagonal de A, ver Ejemplo 14.2.2), vimos que esta relación es simétrica (Ejemplo 15.2.6). Veamos que también esta relación es antisimétrica: sean $a, b \in A$ cualesquiera tales que $(a, b) \in \Delta_A$ y $(b, a) \in \Delta_A$. Por definición de Δ_A, como $(a, b) \in \Delta_A$, tenemos que $a = b$. Por lo tanto, Δ_A es antisimétrica. De esta manera, tenemos un ejemplo de una relación que simultáneamente es *simétrica* y *antisimétrica*.

Ejemplo 15.3.5. $\emptyset$ como relación (Ejemplo 14.1.2) en $A \neq \emptyset$ es una relación antisimétrica. De lo contrario, existirían $x, y \in A$ tales que $(x, y) \in \emptyset$, $(y, x) \in \emptyset$ (lo que claramente contradice la definición del conjunto vacío $\emptyset$) y $x \neq y$.

Ejemplo 15.3.6. Dados $A = \{2, 3, 4, 5\}$ y $B = \{a, b, c, d\}$, no tiene sentido examinar si la relación $\mathcal{R} := \{(2, b), (3, c), (4, c)\}$ del Ejemplo 14.1.3 es antisimétrica, porque el conjunto de llegada no es el mismo conjunto de salida.

Ejemplo 15.3.7. La relación $\subseteq$, del Ejemplo 14.1.4 *ser subconjunto de*, es una relación antisimétrica, puesto que dados $P, Q \in \mathcal{P}(X)$

cualesquiera tales que $P \subseteq Q$ y $Q \subseteq P$, por la definición de igualdad entre conjuntos (ver Sección 10.3), tenemos que $P = Q$.

Ejemplo 15.3.8. La relación

$$\leq := \{(x, y) \in \mathbb{R} \times \mathbb{R} : x \text{ es menor o igual que } y\}$$

es antisimétrica (ver apéndice) puesto que dados $x, y \in \mathbb{R}$ si $x \leq y$ y $y \leq x$, entonces $x = y$ (¿por qué?).

Ejemplo 15.3.9. En $\mathbb{Z}^+$, la relación de *divisibilidad*

$$| := \{(m, n) \in \mathbb{Z}^+ \times \mathbb{Z}^+ : m \text{ divide a } n\}$$

es antisimétrica. En efecto, sean m y $n \in \mathbb{Z}^+$. Supongamos que $m \mid n$ y $n \mid m$. Esto significa que existen $k, l \in \mathbb{Z}$ tales que $n = m \cdot k$ y $m = n \cdot l$. Reemplazando $m = n \cdot l$ en la primera igualdad, y usando la asociatividad de la multiplicación en $\mathbb{Z}$, tenemos que $n = (n \cdot l) \cdot k = n \cdot (k \cdot l)$, por consiguiente $k \cdot l = 1$ (¿por qué?). Como m, n son enteros positivos, entonces $k = l = 1$ (¿por qué?). Por lo tanto, $m = n$, de donde concluimos que esta relación es antisimétrica.

Ejemplo 15.3.10. Dado $n \in \mathbb{Z}^+$, la relación $\equiv_n$ (Ejemplo 14.1.7) no es antisimétrica en general. Tomemos por ejemplo $n = 2$. Tenemos que $2 \equiv_2 6$ y $6 \equiv_2 2$ (¿por qué?), sin embargo $2 \neq 6$.

15.4. Relaciones transitivas

Imaginemos que Daniel confía en su amigo Juan, y que Juan confía en Ana; es probable que Daniel también sienta que puede confiar en Ana, incluso si no la conoce directamente. Esta idea de "transmitir" una relación a través de un intermediario ejemplifica lo que se conoce como *transitividad*.

Definición 15.4.1. Una relación $\mathcal{R}$ en A se dice *transitiva* si para cualesquiera $x, y, z \in A$, si $x\mathcal{R}y$ y $y\mathcal{R}z$ entonces $x\mathcal{R}z$.

Observación 15.4.2. Una relación $\mathcal{R}$ en A *no* es *transitiva* en A si y solo si existen $x, y, z \in A$ tales que $x\mathcal{R}y$ y $y\mathcal{R}z$ pero $x\not\mathcal{R}z$.

Continuamos refiriéndonos a las relaciones que se presentaron en los Ejemplos 14.1.2, 14.1.3, 14.1.4, 14.1.5, 14.1.6, 14.1.7 y 14.2.2.

Ejemplo 15.4.3. La relación vacía $\mathscr{R} := \varnothing$ como relación en A –sin importar si $A = \varnothing$ o $A \neq \varnothing$– es transitiva (¿por qué?).

Ejemplo 15.4.4. La relación $\subseteq$ del Ejemplo 14.1.4 *ser subconjunto de* en $\mathscr{P}(X)$ es una relación transitiva. Sean $P, Q, R \in \mathscr{P}(X)$ cualesquiera tales que $P \subseteq Q$ y $Q \subseteq R$. Por la parte 3 de la Proposición 10.2.5 concluímos que $P \subseteq R$.

Ejemplo 15.4.5. La relación diagonal respecto al conjunto A del Ejemplo 14.2.2, Δ_A, es transitiva en A. En efecto, sean $a, b, c \in A$ tales que $(a, b), (b, c) \in \Delta_A$. Por la definición de Δ_A tenemos que $a = b$ y $b = c$, por lo tanto, $a = c$, es decir $(a, c) \in \Delta_A$.

Ejemplo 15.4.6. El *orden usual de los números reales* es transitiva en $\mathbb{R}$ (ver apéndice). Dados $x, y, z \in \mathbb{R}$, si $x \leq y$ y $y \leq z$ entonces $x \leq z$.

Ejemplo 15.4.7. La relación de divisibilidad en $\mathbb{Z}^+$ definida en el Ejemplo 14.1.6 es transitiva. Esto se sigue de la Proposición 6.4.8.

Ejemplo 15.4.8. Dado $n \in \mathbb{Z}^+$, la relación congruencia módulo n en $\mathbb{Z}$ (Ejemplo 14.1.7) es transitiva tal y como se vió en la parte 3 de la Proposición 14.8.4.

15.5. Ejercicios

Ejercicio 15.5.1. Sean X un conjunto y $\mathscr{R}$ una relación en X.

1. Suponga que $\mathscr{R}$ es reflexiva. Pruebe que $\bigcup_{x \in X} [x] = X$.
2. Suponga que $\mathscr{R}$ es simétrica. Pruebe que $x \in [y]$ si y solo si $y \in [x]$, para cualesquiera $x, y \in X$.
3. Suponga que $\mathscr{R}$ es transitiva. Pruebe que si $x\mathscr{R}y$, entonces $[y] \subseteq [x]$, para cualesquiera $x, y \in X$.

Ejercicio 15.5.2. Sean $\mathscr{R}$ y $\mathscr{S}$ dos relaciones reflexivas en un conjunto A. Para cada una de las siguientes afirmaciones diga si es verdadera o falsa. Si es verdadera, demuéstrela. Si es falsa, dé un contraejemplo.

1. $\mathcal{R} \cap \mathcal{S}$ es también una relación reflexiva en A.

2. $\mathcal{R} \cup \mathcal{S}$ es también una relación reflexiva en A.

Ejercicio 15.5.3. Sean $\mathcal{R}$ y $\mathcal{S}$ dos relaciones en A simétricas (resp. antisimétricas, transitivas). Para cada una de las siguientes afirmaciones diga si es verdadera o falsa. Si es verdadera, demuéstrela. Si es falsa, dé un contraejemplo.

1. $\mathcal{R} \cap \mathcal{S}$ es una relación simétrica (resp. antisimétrica, transitiva) en A.

2. $\mathcal{R} \cup \mathcal{S}$ es una relación simétrica (resp. antisimétrica, transitiva) en A.

Lección

dieciséis

Relaciones de equivalencia

En matemáticas (y también en la vida real), a veces podemos identificar elementos de un conjunto (no vacío) A como si fueran el mismo aunque sean diferentes (por ejemplo, si nos piden escoger alguien de un país en particular, daría lo mismo escoger al Papa Francisco o a Mercedes Sosa porque ambos son de Argentina). Adicionalmente, también comparamos elementos (por ejemplo, en una empresa podemos comparar en un organigrama la jerarquía dentro de ella). Para poder hacer esto bien desde las matemáticas, tenemos que aislar algunas propiedades básicas que estudiaremos en esta lección.

16.1. ¿Qué es una relación de equivalencia?

Definición 16.1.1. Sea A un conjunto y sea $\mathcal{R}$ una relación en A. Se dice que $\mathcal{R}$ es una *relación de equivalencia* en A cuando ella es reflexiva en A, simétrica y transitiva. En general denotaremos una relación de equivalencia por $\sim$.

Ejemplo 16.1.2. La relación $\varnothing$, ver Ejemplo 14.1.2, es reflexiva en $A = \varnothing$ (Ejemplo 15.1.3), simétrica (Ejemplo 15.2.3) y transitiva (Ejemplo 15.4.3). Por lo tanto, la relación $\varnothing$ es de equivalencia en $A = \varnothing$.

Ejemplo 16.1.3. Dado un conjunto $A \neq \varnothing$, Δ_A es reflexiva en A (Ejemplo 15.1.6), simétrica (Ejemplo 15.2.6) y transitiva (Ejemplo 15.4.5), por lo tanto, Δ_A es una relación de equivalencia en A.

Ejemplo 16.1.4. Dado $n \in \mathbb{Z}^+$, la relación de congruencia módulo n en los enteros ($\equiv_n$) ver Ejemplo 14.1.7, es reflexiva en $\mathbb{Z}$ (Ejemplo 15.1.9), simétrica (Ejemplo 15.2.9) y transitiva (Ejemplo 15.4.8), por lo tanto, es una relación de equivalencia en $\mathbb{Z}$.

Ejemplo 16.1.5. Otros ejemplos de relaciones de equivalencia son los siguientes: la igualdad en el conjunto de los números reales $\mathbb{R}$, es decir $\Delta_{\mathbb{R}}$, la relación de semejanza de triángulos en el conjunto de todos los triángulos del plano, la relación entre personas dada por haber nacido en la misma fecha del año.

16.2. Caracterización de clases de equivalencia

El siguiente teorema es una generalización del Teorema 14.9.1.

Teorema 16.2.1. *Sean A un conjunto no vacío, $\sim$ una relación de equivalencia en A y $x, y \in A$ cualesquiera.*

1. *Si $x \sim y$, entonces $[x] = [y]$.*
2. *Si $x \nsim y$, entonces, $[x] \cap [y] = \emptyset$.*
3. *$\bigcup_{x \in A}[x] = A$.*

Demostración. Las demostraciones de 1 y 2 son muy similares a las demostraciones de 1 y 2 del Teorema 14.9.1 en las que se usa principalmente que la relación es simétrica y transitiva (ejercicio para el lector).

Por definición de las clases sabemos que $[x] \subseteq A$ para todo $x \in A$, lo cual implica que $\bigcup_{x \in A}[x] \subseteq A$ (Proposición 12.4.1 parte 4).

Sea $a \in A$ cualquiera. Como $\sim$ es reflexiva en A se tiene que $a \sim a$, por lo tanto, $a \in [a] \subseteq \bigcup_{x \in A}[x]$ (Proposición 12.4.1 parte 3); es decir, $A \subseteq \bigcup_{x \in A}[x]$. Como $\bigcup_{x \in A}[x] \subseteq A$ y $A \subseteq \bigcup_{x \in A}[x]$, podemos concluir 3 (definición de igualdad entre conjuntos). ☑

Observación 16.2.2. Nótese que la reflexividad, la simetría y la transitividad de $\sim$ fueron propiedades claves en las demostraciones del teorema anterior. También es importante resaltar que en una relación de equivalencia muchas clases pueden coincidir a pesar que provengan de elementos diferentes. Por ejemplo, recordemos que en el caso de la relación de congruencia módulo n, la clase de un entero k coincide con la clase del residuo r resultante al dividir k entre n. De esta manera, para tomar toda la unión $\bigcup_{x \in \mathbb{Z}}[x]$ no es necesario hacer la unión de todas las clases $[x]$ ($x \in \mathbb{Z}$) sino que es apenas suficiente unir las clases $[0], \cdots, [n-1]$ (Teorema 14.9.1 parte 3), por lo que tomar la unión $\bigcup_{x \in A}[x]$ sobre todos los elementos $x \in A$ se vuelve redundante en muchos de los ejemplos de relaciones de equivalencia (no en todas, por ejemplo en la relación diagonal Δ_A, con $A \neq \emptyset$, tenemos que unir *todas* las clases de equivalencia para obtener a A, ¿por qué?).

Corolario 16.2.3. *Sean A un conjunto no vacío, $\sim$ una relación de equivalencia en A y $x, y \in A$ cualesquiera. Entonces, $[x] = [y]$ si y solo si $x \sim y$.*

Este resultado es consecuencia inmediata de 1 y 2 del Teorema 16.2.1.

Demostración. Sean $x, y \in A$ cualesquiera. Supongamos que $[x] = [y]$. Como $x \in [x]$ (puesto que $\sim$ es reflexiva en A), entonces $[x] \cap [y] \neq \emptyset$ (¿por qué?), y por el contrarrecíproco del Teorema 16.2.1 parte 2, tenemos que $x \sim y$. El recíproco es exactamente el Teorema 16.2.1 parte 1. ☑

En la lección anterior, para cada $n \in \mathbb{Z}^+$ se definió el conjunto $\mathbb{Z}_n$ conformado por todas las clases con respecto a la relación congruencia módulo n. Definimos a continuación los conjuntos análogos a estos para relaciones de equivalencia arbitrarias.

Definición 16.2.4. Sean A un conjunto y $\sim$ una relación de equivalencia en A. El *conjunto cociente* de A con respecto a $\sim$, que denotaremos por $A/\sim$, es el conjunto definido como sigue a continuación:

$$A/\sim = \{[x] : x \in A\}.$$

Formalmente,

$$A/\sim = \{Y \in \mathcal{P}(A) : \text{ existe } x \in A \text{ tal que } Y = [x]\}.$$

La familia $A/\sim$ está conformada por todas las clases de A con respecto a $\sim$. Debe tenerse en cuenta que en el conjunto $A/\sim$ pueden haber elementos repetidos $[x] = [y]$ incluso si $x \neq y$, lo cual ocurre cuando $x \sim y$ ($x, y \in A$). Así, cada clase puede tener varios nombres pero aparece una única vez en la colección $A/\sim$.

Ejemplo 16.2.5. Sea A el conjunto de todas las personas y sea $\sim$ la relación en A definida por: $x \sim y$ si y solo si x y y cumplen años el mismo día. Observemos que $\sim$ es una relación de equivalencia en A. Si la persona x cumple años el 5 de julio, entonces la clase de equivalencia de x es el conjunto de todas las personas que cumplen años el 5 de julio. Como cada elemento de $A/\sim$ es así mismo un conjunto, los elementos del conjunto cociente son los siguientes: el conjunto formado por todas las personas que cumplen años el 1^o de enero, otro elemento es el conjunto conformado por las personas que cumplen años el 2 de enero, etcétera. Aunque hay miles de millones de personas en A, hay apenas 366 clases según la relación $\sim$ (es decir, elementos de $A/\sim$) porque hay 366 fechas distintas en que las personas cumplen años.

16.3. Particiones

Como siempre, pensemos en un ejemplo coloquial a manera de motivación para introducir el concepto de partición. Tomando A como el conjunto de los seres humanos, pensemos en la siguiente relación: la persona X se relaciona con la persona Y si y solo si X y Y nacieron en el mismo país (no pensemos en términos de nacionalidad porque una misma persona puede tener múltiples nacionalidades, pero tampoco pensemos en la posibilidad de que alguien haya nacido exactamente en la frontera de dos países en cuyo caso tomemos el país de nacimiento como el lugar donde fue registrado su nacimiento). De esta manera, Marco Coll (el jugador de fútbol famoso por ser el único jugador en anotar un gol olímpico en una Copa del Mundo de fútbol) y Rodolfo Llinás (neurocirujano reconocido por sus estudios sobre el cerebro) están relacionados porque ambos nacieron en Colombia. Bernard Bolzano (matemático conocido por su demostración de una de las formas equivalentes del *Teorema del valor intermedio* que se estudia en Cálculo Diferencial) y Kurt Gödel (renombrado lógico reconocido por su famoso *Teorema de incompletitud* que enuncia que axiomatizaciones razonables de la aritmética de los números naturales –e.g., la aritmética de Peano– no alcanzan a demostrar propiedades aritméticas que son verdaderas en los números naturales) están relacionados porque ambos nacieron en ciudades que actualmente pertenecen a República Checa (Praga y Brno, respectivamente, aunque en su momento Praga era parte del Reino de Bohemia y Brno era parte del Imperio Austrohúngaro, pero no nos compliquemos la vida por ahora).

Nótese que cada clase de equivalencia corresponde a *partir* el conjunto de seres humanos en grupos dependiendo del país donde haya nacido cada uno. Un mapamundi es una representación de esta partición.

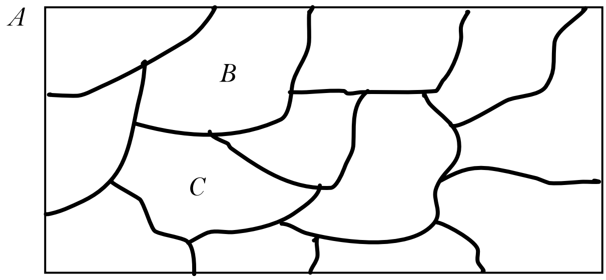
Supongamos que tenemos un conjunto cociente $A/\sim$. Del Teorema 16.2.1 sabemos que cualesquiera dos clases de equivalencia distintas de $A/\sim$ son disyuntas y que la unión de todas las clases de equivalencia es el conjunto original A. Teniendo en cuenta esto, podemos imaginar que $A/\sim$ determina una ruptura del conjunto A en subconjuntos disyuntos. La siguiente definición generaliza este comportamiento que hemos analizado en los ejemplos anteriores.

Definición 16.3.1. Sea A un conjunto no vacío. Una *partición* de A es una familia $\mathscr{P}$ de subconjuntos no vacíos de A tal que

i. Si $B, C \in \mathscr{P}$ y $B \neq C$, entonces, $B \cap C = \varnothing$ ($\mathscr{P}$ es una familia de conjuntos *disyuntos dos a dos*; es decir, cualquier par de conjuntos de $\mathscr{A}$ distintos, son disyuntos)

ii. $\bigcup_{B \in \mathscr{P}} B = A$.

La siguiente es una representación de una partición de un conjunto no vacío A.



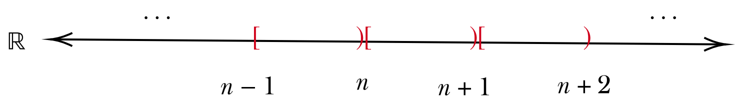
Podemos pensar al conjunto A como si fuera una bandeja de porcelana. Si se “quiebra” dicho conjunto, cada una de las piezas en que se ha “roto” es disyunta de las demás. Pero si “pegamos” todas las piezas en que se ha roto nuestra “bandeja”, obtenemos nuevamente a nuestro conjunto A. Esta es una motivación informal del porqué llamamos de esta manera a las *particiones*.

Ejemplo 16.3.2.

1. Sea P el conjunto de todos los números enteros pares e I el conjunto de todos los enteros impares. Entonces, $\mathscr{P} = \{P, I\}$ es una partición de $\mathbb{Z}$.

2. La familia $\mathscr{P} = \{\mathbb{Z}^-, \{0\}, \mathbb{Z}^+\}$ es otra partición de los números enteros $\mathbb{Z}$.

3. $\mathscr{P} = \{[n, n+1) \ : \ n \in \mathbb{Z}\}$ es una partición de los números reales $\mathbb{R}$.



La siguiente afirmación es una consecuencia inmediata del Teorema 16.2.1.

Corolario 16.3.3. *Sea A un conjunto y $\sim$ una relación de equivalencia en A. Entonces, $A/\sim$ es una partición de A.*

El anterior colorario es llamado por algunos autores (por ejemplo, [1]) *Teorema fundamental de las relaciones de equivalencia*.

Por otro lado, una partición $\mathscr{P}$ de un conjunto no vacío A nos determina una relación de equivalencia $\mathscr{R}_{\mathscr{P}}$ en A, como veremos a continuación.

Proposición 16.3.4. *Sea $A \neq \varnothing$ un conjunto y $\mathscr{P}$ una partición de A. La relación*

$$\mathscr{R}_{\mathscr{P}} := \{(a, b) \in A \times A : \textit{existe } B \in \mathscr{P} \textit{ tal que } a \in B \textit{ y } b \in B\}$$

es una relación de equivalencia en A.

Demostración. Sea $A \neq \varnothing$ un conjunto y $\mathscr{P}$ una partición de A. Veamos que $\mathscr{R}_{\mathscr{P}}$ es una relación de equivalencia en A.

Reflexividad en A: sea $a \in A$ cualquiera. Como $\mathscr{P}$ es una partición en A, entonces $\bigcup_{B\in\mathscr{P}} B = A$, luego existe $B \in \mathscr{P}$ tal que $a \in B$; como $a \in B$ y $a \in B$ (valga la redundancia de esta afirmación), por la definición de $\mathscr{R}_{\mathscr{P}}$ tenemos que, $a\mathscr{R}_{\mathscr{P}}a$.

Simetría: sean $a, b \in A$ arbitrarios tales que $a\mathscr{R}_{\mathscr{P}}b$. Por definición de $\mathscr{R}_{\mathscr{P}}$ existe $B \in \mathscr{P}$ tal que $a \in B$ y $b \in B$, por lo tanto, $b \in B$ y $a \in B$ (¿por qué?) y así por la definición de $\mathscr{R}_{\mathscr{P}}$ tenemos que $b\mathscr{R}_{\mathscr{P}}a$.

Transitividad: sean $a, b, c \in A$ cualesquiera tales que $a\mathscr{R}_{\mathscr{P}}b$ y $b\mathscr{R}_{\mathscr{P}}c$. Luego, existen $B, C \in \mathscr{P}$ tales que $a, b \in B$ y $b, c \in C$. En particular, tenemos que $b \in B$ y $b \in C$ por lo que $B \cap C \neq \varnothing$. Como $\mathscr{P}$ es una partición de A y $B \cap C \neq \varnothing$, entonces $B = C$. Por lo tanto, $a, c \in B = C$, por lo que $a\mathscr{R}_{\mathscr{P}}c$.
Puesto que $\mathscr{R}_{\mathscr{P}}$ es reflexiva en A, simétrica y transitiva, entonces $\mathscr{R}_{\mathscr{P}}$ es una relación de equivalencia. ☑

Dada $\sim$ una relación de equivalencia en A, por el Colorario 16.3.3 tenemos que $\mathscr{P} := A/\sim$ es una partición de A. De lo anterior, tenemos que $\mathscr{R}_{A/\sim}$ es una relación de equivalencia en A. Una pregunta natural es cómo están relacionadas $\sim$ y $\mathscr{R}_{A/\sim}$. No es de sorprender que, por lo estudiando en esta lección, $\sim$ y $\mathscr{R}_{A/\sim}$ son exactamente la misma relación (ejercicio –demostrar esta afirmación vía doble contenencia entre conjuntos, Definición 14.4.5–).

16.4. Ejercicios

Ejercicio 16.4.1. ¿Cuáles de las siguientes familias de subconjuntos de $\mathbb{R}$ son particiones de $[0, +\infty)$?

1. $\mathscr{A} = \{\{a\}\}_{a\in[0,+\infty)}$.
2. $\mathscr{B} = \{(n-1, n]\}_{n\in\mathbb{Z}^+}$.

3. $\mathscr{C} = \{[n-1, n)\}_{n\in\mathbb{Z}^+}$.
4. $\mathscr{D} = \{[0, x)\}_{x\in[0,+\infty)}$.
5. $\mathscr{E} = \{[x-1, x)\}_{x\in[0,+\infty)}$.
6. $\mathscr{F} = \{[2^n, 2^{n+1})\}_{n\in\mathbb{Z}}$.

Ejercicio 16.4.2. Para cada una de las siguientes relaciones de equivalencia describa la correspondiente partición.

1. Sea P el conjunto de todas las personas y sea $\sim$ la relación de equivalencia en P definida así: dados a, b elementos de P, $a \sim b$ si y solo si a y b tienen la misma madre biológica.
2. Sea $\simeq$ la relación en $\mathbb{R}$ definida por $x \simeq y$ si y solo si $|x| = |y|$ para cualesquiera $x, y \in \mathbb{R}$.

Ejercicio 16.4.3. Para cada una de las siguientes relaciones de equivalencia presentar una descripción geométrica de las correspondientes clases de equivalencia.

1. Sea $\approx$ la relación en $\mathbb{R}^2$ definida por $(a, b) \approx (c, d)$ si y solo si $a^2 + b^2 = c^2 + d^2$, para cualesquiera $(a, b), (c, d) \in \mathbb{R}^2$.
2. Sea $\asymp$ la relación en $\mathbb{R}^2$ definida por $(a, b) \asymp (c, d)$ si y solo si $\sqrt[3]{a^3 + b^3} = \sqrt[3]{c^3 + d^3}$, para cualesquiera $(a, b), (c, d) \in \mathbb{R}^2$.

Ejercicio 16.4.4. Para cada una de las siguientes particiones describa la correspondiente relación de equivalencia.

1. Sea $\mathscr{A}$ la partición del conjunto $\{a, e, i, o, u\}$ dada por $\mathscr{A} = \{\{a, e, o\}, \{i, u\}\}$.
2. Sea $\mathbb{Q}$ la partición de $\mathbb{R} - \{0\}$ dada por $\mathbb{Q} = \{Q_n\}_{n\in\mathbb{Z}}$ donde $Q_n = \{x \in \mathbb{R} : 1 \leq |x/2^n| < 2\}$.

Ejercicio 16.4.5. Sean $\mathscr{R}$ y $\mathscr{S}$ dos relaciones de equivalencia en un conjunto A. Para cada una de las siguientes afirmaciones diga si es verdadera o falsa. Si es verdadera, demuéstrela. Si es falsa, dé un contraejemplo.

1. $\mathscr{R} \cap \mathscr{S}$ es también una relación de equivalencia en A.

2. $\mathscr{R} \cup \mathscr{S}$ es también una relación de equivalencia en A.

Ejercicio 16.4.6. Sean $X = \{a, e, i, o, u\}$ y $\mathscr{R}$ una relación de equivalencia en X. Suponga que $\mathscr{R}$ tiene tres clases de equivalencia y que $e\mathscr{R}i$ y $u\mathscr{R}o$. Liste todos los elementos de $\mathscr{R}$. Haga un gráfico de $\mathscr{R}$.

Lección

diecisiete

Relaciones de orden

En la lección anterior estudiamos un tipo especial de relaciones llamadas *de equivalencia*, en los cuales identificábamos elementos que, aunque podrían ser diferentes, eran vistos como si fueran el mismo. En esta lección, abordaremos otro tipo especial de relaciones que nos permite organizar los elementos de un conjunto no vacío.

Estamos acostumbrados a organizar cosas de acuerdo con ciertos criterios: ordenamos números de menor a mayor, organizamos tareas según su prioridad, o clasificamos objetos según tamaño o preferencia. Esta idea de "colocar en orden" es la que subyace bajo el concepto que estudiamos en esta lección.

Por ejemplo, una noción básica que aprendemos desde la primaria es el orden en los números naturales. Decimos que un número natural n es *menor o igual* que otro número natural m si y solo si existe un número natural k tal que $n + k = m$.

17.1. Conjuntos ordenados

Un conjunto ordenado es un conjunto en el cual se ha definido una relación de orden que proporciona un sentido de secuencia o jerarquía entre sus elementos.

Definición 17.1.1. Sea X cualquier conjunto. Una relación $\mathscr{R}$ en X se dice *de orden* en X cuando es reflexiva en X, antisimétrica y transitiva. Usaremos el símbolo $\preccurlyeq$ en lugar de $\mathscr{R}$ para denotar las relaciones de orden. El par $(X, \preccurlyeq)$ será llamado *conjunto parcialmente ordenado*, o simplemente *conjunto ordenado*.

Observación 17.1.2. Una referencia muy frecuente en inglés para estas estructuras es *poset* (*Partially Order SET*), pero no la recomendamos por evitar anglicismos en la referencia de los nombres de definiciones matemáticas (simplemente la mencionamos para que los estudiantes puedan encontrar este término en la literatura que hay en inglés).

Definición 17.1.3. Sea X cualquier conjunto. Una relación ($\preccurlyeq$ en X se dice un *orden total* si y solo si $\preccurlyeq$ es una relación de orden en X, y si para cada $a, b \in X$, al menos una de las siguientes afirmaciones se tiene: $a \preccurlyeq b$ o $b \preccurlyeq a$. El par $(X, \preccurlyeq)$ será llamado *conjunto totalmente ordenado*.

Un conjunto ordenado es un par $(X, \preccurlyeq)$; sin embargo, cuando la relación $\preccurlyeq$ es sobreentendida del contexto o no es importante designar el símbolo para la relación, simplemente diremos que X es un conjunto ordenado. De manera similar para los conjuntos totalmente ordenados. Nótese que de las definiciones anteriores observamos que todo conjunto totalmente ordenado es en particular un conjunto ordenado.

Ejemplo 17.1.4. Hay muchas relaciones que son reflexivas y transitivas que no son antisimétricas. En particular, cualquier relación de equivalencia en un conjunto que tiene elementos distintos relacionados no puede ser antisimétrica. Por ejemplo, la relación de congruencia módulo n para cualquier $n \in \mathbb{Z}^+$ con $n \neq 1$ (Ejemplo 14.1.7) es reflexiva en $\mathbb{Z}$ (Ejemplo 15.1.9) y transitiva (Ejemplo 15.4.8) pero no antisimétrica (en el Ejemplo 15.3.10 se analizó el caso $n = 2$, como ejercicio argumente qué ocurre para $n > 2$). Como ejercicio, demuestre esta afirmación para cualquier relación de equivalencia en un conjunto que tenga al menos un par de elementos diferentes que estén relacionados.

Ejemplo 17.1.5. Cada uno de los conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ con la relación de orden usual en esos sistemas numéricos es un conjunto totalmente ordenado.

Ejemplo 17.1.6. Sea X un conjunto. Entonces $(\mathscr{P}(X), \subseteq)$ es un conjunto ordenado: es reflexiva en X (Ejemplo 15.1.5), antisimétrica (Ejemplo 15.3.7) y transitiva (Ejemplo 15.4.4).

Ejemplo 17.1.7. La relación de divisibilidad en $\mathbb{Z}^+$ (Definición 14.1.6), es reflexiva en $\mathbb{Z}^+$ (Ejemplo 15.1.8), antisimétrica (Ejemplo 15.3.9) y transitiva (Ejemplo 15.4.7). Por lo tanto, $(\mathbb{Z}^+, \mid)$ es un conjunto ordenado pero no es un conjunto totalmente ordenado porque por ejemplo, $2 \nmid 3$ y $3 \nmid 2$ (¿por qué?).

17.2. Diagramas de Hasse

Los diagramas de Hasse corresponden a una manera *minimalista* de representar gráficamente un conjunto ordenado. La idea es representar mediante puntos y conexiones entre estos colocando la menor cantidad de datos posible que nos dé toda la información relativa al orden considerado.

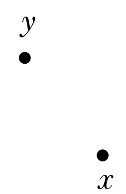
Definición 17.2.1. Sea $(X, \preccurlyeq)$ un conjunto ordenado y sean $a, b \in X$. El elemento b *cubre* al elemento a si $a \preccurlyeq b$ y $a \neq b$ y no existe $c \in X$ tal que $a \preccurlyeq c \preccurlyeq b$ con $a \neq c$ y $c \neq b$.

Ejemplo 17.2.2. Tomemos el conjunto ordenado $(\mathscr{P}(X), \subseteq)$ con $X := \{0, 1, 2\}$. Nótese que $A := \{0\} \subsetneq \{0, 1\} =: B$ (¿por qué?). Si existiera $C \in \mathscr{P}(X)$ tal que $A \subsetneq C \subsetneq B$, $A \subsetneq C$ diría que existiría $x \in C$ tal que $x \notin A$, es decir $x \neq 0$ (puesto que $A := \{0\}$). Puesto que en particular $C \subseteq B := \{0, 1\}$, $x \in C$ y $x \neq 0$, entonces $x = 1$; por lo tanto, $1 \in C$. Como en particular $\{0\} =: A \subseteq C$, entonces $0 \in C$. De esta manera, $B := \{0, 1\} \subseteq C$ (¿por qué?). Como $C \subseteq B$ y $B \subseteq C$, por la definición de igualdad entre conjuntos tenemos que $B = C$ (contradice el hecho de que $C \subsetneq B$). Por lo tanto, B cubre a A.

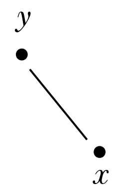
Ejemplo 17.2.3. Tomemos el conjunto ordenado $(\mathbb{R}, \leq_{usual})$. Vemos que a pesar de que $x, y \in \mathbb{R}$ satisfagan $x \leq y$ y $x \neq y$, y no cubre a x puesto que si tomamos $z := \frac{x+y}{2}$, vemos que $x \leq z \leq y$ pero $x \neq z$ y $z \neq y$.

Para graficar el diagrama de Hasse de un conjunto ordenado finito $(X, \preccurlyeq)$ $(X \neq \emptyset)$, procedemos de la siguiente manera:

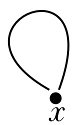
1. Representamos a cada elemento de X por un punto de tal manera que, dados $x, y \in X$, si $x \preccurlyeq y$, con $x \neq y$, entonces el punto que representa a y lo ubicamos más alto que el punto que representa a x.



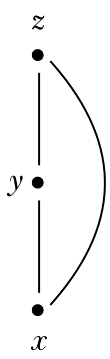
2. Trazamos una línea que una los puntos que representan a dos elementos en X en caso de que uno de esos puntos cubra al otro.



¿Por qué esto es suficiente? Si quisiéramos trazar una línea entre dos elementos $x, y \in X$ en el caso de que $x \preccurlyeq y$, debido a la reflexividad de $\preccurlyeq$ siempre deberíamos dibujar una línea entre cualquier punto y él mismo, lo cual saturaría el gráfico. Como a priori estamos suponiendo que $\preccurlyeq$ es reflexiva en X, estos bucles son redundantes.

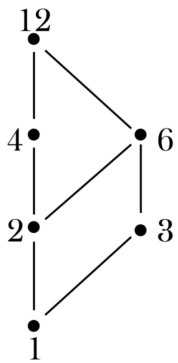


Adicionalmente, si trazáramos siempre una línea cada vez que $x \preccurlyeq y$, en caso de que también tuviéramos $y \preccurlyeq z$ tendríamos la siguiente situación:



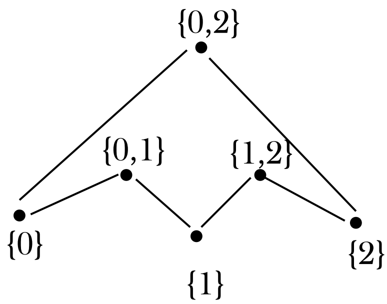
Suponiendo que todos estos elementos sean diferentes, observamos que z no cubre a x puesto que tendríamos a y en el medio. En el caso de que z cubra a y y que y cubra a x, basta dibujar una línea entre x y y y otra entre y y z. La línea entre x y z no sería necesaria, puesto que a priori estamos suponiendo que $\preccurlyeq$ es transitiva, de manera que podemos ir desde el punto x al punto z pasando a través de y. Así, la línea entre x y z sería redundante.

Ejemplo 17.2.4. Considere $A = \{n \in \mathbb{Z}^+ : n \text{ es divisor de } 12\}$ con la relación de orden $|$ (divisibilidad, Ejemplo 14.1.6). El diagrama de Hasse de este conjunto ordenado es el siguiente:



Vemos por ejemplo que como 1 divide a cualquier entero, en particular a cualquier elemento en A, luego el punto que lo representa está bien abajo en nuestro diagrama de Hasse. Un nivel más arriba tenemos los puntos que representan a 2 y a 3, que son números primos, donde trazamos una línea entre 1 y estos dos elementos, puesto que 2 y 3 cubren a 1 en este conjunto. Observe también que $2 \nmid 3$ ni $3 \nmid 2$. Un nivel más arriba tenemos a 4 y a 6, donde 4 cubre a 2 y 6 cubre tanto a 2 como a 3. Por último, ubicamos a 12 bien arriba de nuestro diagrama, donde 12 cubre tanto a 4 como a 6. Notemos que pese a que 2 divide a 12, no trazamos una línea entre 2 y 12 puesto que hay un elemento diferente en el medio según este orden (4) por lo que 12 no cubre a 2, pero dado que hay al menos una forma de ir de 2 a 12 (pasando a través de 4), apelando a la transitividad de la divisibilidad podemos inferir que 2 se relaciona con 12 según esta gráfica. Fijémonos además en que no trazamos por ejemplo una línea entre 2 y 3 puesto que $2 \nmid 3$ y $3 \nmid 2$ (¿por qué? Argumente usando el Algoritmo de la división - Hecho 14.8.1).

Ejemplo 17.2.5. Considere el conjunto $X := \{0, 1, 2\}$ y el conjunto ordenado $(A, \subseteq)$ donde $A := \mathcal{P}(X) \setminus \{X, \varnothing\}$.



Notemos por ejemplo que colocamos una línea entre $\{1\}$ y $\{0, 1\}$ puesto que $\{1\} \subseteq \{0, 1\}$ y además $\{0, 1\}$ cubre a $\{1\}$ (podemos dar un argumento similar al hecho en el Ejemplo 17.2.2). Las demás líneas las pueden ser justificadas de manera análoga (ejercicio para el lector).

17.3. Ejercicios

Ejercicio 17.3.1. Dado un conjunto $A \neq \varnothing$, decimos que $\prec$ es una relación *estricta de orden* si y solo si se satisfacen las siguientes condiciones:

1. $\prec$ es *irreflexiva* en A; es decir, para todo $a \in A$ tenemos que $a \nprec a$.
2. $\prec$ es transitiva.

En este caso, decimos que $(A, \prec)$ es un *conjunto ordenado estrictamente*. Dada $\preccurlyeq$ una relación en A y definiendo $\prec := \preccurlyeq \setminus \Delta_A$, demuestre que $(A, \preccurlyeq)$ es un conjunto ordenado si y solo si $(A, \prec)$ es un conjunto ordenado estrictamente.

Ejercicio 17.3.2. Demuestre o refute: si $(A, \preceq)$ es un conjunto ordenado, entonces $(A, \succeq)$ también es un conjunto ordenado, donde $\succeq := \{(x, y) \in A \times A : y \preceq x\}$.

Ejercicio 17.3.3. Dado $A := \{1, 2, 3, 4, 5, 6\}$, defina una relación de orden en A. Represente el conjunto ordenado obtenido mediante un diagrama de Hasse.

Ejercicio 17.3.4. Considere el conjunto $A := \{n \in \mathbb{N} : 0 \leq n \leq 20\}$. Realice el diagrama de Hasse del conjunto ordenado $(A, \mid)$.

Ejercicio 17.3.5. Considere el conjunto $A := \{1, 2, 3, 4\}$. Realice el diagrama de Hasse del conjunto ordenado $(\mathscr{P}(A), \subseteq)$.

Ejercicio 17.3.6. Dados $(A, \preccurlyeq_A)$ y $(B, \preccurlyeq_B)$ conjuntos ordenados, definimos las siguientes relaciones en $A \times B$:

1. $(a, b) \preccurlyeq_{prod} (a', b')$ si y solo si $a \preccurlyeq_A a'$ y $b \preccurlyeq_B b'$.
2. $(a, b) \preccurlyeq_{lex} (a', b')$ si y solo si se da uno de los siguientes casos:
   i) $a \preccurlyeq_A a'$ y $a \neq a'$ o
   ii) $a = a'$ y $b \preccurlyeq_B b'$.

Demuestre que $\preccurlyeq_{prod}$ y $\preccurlyeq_{lex}$ son relaciones de orden en $A \times B$, los cuales son denominados *orden producto* y *orden lexicográfico* respectivamente.

Lección

dieciocho

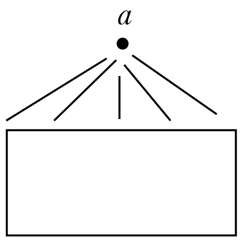
Elementos extremales. Buenos órdenes

Los elementos extremales de un conjunto ordenado son cruciales porque nos permiten identificar puntos claves en la estructura de los conjuntos y nos brindan información sobre el comportamiento y la organización de sus elementos.

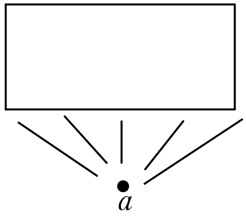
18.1. Máximos y mínimos

Cuando trabajamos con conjuntos, dotados de una relación de orden, podemos identificar ciertos elementos que ocupan posiciones extremas dentro de ese conjunto. Algunos de estos elementos son aquellos que están por debajo de todos o están por encima de todos los otros elementos bajo la relación de orden dada.

Definición 18.1.1. Sean $(A, \preccurlyeq)$ un conjunto ordenado y $a \in A$. Un elemento $a \in A$ se dice un *máximo* o un *mayor* elemento de A cuando $x \preccurlyeq a$ para todo $x \in A$.



Un elemento $a \in A$ se dice un *mínimo* o un *menor* elemento de A cuando $a \preccurlyeq x$ para todo $x \in A$.



Observación 18.1.2. En un conjunto ordenado $(A, \preccurlyeq)$, un elemento $a \in A$ *no* es *máximo* de A si existe un elemento $x \in A$ tal que $x \not\preccurlyeq a$. En un conjunto ordenado $(A, \preccurlyeq)$, un elemento $a \in A$ *no* es *mínimo* de A si existe un elemento $x \in A$ tal que $a \not\preccurlyeq x$.

Recordemos que $a \not\preccurlyeq x$ *no* quiere decir en general que $x \preccurlyeq a$ (lo cual solo ocurre en un orden total), pues por ejemplo en el conjunto ordenado $(\mathscr{P}(X), \subseteq)$ con $X := \{0, 1, 2\}$ tenemos que $\{0, 1\} \not\subseteq \{0, 2\}$ pero $\{0, 2\} \not\subseteq \{0, 1\}$ (¿por qué?).

Ejemplo 18.1.3. El conjunto ordenado $(\mathbb{Z}, \leq)$ no tiene máximo ni mínimo. Tomemos por ejemplo cualquier entero m, vemos que al considerar $x := m + 1$ tenemos que $x := m + 1 \not\leq m$, por lo tanto, m no puede ser máximo de $\mathbb{Z}$ de acuerdo el orden usual $\leq$. Tampoco m es mínimo de $\mathbb{Z}$ puesto que al tomar $x := m - 1$ notamos que $m \not\leq m - 1 =: x$.

Ejemplo 18.1.4. Tomemos el conjunto ordenado $(A, \subseteq)$ con $A := \mathscr{P}(X) \setminus \{\varnothing, X\}$ ($X := \{0, 1, 2\}$, Ejemplo 17.2.5). Observemos que $\{0\}$ no es mínimo de este conjunto ordenado puesto que $\{0\} \not\subseteq \{1\}$ (¿por qué?). Como ejercicio, demuestre que ningún otro elemento de este conjunto ordenado es mínimo. Por otro lado, vemos que $\{0, 2\}$ no es máximo de este conjunto ordenado puesto que $\{1\} \not\subseteq \{0, 2\}$ (¿por qué?). Como ejercicio, demuestre que ningún otro elemento de este conjunto ordenado es máximo.

Ejemplo 18.1.5. Considere el conjunto ordenado $(\mathscr{P}(X), \subseteq)$ en el que X es un conjunto arbitrario pero fijo. Observemos que dado cualquier conjunto $A \in \mathscr{P}(X)$, por definición de conjunto potencia (Definición 10.4.1), tenemos que $A \subseteq X$ y, como $X \in \mathscr{P}(X)$, entonces tenemos que X es máximo de este conjunto ordenado. Por otro lado, como para todo conjunto A se tiene que $\varnothing \subseteq A$ (Proposición 10.2.5 parte 1), en particular si tomamos $A \in \mathscr{P}(X)$ arbitrario, entonces $\varnothing$ es mínimo de $(\mathscr{P}(X), \subseteq)$ porque $\varnothing \in \mathscr{P}(X)$.

El siguiente teorema nos dice que si existe un elemento máximo en un conjunto, este es único. Análogamente, si existe un elemento mínimo en un conjunto, este es único. Este resultado nos permite precisar nuestro lenguaje en el momento de referirnos a estos elementos extremos de A pues no diremos apenas que a es un elemento máximo de A sino que diremos mas precisamente que a es EL máximo o EL mayor de A. De manera similar, no diremos apenas que b es un elemento mínimo de A sino que diremos mas precisamente que b es EL mínimo o EL menor de A.

Teorema 18.1.6. *Sea $(A, \preccurlyeq)$ un conjunto ordenado. Si $a \in A$ es un elemento máximo de A entonces a es único. Analogamente, si $b \in A$ es un elemento mínimo de A entonces b es único.*

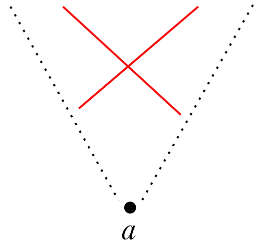
Demostración. Sean $a, \alpha \in A$ elementos máximos de A. Por definición de elemento máximo, $x \preccurlyeq a$ para todo $x \in A$, en particular, $\alpha \preccurlyeq a$. Del mismo modo, $x \preccurlyeq \alpha$ para todo $x \in A$, en particular, $a \preccurlyeq \alpha$. Por antisimetría se tiene que $\alpha = a$. Un argumento similar funciona para probar la segunda parte del teorema. Esto es dejado como ejercicio para el lector. ☑

Notación 18.1.7. Dado $(A, \preccurlyeq)$ un conjunto ordenado, como en el Teorema 18.1.6 hemos demostrado que de tener A máximo este es único, en caso de que tal máximo exista lo denotamos por $\max A$. Por otro lado, como en el Teorema 18.1.6 también hemos demostrado que de tener A mínimo este es único, en caso de que tal mínimo exista lo denotamos por $\min A$.

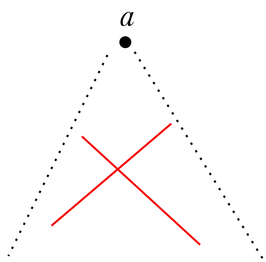
18.2. Maximales y minimales

Otros elementos extremales de un conjunto ordenado son aquellos para los cuales no hay nadie por encima de ellos o nadie por debajo de ellos.

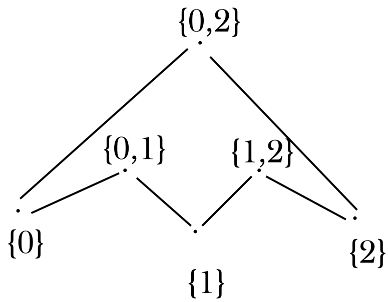
Definición 18.2.1. Sean $(A, \preccurlyeq)$ un conjunto ordenado y $a \in A$. El elemento a se dice un *maximal* de A cuando no existe $x \in A$ tal que $a \preccurlyeq x$ y $a \neq x$. En otras palabras, a es *maximal* si no hay nadie por encima de él según el orden $\preccurlyeq$ (en la representación de un diagrama de Hasse, como el mostrado a continuación, a es *maximal* si en la zona tachada con rojo *no* hay ningún elemento del conjunto ordenado).



El elemento a se dice un *minimal* de A cuando no existe $x \in A$ tal que $x \preccurlyeq a$ y $a \neq x$. En otras palabras, a es *minimal* si no hay nadie por debajo de él según el orden $\preccurlyeq$ (en la representación de un diagrama de Hasse dado como se sigue, a es *mimimal* si en la zona tachado con rojo *no* hay ningún elemento del conjunto ordenado).



Observación 18.2.2. En un conjunto ordenado $(A, \preccurlyeq)$, un elemento maximal $a \in A$ *no* necesariamente es máximo de A. Consideremos el Ejemplo 17.2.5. Veamos que $\{0, 1\}$ es un elemento maximal en $(A, \subseteq)$, donde $A := \mathscr{P}(X) \setminus \{\varnothing, X\}$ con $X := \{0, 1, 2\}$. Si existiera $B \in A$ tal que $\{0, 1\} \subsetneq B$, esto diría que existe $x \in B$ tal que $x \notin \{0, 1\}$, y puesto que $B \in \mathscr{P}(X) \setminus \{\varnothing, X\}$ en particular $B \in \mathscr{P}(X)$ (con $X := \{0, 1, 2\}$), por lo tanto, $x = 2$. Puesto que $\{0, 1\} \subseteq B$, entonces tenemos que $X := \{0, 1, 2\} \subseteq B$, luego $B = X$ (¿por qué?). Esto es una contradiccón puesto que $B \in \mathscr{P}(X) \setminus \{\varnothing, X\}$. Por lo tanto, $\{0, 1\}$ es maximal en $(A, \subseteq)$. En el Ejemplo 18.1.4 observamos que $\{0, 1\}$ *no* es máximo de $(A, \subseteq)$. Nótese que en el diagrama de Hasse de este conjunto ordenado, por encima de $\{0, 1\}$ no hay ningún elemento de A.



Análogamente, en general también tenemos que un elemento minimal $a \in A$ *no* necesariamente es mínimo de A. Por ejemplo, tenemos que $\{1\}$ es un elemento minimal en $(A, \subseteq)$, con $A := \mathscr{P}(X) \setminus \{\varnothing, X\}$ $(X := \{0, 1, 2\})$. Demostrar este hecho lo dejamos como ejercicio para el lector, donde tenemos que $\{1\}$ no es *mínimo* de $(A, \subseteq)$ (ver Ejemplo 18.1.4). Notemos que en el diagrama de Hasse de este conjunto ordenado, por debajo de $\{1\}$ no hay ningún elemento de A.

Por otro lado, observemos que el elemento $\{0, 2\}$ también es un elemento maximal en $(A, \leq)$ (ejercicio para el lector, de todas maneras notemos que en el diagrama de Hasse de este conjunto ordenado, no hay nadie por encima de $\{0, 2\}$). Esto demuestra que en general *no* tenemos *unicidad de maximales*. Adicionalmente, vemos que $\{0\}$ también es minimal en $(A, \leq)$ (ejercicio para el lector), por lo que esto también demuestra que en general *tampoco* tenemos *unicidad de minimales*.

Ejemplo 18.2.3. El conjunto ordenado $(\mathbb{Z}, \leq)$ no tiene elementos ni maximales ni minimales. En efecto, sea $m \in \mathbb{Z}$, como al tomar $x := m + 1$ tenemos que $m \leq m + 1$ y $m \neq m + 1$ entonces m *no* es maximal en $(\mathbb{Z}, \leq)$ puesto que hay alguien más en ese conjunto ordenado por encima de él. De manera dual, podemos ver que m tampoco es minimal en $(\mathbb{Z}, \leq)$ (ejercicio para el lector).

18.2.1. Cotas superiores e inferiores de un conjunto

Definición 18.2.4. Sean $(A, \preccurlyeq)$ un conjunto ordenado, $X \subseteq A$ un subconjunto no vacío de A y $a \in A$.

1. El elemento a se dice una *cota superior* de X cuando $x \preccurlyeq a$ para todo $x \in X$. En caso de que X tenga una cota superior, decimos que X es *acotado superiormente*.
2. El elemento a se dice una *cota inferior* de X cuando $a \preccurlyeq x$ para todo $x \in X$. En caso de que X tenga una cota inferior, decimos que X es *acotado inferiormente*.

Dados un conjunto ordenado $(A, \preccurlyeq)$ y $X \subseteq A$, denotamos por $\uparrow X$ al conjunto de cotas superiores de X y por $\downarrow X$ al conjunto de cotas inferiores de X. Esta notación es la usual tomada en *Teoría de retículos*.

Ejemplo 18.2.5. Tomemos el orden parcial $(\mathbb{R}, \leq)$ (el orden usual en $\mathbb{R}$, ver apéndice) y $X := [2, 5) := \{x \in \mathbb{R} : 2 \leq x < 5\}$ (el intervalo real definido de manera usual). Notamos que $5 \in \mathbb{R}$ es cota superior de X: en efecto, por definición del intervalo $[2, 5)$ dado cualquier $y \in [2, 5)$ entonces $y < 5$, en particular $y \leq 5$, por lo tanto, 5 es *cota superior* de X.

Ejemplo 18.2.6. Tomemos el orden parcial $(\mathbb{R}, \leq)$ (el orden usual en $\mathbb{R}$, ver apéndice) y $X := [2, 5) := \{x \in \mathbb{R} : 2 \leq x < 5\}$ (el intervalo real definido de manera usual). Vemos que $2 \in \mathbb{R}$ es cota inferior de X: en efecto, por definición del intervalo $[2, 5)$ dado cualquier $y \in [2, 5)$ tenemos que $2 \leq y$, por lo tanto, 2 es *cota inferior* de X.

Ejemplo 18.2.7. Tomemos el orden parcial $(\mathbb{R}, \leq)$ (el orden usual en $\mathbb{R}$, ver apéndice) y $X := [4, +\infty) := \{x \in \mathbb{R} : 4 \leq x\}$ (el intervalo real definido de manera usual). Veamos que X no es acotado superiormente. En efecto, si razonando por reducción al absurdo suponemos que X tiene una cota superior $z \in \mathbb{R}$, entonces para todo $y \in X := [4, +\infty)$ tendríamos que $y \leq z$. Por definición del intervalo $[4, +\infty)$ tenemos que $4 \leq y$ y como $y \leq z$, entonces tenemos que

$4 \le z$. Tomando $w := z + 1$, notemos que $4 \le z < w$, por lo tanto, $4 < w$ y como en particular $4 \le w$ entonces $w \in X := [4, +\infty)$. Como $z < w$, por la tricotomía del orden usual de los números reales (ver Apéndice) tendríamos que $w \nleq z$. Como $w \in X$, esto contradiría que z es cota superior de X. Por lo tanto, X no es acotado superiormente.

18.3. Supremos e ínfimos

Definición 18.3.1. Sean $(A, \preccurlyeq)$ un conjunto ordenado y $X \subseteq A$. Un elemento $a \in X$ se dice *supremo* de X cuando a es la menor de las cotas superiores de X (si tal existe), es decir, a es una cota superior de X y $a \preccurlyeq z$ para cualquier otra cota superior z de X. En otras palabras, a es *supremo* de X si $\text{mín} \uparrow X$ existe y $a = \text{mín} \uparrow X$.

Un elemento $a \in X$ se dice *ínfimo* de X cuando a es la mayor de las cotas inferiores de X (si tal existe), es decir, a es una cota inferior de X y $z \preccurlyeq a$ para cualquier otra cota inferior z de X. En otras palabras, a es *ínfimo* de X si $\text{máx} \downarrow X$ existe y $a = \text{máx} \downarrow X$.

Ejemplo 18.3.2. Tomemos el conjunto ordenado $(\mathbb{R}, \le)$ y $X := [2, 5) := \{x \in \mathbb{R} : 2 \le x < 5\}$ (el intervalo real definido de manera usual). Vimos en el Ejemplo 18.2.5 que 5 es cota superior de X. Veamos que 5 es supremo de X, es decir, es la menor de las cotas superiores de X. En efecto, supongamos que $z \in \mathbb{R}$ es cota superior de X, luego por definición de cota superior de X para todo $y \in X := [2, 5)$ tenemos que $y \le z$. Por reducción al absurdo, supongamos que $5 \nleq z$, luego como $(\mathbb{R}, \le)$ es un orden total entonces $z \le 5$ pero como $5 \nleq z$ en particular $5 \neq z$ por lo que podemos decir que $z < 5$. Como $2 \in X := [2, 5)$ y z es cota superior de X, en particular tenemos que $2 \le z$. Como $z < 5$, por la densidad de $\le$ (ver apéndice), existe $w \in \mathbb{Q}$ (en particular $w \in \mathbb{R}$) tal que $2 \le z < w < 5$, luego $w \in X := [2, 5)$. Esto quiere decir que existe $w \in X := [2, 5)$ tal que $z < w$, pero por la tricotomía del orden usual de $\mathbb{R}$ (ver Apéndice) tenemos que $w \nleq z$, luego esto contradice que z es cota superior de X. De esta manera, podemos decir que $5 \le z$ y, por tanto, 5 es la menor de las cotas superiores de X (es decir, 5 es supremo de X).

Ejemplo 18.3.3. Tomemos el conjunto ordenado $(\mathbb{R}, \le)$ y $X := [2, 5) := \{x \in \mathbb{R} : 2 \le x < 5\}$. Vimos en el Ejemplo 18.2.6 que

2 es cota inferior de X. Veamos que 2 es ínfimo de X, es decir, es la mayor de las cotas inferiores de X. En efecto, supongamos que $z \in \mathbb{R}$ es cota inferior de X, luego por definición de cota inferior de X para todo $y \in X := [2, 5)$ tenemos que $z \leq y$. Como en particular $2 \in X := [2, 5)$, entonces $z \leq 2$. De esta manera, podemos decir que 2 es la mayor de las cotas inferiores de X (es decir, 2 es ínfimo de X).

Ejemplo 18.3.4. Consideremos de nuevo $(\mathbb{R}, \leq)$ y $X := [4, +\infty) := \{x \in \mathbb{R} : 4 \leq x\}$. Como ejercicio para el lector, dejamos la demostración de que 4 es ínfimo de X. Como X no es acotado superiormente (Ejemplo 18.2.7), entonces X no tiene supremo.

Ejemplo 18.3.5. Consideremos el conjunto ordenado $(\mathbb{R}, \leq)$ y $X := (-\infty, \pi) := \{x \in \mathbb{R} : x < \pi\}$. Como ejercicio para el lector, dejamos verificar que X no tiene cotas inferiores, por tanto, tampoco tiene ínfimo.

Observación 18.3.6. Sean $(A, \preccurlyeq)$ un conjunto ordenado y $X \subseteq A$. Si X tiene supremo, este es único. Igual sucede en caso que A tenga ínfimo. Esto se sigue del Teorema 18.1.6, dado que si X tiene supremo, tal supremo es exactamente $\text{mín} \uparrow X$, que denotaremos por $\sup X$. En el caso de que X tenga ínfimo tenemos que corresponde a $\text{máx} \downarrow X$, que denotaremos por $\text{ínf}\, X$.

18.4. Buenos órdenes

Consideremos al conjunto de los números naturales $\mathbb{N}$ junto a su orden usual $\leq$. Dentro de las propiedades que tiene este orden tenemos las siguientes:

1. $\mathbb{N}$ tiene mínimo (dependiendo de la discusión si 0 es natural o no, dicho mínimo sería 0 o 1, recordemos que para nosotros en este texto 0 es natural).
2. $\mathbb{N}$ no tiene máximo.
3. $\mathbb{N}$ es un orden total, donde además es un orden *discreto* (es decir, dado $n \in \mathbb{N}$, no existe $k \in \mathbb{N}$ tal que $n < k < n + 1$).

4. Todo $X \subseteq \mathbb{N}$, con $X \neq \varnothing$, tiene mínimo.

Centrémonos en esta última propiedad. Aunque por la intuición que tenemos de los números naturales pueda parecernos "obvia" esta propiedad, tenemos que demostrarla. Veamos una demostración de este hecho.

Proposición 18.4.1. *En el conjunto ordenado* $(\mathbb{N}, \leq)$*, todo* $X \subseteq \mathbb{N}$*, con* $X \neq \varnothing$*, tiene mínimo.*

Demostración. Por reducción al absurdo, supongamos que existe $X \subseteq \mathbb{N}$, $X \neq \varnothing$, que no tiene mínimo. Consideremos la propiedad $P(x)$: "$x \in \mathbb{N} \setminus X$". Supongamos que para cierto $k \in \mathbb{N}$ se tiene que todo natural $n < k$ satisface $P(n)$; es decir, $n \notin X$ (*hipótesis de inducción*). Si $k \in X$, por la hipótesis de inducción ningún elemento menor a k está en X, luego k sería el mínimo de X (contradice el hecho de que X no tiene mínimo), por lo tanto, $k \notin X$ (k satisface la propiedad $P(k)$).
Por el *Principio de inducción matemática forma III* (Proposición 9.3.1 tenemos que todo natural n satisface la propiedad P, es decir $\mathbb{N} \setminus X = \mathbb{N}$, por lo tanto, $X = \varnothing$ (contradice el hecho de que X se tomó no vacío).
Por lo tanto, todo subconjunto no vacío de $\mathbb{N}$ tiene mínimo (con respecto al orden usual de $\mathbb{N}$). ☑

Veamos una prueba alternativa de esta Proposición 18.4.1 usando el *Principio de inducción matemática forma I*, Proposición 9.1.1.

Demostración alternativa. Sea $X \subseteq \mathbb{N}$ cualquiera no vacío. Consideremos el conjunto de las cotas inferiores de X:

$$\downarrow X = \{n \in \mathbb{N} : n \leq x \text{ para todo } x \in X\}.$$

1. $0 \in \downarrow X$ porque $0 \leq x$ para todo $x \in \mathbb{N}$, en particular, $0 \leq x$ para todo $x \in X$.

2. Como $X \neq \varnothing$ existe $y \in X$. Luego, $y+1 \notin \downarrow X$, porque $y+1 \not\leq y$. Por lo tanto, $\downarrow X \neq \mathbb{N}$.

Como $0 \in \downarrow X$ y $\downarrow X \neq \mathbb{N}$, por aplicación de la afirmación contrarrecíproca del *Principio de inducción matemática forma I*, Proposición 9.1.1, existe $k \in \downarrow X$ tal que $k + 1 \notin \downarrow X$.

Veamos que $k = \min X$. Como $k \in \downarrow X$, entonces $k \leq x$ para todo $x \in X$. Solo falta ver que $k \in X$. Si $k \notin X$, se tendría que $k < x$ para todo $x \in X$. Luego, $k + 1 \leq x$ para todo $x \in X$ (¿por qué?). Esto implicaría que $k+1 \in \downarrow X$, lo cual es absurdo. Así $k \in X$. Por lo tanto, $k = \min X$. ☑

Esta propiedad que acabamos de demostrar para el orden usual de $\mathbb{N}$ la denominamos *Principio de buen orden de* $\mathbb{N}$. Cualquier conjunto ordenado que cumpla esta propiedad lo denominamos *buen orden*. Más precisamente:

Definición 18.4.2. Sea $(A, \preccurlyeq)$ un conjunto ordenado. Decimos que $(A, \preccurlyeq)$ es un *buen orden* si y solo si todo $X \subseteq A$, con $X \neq \varnothing$ tiene mínimo.

Es un hecho bien conocido que todo buen orden es un orden total (ejercicio para el lector).

18.5. Ejercicios

Ejercicio 18.5.1. Dado $A := \{1, 2, 3, 4, 5, 6\}$, en cada literal defina una relación de orden en A que cumpla las condiciones dadas. Además, represente el orden con un diagrama de Hasse.

1. Que sea orden total con mínimo 3.
2. Que sea orden parcial sin mínimo y con máximo 5.
3. Que tenga tres maximales.
4. Que tenga mínimo 6 y máximo 1.

5. Que sea un buen orden.

6. Que sea orden total con máximo 4 y mínimo 3.

Ejercicio 18.5.2. Dado $A := \{x \in \mathbb{N} : 1 \leq x \leq 10\}$, considere el conjunto ordenado $(X, \preccurlyeq)$ donde $a \preccurlyeq b$ si y solo si a es divisor de b y el subconjunto $B = \{4, 6, 10\}$.

1. Haga una representación de este orden por medio de un diagrama de Hasse.

2. Determine el conjunto de elementos maximales de X.

3. Determine $\uparrow B$ (el conjunto de cotas superiores de B).

4. Determine $\downarrow B$ (el conjunto de cotas inferiores de B).

5. Si existen, encuentre $\text{ínf}\, B$, $\sup B$, $\text{máx}\, B$ y $\text{mín}\, B$. Justifique su respuesta.

6. Determine si A tiene máximo, justificando su respuesta. Determine si A tiene mínimo, justificando su respuesta. En caso de que existan, determine qué elemento sería el máximo de A y cuál elemento sería el mínimo de A.

Ejercicio 18.5.3. En el conjunto $\mathbb{N}$ de los números naturales defina, si es posible, un orden que satisfaga la condición dada en cada caso.

1. Tener infinitos minimales.

2. Tener un único minimal y no tener mínimo.

3. Tener mínimo y máximo.

Ejercicio 18.5.4. En cada uno de los siguientes numerales, damos un conjunto ordenado y varios subconjuntos que llamamos B. En cada caso determinar (si es posible) el $\uparrow B$, $\downarrow B$, $\text{ínf}\, B$, $\sup B$, $\text{máx}\, B$ y $\text{mín}\, B$, justificando su respuesta.

1. En $(\mathbb{R}, \leq)$,

i) $B := [1, 3]$. ii) $B := (-3, 1] \cup (2, 4]$.
iii) $B := \mathbb{Q} \cap (-2, 3]$. iv) $B := [-2, \infty)$.
v) $B := \mathbb{Z}$. vi) $B := \mathbb{N}$.
vii) $B := \varnothing$.

2. En $(D_{30}, |)$,

   i) $B = \{2, 3\}$. ii) $B = \{2, 5, 10\}$. iii) $B = \varnothing$.

3. En $(\mathscr{P}(A), \subseteq)$ donde $A = \{a, b, c, d, e\}$,

   i) $B = \{\{a\}, \{e\}\}$.
   ii) $B = \{\{b\}, \{b, c\}, \{a, b, c\}\}$.
   iii) $B = \{\{a, c\}, \{b, c\}, \{b, e\}\}$.

Ejercicio 18.5.5. Demuestre o refute, justificando su respuesta.

1. Si $(A, \preccurlyeq)$ es un conjunto ordenado, $\uparrow \varnothing = A = \downarrow \varnothing$.
2. En cualquier conjunto ordenado $(A, \preccurlyeq)$, $\sup \varnothing$ e $\inf \varnothing$ siempre existen.
3. Si $(A, \preccurlyeq)$ tiene más de un maximal, entonces $(A, \preccurlyeq)$ no es orden total.
4. Si $(X, \preccurlyeq)$ es un conjunto ordenado tal que $\varnothing$ tiene supremo, entonces X tiene mínimo.
5. Todo buen orden es un orden total.
6. $(D_{100}, |)$ es un buen orden (D_{100} es el conjunto de los divisores de 100 con el orden de la divisibilidad).
7. Cualquiera sea el conjunto X y cualquiera que sea $\varnothing \neq \mathscr{B} \subseteq \mathscr{P}(X)$, en el conjunto ordenado $(\mathscr{P}(X), \subseteq)$, $\mathscr{B}$ es acotado superiormente y es acotado inferiormente.
8. Si $(X, \preccurlyeq)$ es orden total, entonces $(X, \preccurlyeq)$ tiene mínimo.
9. Si $(X, \preccurlyeq)$ tiene más de un minimal, entonces $(X, \preccurlyeq)$ no tiene mínimo.
10. Si $(X, \preccurlyeq)$ tiene máximo, él es el único maximal.

11. En $\mathbb{R}$ con el orden usual, para todo par de subconjuntos no vacíos S y T de $\mathbb{R}$ se cumple que: si S es acotado superiomente y $T \subseteq S$, entonces T también es acotado superiormente y el conjunto de cotas superiores de T contiene al conjunto de cotas superiores de S.

12. En $\mathbb{R}$ con el orden usual, para todo par de subconjuntos no vacíos S y T de $\mathbb{R}$ se cumple que: si S es acotado superiomente y $T \subsetneq S$, entonces $\sup T < \sup S$.

Ejercicio 18.5.6. Sean $(X, \preceq)$ un conjunto ordenado y $\varnothing \neq A \subseteq X$. Demuestre que si x es supremo de A y $x \in A$, entonces x es máximo de A. Adicionalmente, demuestre que si x es ínfimo de A y $x \in A$, entonces x es mínimo de A.

Ejercicio 18.5.7. Demuestre que tomando $X := \varnothing$ y $\preccurlyeq := \varnothing$, el conjunto ordenado $(X, \preccurlyeq)$ es un buen orden.

Ejercicio 18.5.8. Definimos en $\mathbb{R}^2$ las siguientes relaciones (donde $\leq$ corresponde al orden usual en $\mathbb{R}$):

- $(a, b) \preccurlyeq_l (c, d)$ si y solo si se da uno de los dos siguientes casos:

  i) $a < c$ o

  ii) $a = c$ y $b \leq d$,

  denominado *orden lexicográfico*.

- $(a, b) \preccurlyeq_p (c, d)$ si y solo si $a \leq c$ y $b \leq d$, denominado *orden producto*.

1. Demuestre que $\preccurlyeq_l$ y $\preccurlyeq_p$ son realmente relaciones de orden en $\mathbb{R}^2$.

2. Determine $\{(x, y) : (1, 1) \preccurlyeq_l (x, y)\}$ y represente este conjunto en el plano cartesiano.

3. Determine $\{(x, y) : (1, 1) \preccurlyeq_p (x, y)\}$ y represente este conjunto en el plano cartesiano.

Ejercicio 18.5.9. Pruebe que el *Principio del buen orden* de $\mathbb{N}$ es equivalente al *Principio de inducción matemática forma I*.

Parte V

Funciones

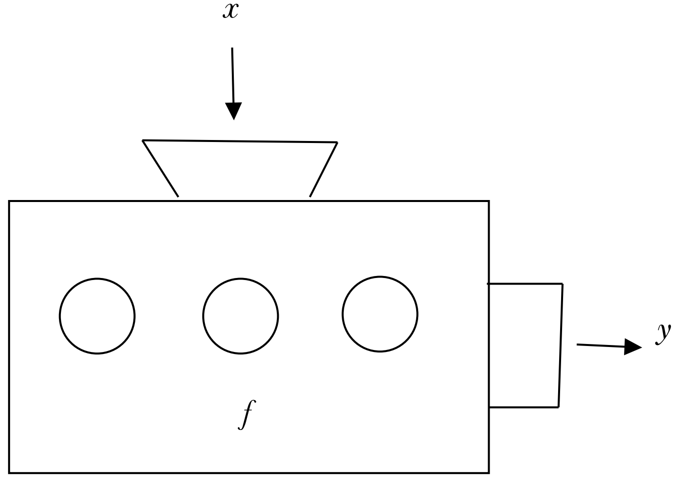
Lección *diecinueve* **Funciones**

19.1. Concepto de función

Podríamos decir que uno de los conceptos centrales en matemáticas es el de *función*, puesto que muy buena parte de los desarrollos de lo conocido como matemáticas modernas (e.g., topología, análisis, álgebra abstracta, geometría no euclidiana, teoría de números, sistemas dinámicos, ecuaciones diferenciales, teoría de modelos, etc.) estudia y también utiliza como herramienta a las funciones.

Pensemos en el siguiente ejemplo coloquial: considerando A el conjunto de todos los seres humanos, tomemos la relación $\mathscr{F}$ definida por $\mathscr{F} := \{(X,Y) \in A \times A : Y \text{ es padre biológico de } X\}$. Notemos que todo ser humano X (quitando de A a seres mitológicos y de relatos religiosos) está relacionado con un único ser humano Y por intermedio de esta relación (es decir, que todo ser humano X tiene un único padre biológico Y).

Las funciones son relaciones que tienen una particularidad muy especial y es que a cada elemento del conjunto de salida le corresponde, o se le asigna, un único elemento del conjunto de llegada. Así, podemos imaginar a las funciones como un cierto tipo de *máquinas abstractas* a las que les introducimos un elemento, digamos x, del conjunto de sálida y esa máquina abstracta nos arroja un único elemento, digamos y, del conjunto de llegada, correspondiente a x.



Esto será simbolizado simplemente por:

$$x \longmapsto y.$$

Una función no se describe necesariamente mediante una fórmula, ni necesita tratar solo con números. Una función puede relacionar elementos de conjuntos que no son números, por ejemplo, considere la función que asigna a cada persona, representada por x, su fecha de nacimiento (en el calendario gregoriano). En este caso tendríamos que:

$$x \longmapsto \text{fecha de nacimiento de } x.$$

Particularmente,

$$\begin{aligned}
\text{Bernhard Riemann} &\longmapsto \text{17 de septiembre de 1826}\\
\text{Georg Cantor} &\longmapsto \text{3 de marzo de 1845}\\
\text{David Hilbert} &\longmapsto \text{23 de enero de 1862}\\
\text{Albert Einstein} &\longmapsto \text{14 de marzo de 1879}\\
\text{Alan Turing} &\longmapsto \text{23 de junio de 1912}\\
&\vdots\\
&\text{etcétera.}
\end{aligned}$$

En lo que sigue daremos una definición rigurosa de función en términos de conjuntos.

Definición 19.1.1. Sean A y B conjuntos. Una *función* f de A en B, en símbolos $f : A \longrightarrow B$, es una relación de A en B, es decir, $f \subseteq A \times B$, que satisface:

i. $dom(f) = A$. Esto significa que para todo $x \in A$ existe $y \in B$ tal que $(x, y) \in f$.

ii. Dados $x \in A$ y $y, y' \in B$, si $(x, y), (x, y') \in f$, entonces $y = y'$.

El conjunto de salida A es llamado *dominio de la función* f, denotado por $dom(f)$, y el conjunto de llegada B es llamado *codominio de la función* f, el cual será denotado por $codom(f)$.

Observación 19.1.2. Nótese que como cualquier función $f : A \longrightarrow B$ es una relación podemos hablar de los conjuntos $dom(f)$ y $rango(f)$, dominio y rango de la relación f, respectivamente. En efecto, en este caso en que f es función,

$$dom(f) = A, \qquad rango(f) \subseteq B$$

y

$$f \subseteq dom(f) \times rango(f).$$

Para referirnos a una función adecuadamente, es necesario decir: "sean A y B conjuntos y $f : A \longrightarrow B$ una función". Muchas veces con el fin de ser más conciso simplemente se dirá: "sea $f : A \longrightarrow B$ una función". De esto se sobreentenderá que A y B son conjuntos. No será suficiente escribir: "sea f una función", sin especificar el dominio y el codominio, a menos que sean conocidos del contexto, como en los cursos elementales de cálculo en los que se estudian funciones de valor y variable real.

Sea $f : A \longrightarrow B$ una función. Dado $x \in A$, como f es una relación, la clase de x respecto a f es $[x]_f = \{b \in B : x\,f\,b\}$. Este conjunto no es vacío por la condición (i) de la Definición 19.1.1 y tiene un único elemento por la condición (ii) de la Definición 19.1.1. Supongamos que y es el único elemento de B para el cual $x\,f\,y$. Denotaremos a este único elemento de $[x]_f$ por $f(x)$. Es decir, $y = f(x)$. Esto se leerá diciendo que "y es *la imagen* de x bajo la función f" o "y es el único elemento de B que toma f en x" o "x es *una preimagen* de y bajo f". Todo esto será simbolizado por

$$\begin{aligned} f : A &\longrightarrow B \\ x &\longmapsto y = f(x) \quad \text{para todo } x \in A. \end{aligned}$$

Observación 19.1.3. Aunque es habitual encontrar frases en cursos elementales como: "sea $f(x)$ una función", esta frase solo será correcta cuando los elementos de B son funciones. Si $f : A \longrightarrow B$ es una función, su nombre es "f", no "$f(x)$". El término "$f(x)$" corresponde al único elemento del codominio B que toma la función f en el elemento x de A; es decir, $f(x)$ es un elemento de B y no el nombre de la función.

19.2. Ejemplos de funciones

Hay algunas funciones particulares que son encontradas a través de todas las matemáticas.

Ejemplo 19.2.1. Sea A un conjunto no vacío. Recordemos el Ejemplo 14.2.2 en el que vimos la relación $\Delta_A = \{(x, y) \in A \times A \ : \ x = y\} \subseteq A \times A$. Veamos que Δ_A es una función:

1. Como Δ_A es una relación en A, sabemos que $dom(\Delta_A) \subseteq A$. Veamos que $A \subseteq dom(\Delta_A)$ para concluir que $dom(\Delta_A) = A$. Sea $x \in A$ cualquiera. Por definición de Δ_A tenemos que $(x, x) \in \Delta_A$. Así, $x \in dom(\Delta_A)$. Esto prueba que $A \subseteq dom(\Delta_A)$.

2. Sean $x, y, y' \in A$ cualesquiera. Supongamos que $(x, y) \in \Delta_A$ y $(x, y') \in \Delta_A$. Por definición de Δ_A se tiene que $x = y$ y $x = y'$. Luego $x = y = y'$.

Concluímos de 1, 2 y la Definición 19.1.1 que Δ_A es función. Usaremos la notación id_A para referirnos a Δ_A como función.

Definición 19.2.2 (Función identidad)**.** Sea A un conjunto no vacío. La función

$$\begin{aligned} id_A : A &\longrightarrow A \\ x &\longmapsto id_A(x) := x, \ \text{ para todo } \ x \in A, \end{aligned}$$

es denominada *función identidad* en A. Vea el Ejemplo 19.2.1. Otras notaciones muy usadas para la función identidad en A son I_A o 1_A.

Ejemplo 19.2.3. Sean $A = \{1, 2, 3, 4, 5\}$, $B = \{a, b, c\}$ y $S = \{1, 3, 5\} \subset A$. Consideremos las relaciones $f \subseteq A \times B$ y $g \subseteq S \times B$ dadas por $f = \{(1, b), (2, b), (3, b), (4, b), (5, b)\}$ y $g = \{(1, b), (3, b), (5, b)\} = \{(x, b) \ : \ x \in S\}$. Vemos que tanto f como g son funciones y que $g \subset f$ (¿por qué?). Más precisamente, la función f coincide con la función g en cada uno de los elementos de S. Esto es, $f(x) = g(x) = b$ para todo $x \in S$. Diremos que g es la *restricción* de la función f al conjunto S, o que f es una *extensión* de la función g al conjunto A.

Definición 19.2.4 (Restricción y extensión de funciones). Sean A, B conjuntos no vacíos y $S \subseteq A$ un subconjunto.

1. Sea $f : A \longrightarrow B$ una función. Consideremos ahora la siguiente función

$$\begin{aligned} g : S &\longrightarrow B \\ x &\longmapsto g(x) := f(x), \text{ para todo } x \in S. \end{aligned}$$

   g es denominada *la función restricción* de f al conjunto S. La función g es denotada por $f|_S$ y se lee "f restringida a S".

2. Sea $g : S \longrightarrow B$ una función. Cualquier función $G : A \longrightarrow B$ tal que $G(x) = g(x)$ para todo $x \in S$ es denominada *una función extensión* de g al conjunto A. En este caso, g es la restricción de G al conjunto S, $G|_S$.

Ejemplo 19.2.5 (Función inclusión). Sea A conjunto no vacío y $S \subseteq A$. Consideremos la siguiente función

$$\begin{aligned} j : S &\longrightarrow A \\ x &\longmapsto j(x) := x, \quad \text{para todo } x \in S. \end{aligned}$$

Como consecuencia de la anterior Definición 19.2.4, j es la restricción de la función id_A al conjunto S, $(id_A)|_S$. La función j es denominada *función inclusión* de S en A.

Ejemplo 19.2.6. Sean A, B, S y f como en el Ejemplo 19.2.3. La relación $f \subseteq A \times B$ es una función. En efecto, $dom(f) = \{1, 2, 3, 4, 5\} = A$ y, dados $x \in A$ y $y, z \in B$ cualesquiera, si $(x, y), (x, z) \in f$ entonces $y = b = z$. Es decir, f es función porque satisface las condiciones (i) y (ii) de la Definición 19.1.1. ese que

$$\begin{aligned} f : A &\longrightarrow B \\ x &\longmapsto f(x) := b, \text{ para todo } x \in A. \end{aligned}$$

Como a cada uno de los elementos de A le corresponde por f la misma imagen que es el elemento $b \in B$, esta función es llamada función *constante*. Obsérvese también que con respecto a la función g del Ejemplo 19.2.3, f es una extensión de g al conjunto A, es decir $f|_S$ coincide con g.

Definición 19.2.7 (Función constante)**.** Sean A, B conjuntos no vacíos y sea b algún elemento fijo de B. Consideremos la función

$$\begin{aligned} f_b : A &\longrightarrow B \\ x &\longmapsto f_b(x) := b \quad \text{para todo } \; x \in A. \end{aligned}$$

f_b es denominada *función constante*.

La manera adecuada de definir una función es fijar su dominio, su codominio y determinar lo que la función hace a cada elemento del dominio (lo cual es exactamente lo mismo que definir un subconjunto apropiado del producto cartesiano entre el dominio y el codominio). Por ejemplo, podemos escribir: "sea $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ una función definida por la fórmula algebraica $f(x) := 5x^4 - 7x + 1$". En este caso se sobreentiende que el dominio de f es $\mathbb{Z}$, su codominio es también $\mathbb{Z}$ y lo que le hace la función a cada elemento $a \in \mathbb{Z}$ está descrito por la expresión algebraica $f(a) := 5a^4 - 7a + 1$. Por ejemplo, si tomamos $a := -1 \in \mathbb{Z}$, tenemos en este caso que $f(-1) = 5(-1)^4 - 7(-1) + 1 = 13$.

Ejemplo 19.2.8. Consideremos la fórmula $f(x) = x/2$. Esta fórmula no define propiamente una función, porque no nos presenta un dominio ni un codominio. Supongamos, por ejemplo, que solo nos importa cuando x es entero y su imagen sea un entero también. Será entendido que, dada una fórmula como esta, se tomará como dominio el mayor subconjunto de $\mathbb{Z}$ en el que todos sus elementos al dividirlos entre 2 sigue siendo entero; en este caso el conjunto $P := \{k \in \mathbb{Z} : k \quad \text{es par}\}$ es tomado como dominio. El codominio será $\mathbb{Z}$, que corresponde justamente al rango de esta función. Sin embargo, el codominio podría ser tomado como cualquier conjunto que contenga a $\mathbb{Z}$.

Ejemplo 19.2.9. En cursos de cálculo elemental, se pueden dar fórmulas algebraicas como $f(x) = \frac{\sqrt{x-1}}{x-1}$. Como las funciones en estos cursos son funciones de valor y variable real, podríamos seguir la práctica estándar de tomar como dominio el mayor subconjunto de $\mathbb{R}$ para el cual la expresión tiene sentido. Nótese que en este caso

$$\begin{aligned} dom(f) &= \{x \in \mathbb{R} : x - 1 \geq 0 \text{ y } x - 1 \neq 0\} \\ &= \{x \in \mathbb{R} : x \geq 1 \text{ y } x \neq 1\} = [1, +\infty) - \{1\} = (1, +\infty). \end{aligned}$$

El codominio puede ser tomado como $\mathbb{R}$, aunque muchos otros subconjuntos de $\mathbb{R}$ pueden ser tomados también como codominios, por ejemplo $[-3, +\infty)$ o $(0, +\infty)$. Este último conjunto es exactamente el rango de f (¿por qué?).

No todas las funciones, incluidas las que tienen como dominio y codominio $\mathbb{R}$, pueden ser definidas por una fórmula algebraica. Inclusive cuando una función es definida por una fórmula algebraica, no siempre es posible usar una única fórmula y algunas veces la fórmula debe ser dada por casos. Consideremos la conocida función valor absoluto

$$\begin{aligned} |\cdot| : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto |x| = \begin{cases} x, & \text{si} \quad x \geq 0 \\ -x, & \text{si} \quad x < 0. \end{cases} \end{aligned}$$

En general, una función puede ser presentada separando su dominio en dos o más subconjuntos disyuntos dos a dos y definiendo la función en cada uno de tales subconjuntos. Con el propósito de destacar los subconjuntos usados en la función $|\cdot|$ anterior escribimos, de una manera más apropiada pero menos elegante y menos usada, así:

$$\begin{aligned} |\cdot| : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto |x| = \begin{cases} x, & \text{si} \quad x \in [0, +\infty) \\ -x, & \text{si} \quad x \in (-\infty, 0). \end{cases} \end{aligned}$$

Definición 19.2.10 (Función definida por partes). Sean A, B conjuntos cualesquiera y $\mathscr{P} = \{A_j \ : \ j \in I\}$ una partición de A, donde I es un conjunto de índices no vacío. Consideramos la función

$$\begin{aligned} f : A &\longrightarrow B \\ x &\longmapsto f(x) = \begin{cases} \quad \vdots \\ f_j(x)\ , \text{ si } \ x \in A_j \\ \quad \vdots \end{cases} \end{aligned}$$

donde $f_j : A_j \longrightarrow B$ es una función para cada $j \in I$. La función f es denominada *función definida por partes*.

f definida de esta manera es función con dominio A por las siguientes razones:

1. Como $\mathscr{P}$ es una partición de A, entonces $\bigcup_{j\in I} A_j = A$, y puesto que $dom(f_j) = A_j$ $(j \in I)$, luego $dom(f) = A$.
2. Como $\mathscr{P}$ es una partición de A, entonces ningún $x \in A$ puede estar simultáneamente en dos conjuntos A_i, A_j diferentes de dicha partición, por lo que $f(x)$ está dada unívocamente por la imagen $f_j(x)$ para el único $j \in I$ tal que $x \in A_j$.

Ejemplo 19.2.11. Consideremos $\mathscr{P} = \{[j, j+1) \ : \ j \in \mathbb{Z}\}$, que es una partición de $\mathbb{R}$, y

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto f(x) = \begin{cases} \qquad \vdots \\ f_{-1}(x), & \text{si } x \in [-1, 0), \\ f_0(x), & \text{si } x \in [0, 1), \\ f_1(x), & \text{si } x \in [1, 2), \\ \qquad \vdots \end{cases} \end{aligned}$$

es decir, $f(x) := f_j(x)$ si $x \in [j, j+1)$ para cada $j \in \mathbb{Z}$, donde

$$\begin{aligned} f_j : [j, j+1) &\longrightarrow \mathbb{R} \\ x &\longmapsto f_j(x) = j. \end{aligned}$$

Así, por ejemplo, $f(\pi) = f_3(\pi)$ porque $3 \leq \pi < 4$, luego, $f(\pi) = f_3(\pi) = 3$. También, $f(-\sqrt{2}) = f_{-2}(-\sqrt{2})$ porque $-2 \leq -\sqrt{2} < -1$, por lo tanto, $f(-\sqrt{2}) = f_{-2}(-\sqrt{2}) = -2$.

Ejemplo 19.2.12 (Sucesiones)**.** Dado A conjunto no vacío, una *sucesión en A* es simplemente una función

$$s : \mathbb{N} \to A.$$

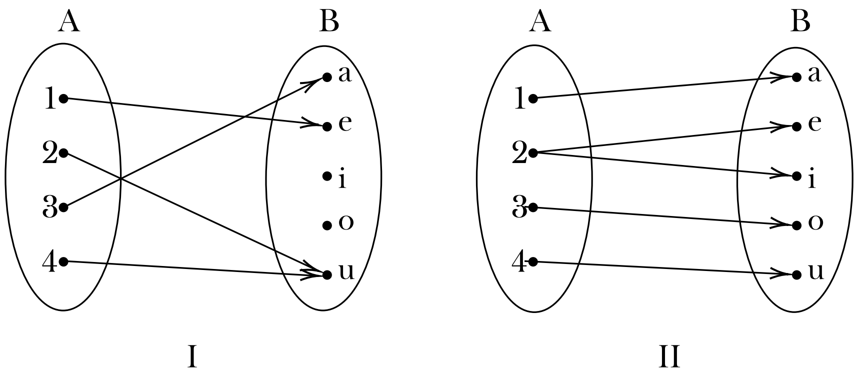
La forma usual en que encontramos denotada una sucesión en la literatura es $(s_n)_{n\in\mathbb{N}}$ o $(s_n)_{n=0}^{\infty}$, donde el elemento s_n corresponde a $s_n := s(n) \in A$ para cada $n \in \mathbb{N}$. En los textos donde el cero no es tomado como un número natural, la notación de este tipo de funciones es $(s_n)_{n=1}^{\infty}$.

19.3. Representación de las funciones

En esta sección presentamos las distintas maneras de representar las funciones que no son diferentes a las formas como fueron representadas las relaciones.

Sean A y B conjuntos. De la Definición 19.1.1 sabemos que toda función $f : A \to B$ es una relación de A en B, es decir, un subconjunto de $A \times B$. Podemos pensar y representar los elementos (a, b) de $A \times B$ que están en esta relación f mediante un diagrama de flechas de tal manera que habrá una flecha partiendo de $a \in A$ y llegando hasta $b \in B$ siempre que (a, b) esté en la relación f; es decir, si $f(a) = b$.

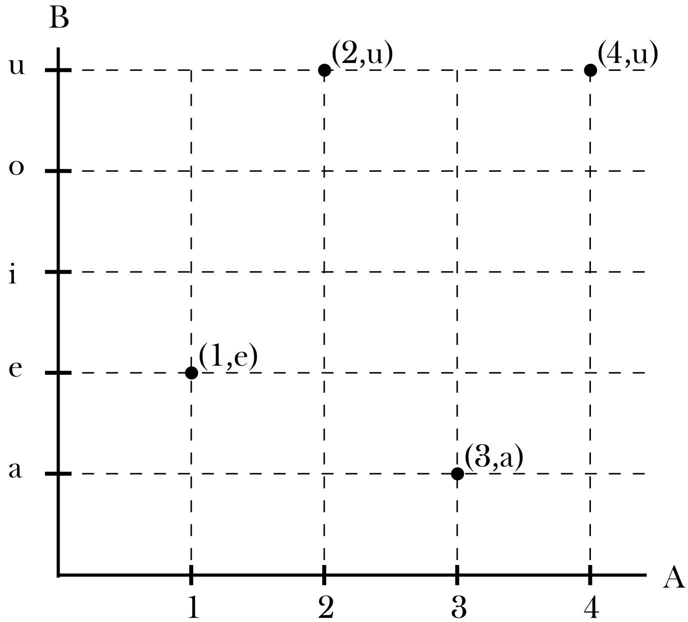
Ejemplo 19.3.1. Sean $A = \{1, 2, 3, 4\}$ y $B = \{a, e, i, o, u\}$. Dos diagramas de flechas de A en B son presentados en la siguiente figura.



En la parte I de la figura, el diagrama de flechas corresponde a la relación $\{(1, e), (2, u), (3, a), (4, u)\} \subseteq A \times B$, la cual es una función, porque de cada elemento de A sale una única flecha. Que haya elementos del codominio B a los que no le lleguen flechas, en este caso i y o, y que haya elementos en el codominio B a los que le lleguen dos flechas, en este caso u, no afecta el hecho de ser función, porque las condiciones pedidas en la definición de función están sobre los elementos del dominio y no sobre los elementos del codominio.

En la parte II de la figura, la relación de A en B representada es $\{(1, a), (2, e), (2, i), (3, o), (4, u)\}$, la cual no es función porque a pesar de que de todos los elementos de A salen flechas, del elemento $2 \in A$ salen dos flechas, es decir, la clase de 2 según esta relación tiene dos elementos distintos, a saber i y e.

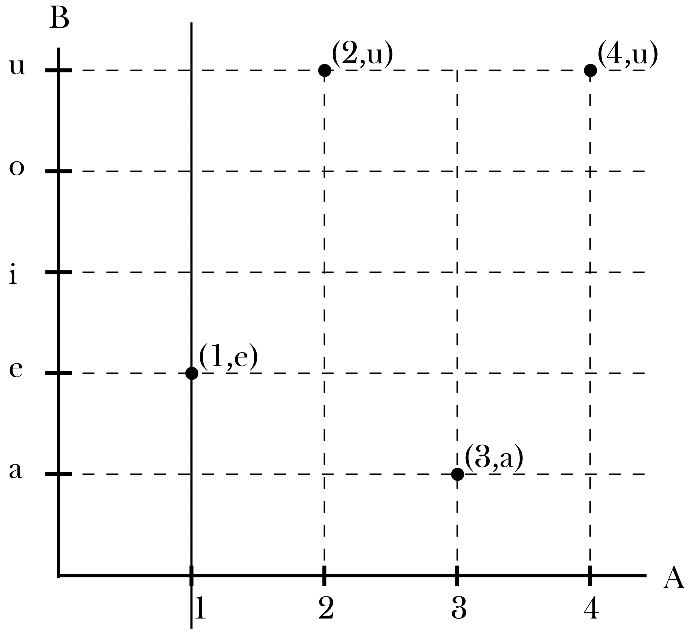
Como podemos notar, tener una representación mediante diagrama de flechas nos permite reconocer si una relación de A en B es una función con dominio A y codominio B. Basta verificar que de todos los elementos del conjunto de salida A salen flechas, esto significa que el dominio de la relación coincide con el conjunto de salida A, y de cada elemento del dominio de la relación sale una única flecha.



Ejemplo 19.3.2. Representamos en este ejemplo la función considerada en la parte I del Ejemplo 19.3.1. Esta representación consiste en resaltar los elementos de A y de B a lo largo de un eje horizontal y a lo largo de un eje vertical, respectivamente. Luego, trazamos líneas paralelas a los ejes y que pasen por las representaciones de los elementos de estos conjuntos. Así obtenemos una cuadrícula en la que cada intersección representa las parejas ordenadas del producto cartesiano $A \times B$. En esta representación resaltamos únicamente las

parejas ordenadas que están en la función que estamos considerando. Ver gráfico anterior.

Observación 19.3.3. Tal como hicimos con las relaciones en la Lección 14, la anterior representación la denominamos *gráfico* de la función f.



Una manera geométrica de verificar si una relación $f \subseteq A \times B$ es una función es centrando nuestra atención en el gráfico de f. Para cada $x \in A$, la Definición 19.1.1 de función implica que x se relaciona con un único elemento $y \in B$ por intermedio de f. Por lo tanto, para todo $x \in A$ existe una y solo una pareja ordenada en el gráfico de f tal que x aparece como primera coordenada. De este modo, si se tiene una representación de f por medio de su gráfico como en el Ejemplo 19.3.2, basta trazar una recta vertical paralela al eje donde están representados los elementos del conjunto B y que pase por x, que estará situado en el eje horizontal. Esta recta debe intersectarse con un único punto del gráfico de f. Así vemos que cada elemento x de A tiene imagen en B y que esta imagen es única. Para ilustrar esto, tomamos como caso particular $x = 1$ en el anterior gráfico de f.

19.4. Igualdad de funciones

En esta parte nos proponemos aclarar qué significa que dos de estos objetos que hemos llamado funciones sean iguales. Supongamos en principio que f y g son funciones tales que $f = g$. Por Definición 19.1.1 tenemos que toda función es una relación; es decir, es un conjunto de parejas ordenadas. Así que vemos la igualdad $f = g$ como una igualdad de conjuntos. Consideremos $x \in dom(f)$ cualquiera. Sabemos que existe $y \in rango(f)$ tal que $(x, y) \in f$. Como $f = g$, entonces $(x, y) \in g$ y por consiguiente $x \in dom(g)$ y $y \in rango(g)$; hemos demostrado así que $dom(f) \subseteq dom(g)$ y que $rango(f) \subseteq rango(g)$. De manera análoga podemos demostrar que $dom(g) \subseteq dom(f)$ y que $rango(g) \subseteq rango(f)$. Por lo tanto, $dom(f) = dom(g)$ y $rango(f) = rango(g)$ siempre que $f = g$. Nótese que los codominios de dichas funciones no necesariamente coinciden. A continuación, presentamos un ejemplo que clarifica esta situación.

Ejemplo 19.4.1. Considere el conjunto $f = \{(n, n + 2) \mid n \in \mathbb{N}\}$. El conjunto f es un subconjunto de $\mathbb{N} \times \mathbb{N}$ que satisface las condiciones de la Definición 19.1.1, y por lo tanto, f es una función de $\mathbb{N}$ en $\mathbb{N}$. Sin embargo, también es válido que $f \subset \mathbb{N} \times \mathbb{Z}$, e inclusive que $f \subset \mathbb{N} \times \mathbb{R}$, que satisfacen las condiciones de la definición de función. Entonces f puede ser también pensada como una función de $\mathbb{N}$ en $\mathbb{Z}$, o de $\mathbb{N}$ en $\mathbb{R}$. Tal ambigüedad no es aceptable cuando usamos funciones rigurosamente, y por este motivo el dominio y el codominio de una función deben ser especificados como parte de la definición de una función, a menos que sea claro del contexto y no se preste para ninguna ambigüedad como en este ejemplo.

De nuevo, suponemos que $f = g$ y sea $x \in dom(f) = dom(g)$ cualquiera. Como $x \in dom(f) = dom(g)$, $(x, g(x)) \in g = f$. Entonces $(x, f(x)), (x, g(x)) \in f = g$. Como g es función, de la condición ii de la Definición 19.1.1 se concluye que, $f(x) = g(x)$. Esto prueba que si $f = g$ entonces $f(x) = g(x)$ para todo $x \in dom(f) = dom(g)$. Recíprocamente, supongamos que $dom(f) = dom(g)$ y que $f(x) = g(x)$ para todo $x \in dom(f) = dom(g)$. Esto implica que

$$f = \{(x, f(x)) : x \in dom(f)\} = \{(x, g(x)) : x \in dom(g)\} = g.$$

Por lo tanto, $f = g$ (como conjuntos) si y solo si $dom(f) = dom(g)$ y $f(x) = g(x)$ para todo $x \in dom(f) = dom(g)$.

Además de lo anterior, exigiremos que los codominios de las respectivas funciones sean iguales cuando queramos ver que dichas funciones son iguales.

Definición 19.4.2 (Igualdad de funciones). Sean $f : A \longrightarrow B$ y $g : C \longrightarrow D$ funciones. Decimos que $f = g$ si y solo si $A = C$, $B = D$ y $f(x) = g(x)$ para todo $x \in A$.

De la Definición 19.4.2 se ve que una demostración de la igualdad de dos funciones $f : A \longrightarrow B$ y $g : C \longrightarrow D$ tiene tres partes. Primero, la prueba de que $dom(f)$ es igual a $dom(g)$, es decir, $A = C$. Segundo, la prueba de que $codom(f)$ es igual a $codom(g)$, es decir $B = D$. Y tercero, la prueba de que $f(x) = g(x)$ para todo $x \in A = C$. Nótese que las dos primeras partes de una demostración de igualdad de funciones corresponden a pruebas de igualdades entre conjuntos y la última parte corresponde a una prueba de igualdad entre elementos de $B = codom(f) = codom(g)$.

Ejemplo 19.4.3 (Función parte entera). Veamos que la función f del Ejemplo 19.2.11 es igual a la función $\lfloor\cdot\rfloor : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $\lfloor x \rfloor = n$ para todo $x \in \mathbb{R}$ donde n es el mayor de los números enteros menores o iguales a x. Esta función es conocida como *función parte entera*. Por definición de las funciones f y $\lfloor\cdot\rfloor$ vemos que

$$codom(f) = codom(\lfloor\cdot\rfloor) = \mathbb{R}.$$

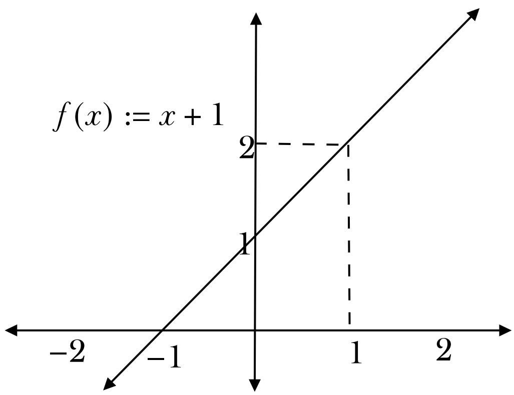
Veamos que $dom(\lfloor\cdot\rfloor) = dom(f) = \mathbb{R}$. Sea $x \in \mathbb{R}$ cualquiera. Tal x está en uno y solo uno de los conjuntos $[j, j+1)$ puesto que P es una partición de $\mathbb{R}$, ver Ejemplo 16.3.2(3). Esto implica que $f(x) = j$ y, por lo tanto, $dom(f) = \mathbb{R}$. También sabemos que para todo $x \in \mathbb{R}$ existe $m \in \mathbb{Z}$ tal que $m \leq x$, de no ser así x sería una cota inferior de $\mathbb{Z}$ lo cual es absurdo. Por lo tanto, el conjunto $(-\infty, x] \cap \mathbb{Z}$ es no vacío y tiene máximo porque cualquier conjunto no vacío, acotado superiormente de números enteros tiene máximo. Esto muestra que $dom(\lfloor\cdot\rfloor) = \mathbb{R}$.

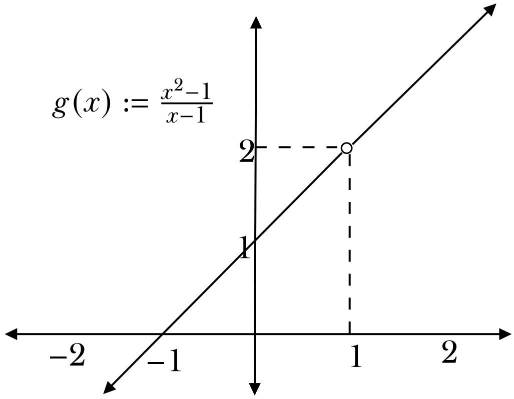
Como $x \in [j, j+1)$, notamos que $j \in (-\infty, x] \cap \mathbb{Z}$ y además $j = \text{máx}\,(-\infty, x] \cap \mathbb{Z}$, pues de no ser así x no estaría en $[j, j+1)$ sino en otro conjunto de la partición P. Esto prueba que $\lfloor x \rfloor = j = f(x)$ para todo $x \in \mathbb{R}$. Concluímos que $f = \lfloor \cdot \rfloor$.

Ejemplo 19.4.4. Consideremos las funciones de $\mathbb{R}$ en $\mathbb{R}$ dadas por las fórmulas algebraicas $f(x) = x + 1$ y $g(x) = \dfrac{x^2 - 1}{x - 1}$.
Vemos que

$$g(x) = \frac{x^2 - 1}{x - 1} = \frac{(x-1)(x+1)}{x - 1} = x + 1 = f(x).$$

Sin embargo, estas identidades son válidas únicamente cuando $x \neq 1$. Es decir, $f(x) = g(x)$ para todo $x \in \mathbb{R} - \{1\}$. Como $dom(f) = \mathbb{R}$ y en cambio $dom(g) = \mathbb{R} - \{1\}$ entonces $dom(f) \neq dom(g)$. Esto implica que $f \neq g$.





19.5. Ejercicios

Ejercicio 19.5.1. Sean $A = \{a, b, c, d\}$, $B = \{a, b, c\}$ conjuntos, y $f = \{(a, b), (b, b), (c, a), (d, c)\}$ función de A en B. ¿Quiénes son $f(a), f(b), f(c)$ y $f(d)$?

Ejercicio 19.5.2. Considere las funciones:
$f : \mathbb{R} \to \mathbb{R}$ definida por la expresión $f(x) = x^3 - 3x$ para todo $x \in \mathbb{R}$, $g : \mathbb{R} \to \mathbb{Z}$ dada por $g = \{(x, n) \in \mathbb{R} \times \mathbb{Z} : n \leq x < n + 1\}$, y $h : N \to C$, donde N es el conjunto de todos los países y C es el conjunto de todas las ciudades, definida así $h(n) :=$ la capital del país n, para cualquier país n. Halle $f(3)$, $f(-3)$, $g(\pi)$, $g(-\pi)$, $g(-\sqrt{7})$, $g(\sqrt{7})$, $h(Italia)$ y $h(India)$.

Ejercicio 19.5.3. Demuestre que una relación f de A en B es una función si y solo si para cualesquiera $x, y \in A$ y $a, b \in B$ tales que $(x, a) \in f$ y $(y, b) \in f$,

$$x = y \text{ implica } a = b.$$

Note que si f es una función de A en B, entonces para cualesquiera $x, y \in A$,

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

Ejercicio 19.5.4. Sean A y B conjuntos no vacíos. Considere

$$\pi_1 : A \times B \longrightarrow A \qquad \text{y} \qquad \pi_2 : A \times B \longrightarrow B$$

definidas por $\pi_1((a, b)) = a$ y $\pi_1((a, b)) = b$ para cualquier $(a, b) \in A \times B$. π_1 y π_2 son conocidas como *funciones proyección* de $A \times B$. Pruebe que π_1 y π_2 son en efecto funciones.

Ejercicio 19.5.5. Sean $f : A \longrightarrow B$ y $g : A \longrightarrow B$ funciones. Determine si la siguiente afirmación es verdadera o falsa. Justifique plenamente su respuesta.

$$f = g \quad \text{si y solo si} \quad rango(f) = rango(g).$$

Ejercicio 19.5.6. Del Ejemplo 19.4.3, demuestre que $rango(\lfloor \cdot \rfloor) = \mathbb{Z}$.

Ejercicio 19.5.7. Sea X un conjunto no vacío y sea $S \subseteq X$ un subconjunto. La *función característica* para A en X, denotado por χ_A, es la función $\chi_A : X \longrightarrow \{0, 1\}$ definida por

$$\chi_A(y) = \begin{cases} 1, & \text{si } \ y \in A, \\ 0, & \text{si } \ y \notin A. \end{cases}$$

Sean $A, B \subseteq X$ subconjuntos. Pruebe que $A = B$ si y solo si $\chi_A = \chi_B$.

Ejercicio 19.5.8. Sean $f : A \longrightarrow C$ y $g : B \longrightarrow C$ funciones.

- Pruebe que si $A \cap B = \emptyset$, entonces la relación $f \cup g$ de $A \cup B$ en C es función.
- Más generalmente, pruebe que $f \cup g$ de $A \cup B$ en C es función si y solo si $f|_{A \cap B} = g|_{A \cap B}$.

Ejercicio 19.5.9. Suponga que $f : A \to B$ es una función y $\mathcal{S}$ es una relación en B. Se define la relación $\mathcal{R}$ en A de la siguiente manera:

$$\mathcal{R} = \{(x, y) \in A \times A \ : \ \big(f(x), f(y)\big) \in \mathcal{S}\}.$$

Pruebe que:

- si $\mathcal{S}$ es reflexiva, entonces $\mathcal{R}$ es reflexiva.
- si $\mathcal{S}$ es simétrica, entonces $\mathcal{R}$ es simétrica.
- si $\mathcal{S}$ es transitiva, entonces $\mathcal{R}$ es transitiva.

Lección *veinte*

Definiciones recursivas

Hasta aquí hemos visto la importancia, la precisión y el papel que juegan las definiciones en las matemáticas. Sin embargo, no todos los conceptos que hemos usado en estas notas se han definido con toda precisión. En tales casos hemos acudido a la intuición que los estudiantes han construido desde sus primeros años de estudio. Algunos de esos conceptos son, por ejemplo, la adición o la multiplicación de números, la potenciación, la suma de finitos números, etc.

En esta lección vamos a restringirnos inicialmente a presentar definiciones (con todo rigor para que no existan dudas o ambigüedades en su significado) de conceptos matemáticos sobre el conjunto de los números naturales. Como, intuitivamente por ahora, sabemos que el conjunto $\mathbb{N}$ de los números naturales es infinito, teniendo en cuenta un análisis similar al que hicimos cuando introdujimos la estrategia de demostración del *Principio de inducción matemática,* no podemos definir un concepto matemático sobre cada uno de los números naturales puesto que por más que deleguemos esta tarea de generación en generación nunca acabaremos. Entonces debemos ser prácticos y buscar una manera de construir, sin dejar de ser rigurosos, este tipo de definiciones. Aquí es donde aparece lo que denominamos *definiciones recursivas*. Pero ¿qué quiere decir *recursividad*? Según la RAE en una de sus definiciones, recursividad quiere decir: "Dicho especialmente de un proceso: que se aplica de nuevo al resultado de haberlo aplicado previamente". Esto describe de muy buena manera la construcción que realizaremos de las definiciones recursivas. Particularmente, para dar la definición de un concepto matemático que depende de un natural $n \neq 0$, aplicaremos cierta *receta* o *procedimiento* que se había aplicado para obtener la definición en sus naturales predecesores (usualmente aplicamos ese procedimiento en $n - 1$ pero veremos aquí algunas otras variantes). En cada una de esas definiciones tendremos que dar por *decreto* la definición en el primer número natural $n = 0$. En efecto, esto tiene mucho el sabor del *Principio de inducción matemática* que estudiamos en la Lección 9.

Antes de presentar rigurosamente el significado de las definiciones de conceptos matemáticos de forma recursiva, recordemos la noción de sucesión introducida en el Ejemplo 19.2.12 que nos ayudará a expresar de manera más simple esta noción de recursión.

20.1. Sucesiones

Sea A conjunto no vacío. Como sabemos, una *sucesión en A*, o una *sucesión de elementos de A*, es simplemente una función

$$s : \mathbb{N} \to A.$$

Escribiremos $s_n := s(n) \in A$, para cada $n \in \mathbb{N}$. Es costumbre denotar la sucesión s por el símbolo $(s_n)_{n\in\mathbb{N}} = (s_0, s_1, \cdots, s_n, \cdots)$ o $(s_n)_{n=0}^{\infty}$. Los elementos del $rango(s)$, esto es, los elementos s_n de A, son llamados los *términos* de la sucesión y así, para n fijo, s_n es llamado el n-ésimo término de la sucesión.

Ejemplo 20.1.1 (Sucesiones de conjuntos)**.** Para cada $n \in \mathbb{N}$, consideremos el conjunto

$$A_n := \{k \in \mathbb{N} \,:\, 0 \leq k \leq n\}.$$

En este caso podemos ver que

$$\begin{aligned} A : \mathbb{N} &\longrightarrow \mathscr{P}(\mathbb{N}) \\ n &\longmapsto A_n := \{k \in \mathbb{N} \,:\, 0 \leq k \leq n\}, \end{aligned}$$

para cada $n \in \mathbb{N}$, es una sucesión de conjuntos de $\mathscr{P}(\mathbb{N})$, $(A_n)_{n\in\mathbb{N}}$ con índices en $\mathbb{N}$. Notemos que el rango de esta sucesión corresponde a la familia indexada de conjuntos $\{A_n\}_{n\in\mathbb{N}}$, ver Definición 12.1.1.

No sobra decir que en este caso

$$\bigcup_{n=0}^{\infty} A_n = \mathbb{N} \quad \text{y} \quad \bigcap_{n=0}^{\infty} A_n = \{0\}.$$

Ejemplo 20.1.2 (Sucesiones numéricas)**.** Consideremos la sucesión de números reales

$$(1, 2^{1/2}, 3^{1/3}, 4^{1/4}, \cdots).$$

Observamos que los términos de esta sucesión tienen la forma $x_n = n^{1/n}$, para cada $n \in \mathbb{Z}^{+} = \mathbb{N} - \{0\}$. En este caso, podemos hacer corresponder esta sucesión con la definición que presentamos de la siguiente manera

$$\begin{aligned} x : \mathbb{N} &\longrightarrow \mathbb{R} \\ n &\longmapsto x_n := (n+1)^{1/(n+1)}, \end{aligned}$$

para cada $n \in \mathbb{N}$. Sin embargo, por facilidad en la notación podemos reescribir esta sucesión de la siguiente manera:

$$\begin{aligned} x : \mathbb{Z}^+ &\longrightarrow \mathbb{R} \\ n &\longmapsto x_n := n^{1/n} \end{aligned}$$

para cada $n \in \mathbb{Z}^+$.

Esto lo podremos hacer debido a que, como podemos ver en este ejemplo, lo realmente importante en una sucesión no es su dominio sino su rango.

Note que los términos de una sucesión no necesariamente son distintos.

Ejemplo 20.1.3 (Sucesión constante). Sea $c \in \mathbb{R}$ fijo. Para cada $n \in \mathbb{N}$, consideremos la sucesión de números reales $s : \mathbb{N} \to \mathbb{R}$ dada por $s_n := c$, para todo $n \in \mathbb{N}$. Esta sucesión $(c, c, \cdots, c, \cdots)$ es conocida como sucesión *constante*. En este caso, $rango(s) = \{c\}$.

20.2. Recursión

Con el propósito de motivar las definiciones de conceptos matemáticos usando recursión, veamos cómo podemos definir rigurosamente la multiplicación de dos números naturales arbitrarios. Fijemos un número natural cualquiera k. Intuitivamente, para cualquier n número natural, desde nuestros primeros años de primaria sabemos que $k \cdot n$ corresponde a sumar n veces el número k. Pero, ¿cómo formalizamos esto? Comenzamos por definir el significado de $k \cdot n$ en el caso en que $n = 0$. Esto lo hacemos por *decreto* y nos da, lo que llamaremos, la *condición inicial* de nuestra definición. Como queremos que $k \cdot 0$ corresponda exactamente a sumar 0 veces el número k, lo natural es definir $k \cdot 0$ como 0 (sin importar k). Habiendo definido así $k \cdot 0$, procedemos a definir $k \cdot n$ en el caso en que $n = 1$. En este caso, $k \cdot 1$ debería corresponder a sumarle k a lo que ya teníamos (que era $k \cdot 0$), es decir, debemos definir $k \cdot 1 := k \cdot 0 + k = 0 + k = k$. Si seguimos con esta idea, $k \cdot 2$ corresponderá a sumarle k a lo que ya teníamos (que era $k \cdot 1$), es decir, $k \cdot 2 := k \cdot 1 + k = k + k$, y continuamos así sucesivamente. Notemos que en la definición de $k \cdot n$, para k fijo y $n \neq 0$ natural, hay un *patrón* puesto que realizamos siempre el mismo proceso, que es, sumar k a lo que ya teníamos definido previamente.

Pero, ¿cómo garantizar que podemos dar esta definición en cada uno de los números naturales? Más precisamente, ¿cómo garantizar que podemos dar esta definición sin tener que hacerla natural por natural (lo cual nunca acabaríamos de hacer, dado que el conjunto de los números naturales es infinito), pero de forma tal que quedemos convencidos de que efectivamente hicimos dicha definición cubriendo todos y cada uno de los números naturales?

La respuesta concreta a esta pregunta está en el siguiente teorema que nos permitirá hacer este tipo de definiciones. En general, como pudimos ver en el caso de la multiplicación de dos naturales arbitrarios, las definiciones recursivas están basadas en dos puntos claves que son: la condición inicial (definición en 0) y la identificación de un patrón que determina el *proceso* o *procedimiento* que nos permite dar la definición para cualquier natural no nulo (i.e., que tiene la forma $n + 1$ para $n \in \mathbb{N}$, que son llamados *números sucesores*).

Definición 20.2.1 (Procedimiento). Dado un conjunto A no vacío, un *procedimiento* en A es una función $g : \mathbb{N} \times A \to A$.

Note que para poder aplicar el siguiente teorema debemos siempre identificar tres ingredientes que son: A conjunto no vacío, $a \in A$ que determina la condición inicial y el procedimiento $g : \mathbb{N} \times A \to A$.

Teorema 20.2.2 (Definiciones recursivas en $\mathbb{N}$). *Sean A un conjunto no vacío, a un elemento fijo de A y $g : \mathbb{N} \times A \to A$ un procedimiento en A. Entonces existe una única sucesión $s : \mathbb{N} \to A$ que cumple las siguientes condiciones:*

- $s_0 := a$ *(condición inicial),*
- $s_{n+1} := g(n, s_n)$, *para todo* $n \in \mathbb{N}$ *(condición recursiva).*

Es decir, el $(n+1)$*-ésimo elemento de la sucesión s corresponde a aplicar el procedimiento g a n y al n-ésimo término,* s_n*, de esta sucesión.*

Aquí no demostraremos este teorema: su prueba es un poco laboriosa para el nivel del curso (de todas maneras, se demostrará con lujo de detalles en el curso Introducción a la Teoría de Conjuntos; aquellos lectores curiosos pueden consultar textos como [6]), por lo que preferimos omitirla y más bien centrarnos en ejemplos de cómo utilizarlo para dar definiciones recursivas.

Por ahora, supondremos que ya hemos definido la suma de naturales[1] y las propiedades que satisface (conmutatividad, asociatividad y que 0 es el neutro de la suma de naturales). Hacemos este supuesto por ahora en estas notas dado que no es nuestro objetivo construir completamente el sistema de los números naturales a la luz de la axiomática de Peano, y menos de axiomáticas de la Teoría de conjuntos como la de Zermelo-Fraenkel; solo pretendemos hacer algunos ejemplos de definiciones recursivas a nivel básico.

20.2.1. Multiplicación de naturales

Ejemplo 20.2.3. Formalizando la motivación que hicimos para introducir las *definiciones recursivas*, utilicemos el Teorema 20.2.2 para mostrar cómo podemos dar esta definición. Fijemos de antemano un número natural k cualquiera. Tomemos los siguientes tres ingredientes: $A := \mathbb{N}$, $a := 0$, que determina nuestra *condición inicial*, esto es, el 0-ésimo elemento de nuestra sucesión, y tomemos nuestro *procedimiento* g en $\mathbb{N}$, esto es, $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, dado por $g(n, b) := b + k$ para cualesquiera $n, b \in \mathbb{N}$. Note que g es constante respecto a n y b representa el término anterior de la sucesión que se supone ya fue definido. Además, el procedimiento g aparece de la identificación del *patrón* encontrado en el análisis descrito en la introducción

[1] Para construir rigurosamente la definición de adición de números naturales requerimos conceptos como el de *número natural* o *sucesor de un número* que serán estudiados en cursos como Sistemas Numéricos e Introducción a la Teoría de Conjuntos.

de esta sección el cual consiste en sumar k a lo que ya tengamos por definición en el paso previo, sin depender de n. El procedimiento g es clave en la determinación de la *condición recursiva*.

Por lo tanto, aplicando el Teorema 20.2.2, existe una única sucesión $K : \mathbb{N} \to \mathbb{N}$ que cumple las siguientes condiciones:

- $K_0 := a = 0$ (condición inicial),
- $K_{n+1} := g(n, K_n) = K_n + k$, para todo $n \in \mathbb{N}$ (condición recursiva).

De este modo, denotando $k \cdot n := K_n$, obtenemos que

- $k \cdot 0 := 0$,
- $k \cdot (n + 1) = k \cdot n + k$, para todo $n \in \mathbb{N}$.

Note que la existencia y unicidad de la función $K : \mathbb{N} \to \mathbb{N}$ garantiza que $k \cdot n$ está definido para cualquier natural n. Como k es fijo pero representa a cualquier natural, esto nos da la definición de $k \cdot n$ para cualesquiera k y n números naturales. En otras palabras, hemos definido recursivamente multiplicar k a cualquier número natural n.

Definición 20.2.4. Sea $k \in \mathbb{N}$ cualquiera pero fijo. Para $n \in \mathbb{N}$ arbitrario definimos recursivamente la multiplicación de k por n de la siguiente manera:

- $k \cdot 0 := 0$,
- $k \cdot (n + 1) = k \cdot n + k$, para todo $n \in \mathbb{N}$.

Ahora que hemos definido recursivamente el *producto* o *multiplicación* entre números naturales podemos demostrar algunas de sus propiedades, utilizando el *Principio de inducción matemática*, como se ve a continuación:

Lema 20.2.5. *Para todo natural n tenemos que $n \cdot 0 = 0 \cdot n = 0$.*

Antes de empezar la demostración de este hecho, observemos que por la condición inicial de la definición recursiva del producto entre naturales, $n \cdot 0 := 0$ para todo $n \in \mathbb{N}$. Así, este lema se reduce a demostrar que para todo natural n vale que $0 \cdot n = 0$. *Demostración.* Razonaremos usando el *Principio de inducción matemática forma I* (Hecho 9.1.1). Consideremos la siguiente propiedad:

$$P(x) : \text{“}0 \cdot x = 0\text{”}.$$

Esta propiedad está dada por el predicado $P(x)$ con variable x.

1. Tomando $k := 0$ en la definición recursiva del producto o multiplicaciónen el Ejemplo 20.2.3, de la condición inicial vemos que, $k \cdot 0 = 0 \cdot 0 := 0$. Luego, concluímos que $P(0)$ es verdadera.

2. Sea n cualquier natural fijo. Supongamos que $P(n)$ es verdadera, es decir, $0 \cdot n = 0$ (*hipótesis de inducción*). Por lo tanto, usando la definición recursiva de multiplicar 0 a cualquier natural (tome $k := 0$ en Ejemplo 20.2.3 y aplique la condición recursiva), tenemos que
$$0 \cdot (n + 1) = 0 \cdot n + 0.$$
Como $0 \cdot n = 0$ (*hipótesis de inducción*) y puesto que 0 es el neutro de la suma de naturales, entonces $0 \cdot (n + 1) = 0 + 0 = 0$. Por lo tanto, $P(n + 1)$ es verdadera.

Por el *Principio de inducción matemática forma I* (Hecho 9.1.1) tenemos que para todo $n \in \mathbb{N}$ la proposición $P(n)$ es verdadera, es decir, $0 \cdot n = 0$. ☑

A continuación enunciaremos una afirmación que utilizaremos en la demostración de la conmutatividad del producto en $\mathbb{N}$.

Hecho 20.2.6. *Para cualesquiera naturales l, k tenemos que* $(k + 1) \cdot l = (k \cdot l) + l$.

La demostración del hecho anterior lo dejamos como ejercicio para el lector (sugerencia: utilice el *Principio de inducción matemática forma I* para la propiedad $P(x)$: “para todo natural k se tiene que $(k+1) \cdot x = k \cdot x + x$”). Esta afirmación tenemos que demostrarla, puesto que la definición recursiva del producto entre naturales involucra naturales de la forma $k + 1$ al lado derecho del producto y aún no hemos demostrado la conmutatividad del producto entre naturales.

Ahora, podemos demostrar la conmutatividad del producto en los naturales.

Proposición 20.2.7 (Conmutatividad del producto de naturales). *Para todo natural m y n tenemos que $m \cdot n = n \cdot m$.*

Demostración. Consideremos la siguiente propiedad:

$P(x)$: "para todo natural m tenemos que $m \cdot x = x \cdot m$".

1. Sea m número natural arbitrario pero fijo. Del Lema 20.2.5, tenemos que $m \cdot 0 = 0 = 0 \cdot m$. Por lo tanto, tenemos que la proposición $P(0)$ es verdadera.

2. Supongamos que para cualquier natural fijo n tenemos que $P(n)$ es verdadera, es decir, para todo natural m tenemos que $m \cdot n = n \cdot m$ (*hipótesis de inducción*). Sea m natural arbitrario pero fijo. Así,

$$\begin{aligned} m \cdot (n+1) &= (m \cdot n) + m \\ &\quad \text{(tomando } k := m\text{, definición recursiva de} \\ &\quad \text{producto entre naturales, Ejemplo 20.2.3)} \\ &= (n \cdot m) + m \\ &\quad \text{(hipótesis de inducción, } m \cdot n = n \cdot m\text{)} \\ &= (n+1) \cdot m \\ &\quad \text{(Hecho 20.2.6, tomando } k := n \text{ y } l := m\text{)} \end{aligned}$$

Por lo tanto, la proposición $P(n+1)$ es verdadera.

De esta manera, por el *Principio de inducción matemática forma I* tenemos que para todo $n \in \mathbb{N}$ la proposición $P(n)$ es verdadera, es decir, para todo $n \in \mathbb{N}$ vale que para cualquier $m \in \mathbb{N}$ tenemos que $m \cdot n = n \cdot m$. ☑

Otras propiedades del producto de números naturales pueden ser demostradas de la misma forma. Vea los Ejercicios 20.3.1, 20.3.2 y 20.3.3.

20.2.2. Potenciación de naturales

Ejemplo 20.2.8 (Potenciación de naturales). Como un segundo ejemplo, daremos la definición *recursiva* de la potenciación de números naturales. Fijemos m número natural arbitrario. Definiremos lo que significa la potencia m^n para cualquier n natural, la cual intuitivamente corresponde a multiplicar n veces el número m. Tomemos los tres ingredientes $A := \mathbb{N}$, $a := 1$ y el procedimiento en $\mathbb{N}$, $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definido para cualesquiera $n, b \in \mathbb{N}$ por $g(n, b) := b \cdot m$. Así, en virtud del Teorema 20.2.2 existe una única función $M : \mathbb{N} \to \mathbb{N}$ (donde denotaremos $m^n := M_n$) tal que

- $m^0 = M_0 := a = 1$ (*condición inicial*: para todo $m \in \mathbb{N}$ fijo definimos por "decreto" $m^0 := 1$, sin importar si m es cero o no[2]),
- $m^{n+1} = M_{n+1} := g(n, M_n) = M_n \cdot m = (m^n) \cdot m$, para todo $n \in \mathbb{N}$ (*condición recursiva*: m^{n+1} corresponde a multiplicarle m a la definición en el paso previo que corresponde a m^n).

Definición 20.2.9. Sea $m \in \mathbb{N}$ cualquiera pero fijo. Para $n \in \mathbb{N}$ arbitrario definimos recursivamente la potenciación de números naturales m^n de la siguiente manera:

- $m^0 := 1$,
- $m^{n+1} = m^n \cdot m$, para todo $n \in \mathbb{N}$.

Lema 20.2.10. *Para todo natural n tenemos que $1^n = 1$.*

Demostración. Consideremos la siguiente propiedad:

$$P(x) : \text{“}1^x = 1\text{”}.$$

Note que $P(x)$ es un predicado con variable x.

1. Tomando $m := 1$, por la definición recursiva de potenciación entre naturales (condición inicial en Ejemplo 20.2.8) tenemos que $1^0 := 1$. Luego, $P(0)$ es verdadera.
2. Supongamos que para cualquier $n \in \mathbb{N}$ fijo tenemos que $P(n)$ es verdadera, es decir, $1^n = 1$ (*hipótesis de inducción*). Entonces, por la definición recursiva de potenciación (condición recursiva en Ejemplo 20.2.8 tomando $m := 1$) tenemos que $1^{n+1} = 1^n \cdot 1$. Aplicando el Ejercicio 20.3.1, tomando m como 1^n, vemos que

[2]Cuando hablemos de *conjuntos de funciones* y su cardinal, más adelante, veremos que 0^0 tiene sentido y realmente se puede definir como 1.

$1^n \cdot 1 = 1^n$. Finalmente, aplicando la hipótesis de inducción obtenemos que

$$1^{n+1} = 1^n \cdot 1 = 1^n = 1.$$

Por lo tanto, $P(n+1)$ es verdadera.

Por el *Principio de inducción matemática forma I* (Hecho 9.1.1) concluímos que $1^n = 1$ es verdadera para todo $n \in \mathbb{N}$. ☑

20.2.3. Factorial

Intuitivamente, dado $n \in \mathbb{N} - \{0\}$, el factorial de n (denotado por $n!$) se define informalmente como el producto de multiplicar todos los naturales k tales que $1 \leq k \leq n$. Con el propósito de dar la definición rigurosa del factorial de cualquier natural, primero que todo, definimos por decreto la condición inicial $0! := 1$. Según la noción anterior, $1!$ debe ser 1, que corresponde a $1! = 1 = 0! \cdot (0+1)$. Así mismo, $2! := 1 \cdot 2 = 1! \cdot (1+1)$. Continuando con esta intuición, vemos que $3! := 1 \cdot 2 \cdot 3 = (1 \cdot 2) \cdot (2+1) = 2! \cdot (2+1)$. Esto nos permite identificar el patrón, para calcular $(n+1)!$ mediante la noción presentada, el cual consiste en multiplicar $n!$ por $(n+1)$. Por lo tanto, el procedimiento $g : \mathbb{N} \times A \to A$ que debemos considerar para esta definición recursiva está dada por $g(n, b) := b \cdot (n+1)$, con $n \in \mathbb{N}$ y $b \in A := \mathbb{N}$. Observe que, en este caso, el procedimiento g no es constante respecto a n como en los ejemplos vistos anteriormente (producto y potenciación de naturales) en los que g no dependía de n sino únicamente de b.

Para definir rigurosamente el factorial de cualquier natural, consideramos los tres ingredientes, que son: $A := \mathbb{N}$, $a := 1 \in A$ y $g : \mathbb{N} \times A \to A$ definida por $g(n, b) := b \cdot (n+1)$ para cualesquiera $n \in \mathbb{N}$ y $b \in A$. Entonces, por el Teorema 20.2.2, existe una única sucesión $F : \mathbb{N} \to \mathbb{N}$ (donde denotaremos $n! := F_n$) tal que

- $0! := F_0 := 1$ *(condición inicial)*,

- $(n+1)! := F_{n+1} = g(n, F_n) = F_n \cdot (n+1) = n! \cdot (n+1)$ para cualquier $n \in \mathbb{N}$ *(condición recursiva)*.

Definición 20.2.11. Sea $n \in \mathbb{N}$ cualquiera pero fijo. Definimos recursivamente el factorial de números naturales $n!$ de la siguiente manera:

- $0! := 1$,
- $(n+1)! := n! \cdot (n+1)$, para todo $n \in \mathbb{N}$.

De esta manera, hemos demostrado la existencia de la función factorial definida en los números naturales.

20.2.4. Sumatoria de números reales

Otro ejemplo de definición recursiva es la que se da para aclarar el significado de sumar finitos números. Seguramente los estudiantes han visto en cursos como Cálculo Diferencial que la suma de números reales es una *operación binaria*; es decir, solo sumamos parejas de números reales. Sin embargo, si tenemos x_0, x_1, x_2 números reales, podemos considerar la suma de estos tres números $x_0 + x_1 + x_2$ porque la podemos interpretar como $(x_0 + x_1) + x_2$ o como $x_0 + (x_1 + x_2)$ debido a que la suma de reales es asociativa (ver apéndice). Pero si tenemos $x_0, \cdots, x_n$ números reales, ¿cómo definir de manera rigurosa la suma $x_0 + \cdots + x_n$? Además, esta notación tiene un "peligro" pues los puntos suspensivos "$\cdots$" podrían hacer que dicha notación se interprete de diferentes maneras. Introducimos el símbolo $\sum_{k=0}^{n} x_k$ para denotar la suma de los números $x_0 + \cdots + x_n$. Esta notación que es más compacta es conocida como notación de *sumatoria*. Nuestro propósito es construir una definición del símbolo $\sum_{k=0}^{n} x_k$ para cada $n \in \mathbb{N}$ de manera rigurosa, es decir, que no lleve a ambigüedades, y que corresponda a la noción de sumar todos los números $x_0, \cdots, x_n$. Para hacer esto usamos recursión.

Definición 20.2.12 (Sumatoria)**.** Dada una sucesión de números reales $(x_k)_{k \in \mathbb{N}}$, para cada natural n, definimos recursivamente $\sum_{k=0}^{n} x_k$ de la siguiente manera:

- $\sum_{k=0}^{0} x_k := x_0$ (*condición inicial*),
- Suponiendo que hemos definido $\sum_{k=0}^{n} x_k$, definimos $\sum_{k=0}^{n+1} x_k := \left(\sum_{k=0}^{n} x_k\right) + x_{n+1}$ para cada $n \in \mathbb{N}$ (*condición recursiva*).

La forma como acabamos de presentar esta definición recursiva de sumatoria es muy usual pero no muestra cómo se aplicó el Teorema 20.2.2. Aclarar esto es un muy buen ejercicio para el lector el cual consiste esencialmente en identificar los tres ingredientes que nos permiten aplicar el teorema. En este caso, elegimos el conjunto no vacío $A := \mathbb{R}$, $a := x_0$, el primer elemento de la sucesión $(x_k)_{k\in\mathbb{N}}$, elemento fijo de $\mathbb{R}$, y un procedimiento $g : \mathbb{N} \times A \to A$. Esto nos garantizará, por el Teorema 20.2.2, que existe una única sucesión $s : \mathbb{N} \to \mathbb{R}$ tal que, para todo $n \in \mathbb{N}$, se tiene que $\sum_{k=0}^{n} x_k := s_n$.[3] Dejamos como ejercicio para el lector determinar cuál es el procedimiento g que debemos considerar en este ejemplo.

20.2.5. Sucesión de Fibonacci

La versión que hemos trabajado hasta ahora de definiciones recursivas permite definir una sucesión $F : \mathbb{N} \to A$ donde $F_{n+1} := F(n+1)$ depende de la definición hecha en el predecesor inmediato F_n . De esta manera, debemos dar solo una condición inicial para definir F_0. Pero también tenemos variantes en los que la definición F_n $(n \geq 2)$ va a depender de la definición de los predecesores $F_{n-k}, \cdots, F_{n-1}$ $(k \geq 2)$, en cuyo caso debemos dar condiciones iniciales para $F_0, \cdots, F_{k-1}$.

Como caso particular, tomemos $k := 2$ y $A := \mathbb{N}$. Tomando como condiciones iniciales $F_0 := 1$ y $F_1 := 1$ y para $n \geq 2$ definimos $F_n := F_{n-2} + F_{n-1}$, la sucesión $(F_n)_{n\in\mathbb{N}}$ definida de esta manera se conoce como *sucesión de Fibonacci*. Como ilustración, vemos que F_2 es definida recursivamente como $F_2 := F_0 + F_1 = 1 + 1 = 2$ y $F_3 := F_1 + F_2 = 1 + 2 = 3$.

Este tipo de definiciones es garantizada por un teorema más general que el Teorema 20.2.2 el cual es demostrado en cursos más avan-

[3]Esta nueva sucesión $(s_n)_{n\in\mathbb{N}}$ es llamada *sucesión de sumas parciales*, o *serie*, correspondiente a la sucesión dada $(x_k)_{k\in\mathbb{N}}$.

zados como Introducción a la Teoría de Conjuntos. Aquellos lectores curiosos pueden encontrar esta demostración en libros como [1].

20.3. Ejercicios

Ejercicio 20.3.1. Demuestre que para todo natural m tenemos que $m \cdot 1 = 1 \cdot m = m$.

Ejercicio 20.3.2 (Asociatividad del producto entre naturales). Demuestre que para cualesquiera naturales m, n, k tenemos que $(m \cdot n) \cdot k = m \cdot (n \cdot k)$ (sugerencia: realice un argumento inductivo sobre la variable k).

Ejercicio 20.3.3 (Distributividad del producto con respecto a la suma de naturales). Demuestre que para cualesquiera naturales m, n, k tenemos que $m \cdot (n + k) = (m \cdot n) + (m \cdot k)$ (sugerencia: realice un argumento inductivo sobre la variable k).

Ejercicio 20.3.4. Demuestre que para cualesquiera naturales m, n, k tenemos que $k^m \cdot k^n = k^{m+n}$ (sugerencia: realice un argumento inductivo sobre la variable n).

Ejercicio 20.3.5. Demuestre que para cualesquiera naturales m, n, k tenemos que $(k^m)^n = k^{m \cdot n}$ (sugerencia: realice un argumento inductivo sobre la variable n).

Ejercicio 20.3.6. Determine explícitamente el procedimiento $g : \mathbb{N} \times \mathbb{R} \to \mathbb{R}$ para poder definir recursivamente la sumatoria $\sum_{k=0}^{n} x_k$ (Definición 20.2.12).

Ejercicio 20.3.7. Demuestre que para toda sucesión de números reales $(a_k)_{k \in \mathbb{N}}$, para todo número natural n y todo real c tenemos que $c \cdot \sum_{i=0}^{n} a_i = \sum_{i=0}^{n} (c \cdot a_i)$.

Ejercicio 20.3.8. Dada una sucesión de números reales $(a_k)_{k \in \mathbb{N}}$, para cada número natural n defina recursivamente $\prod_{i=0}^{n} a_n$ (que intuitivamente sería el producto $a_0 \cdot \ \ldots \ \cdot a_n$).

Ejercicio 20.3.9. Demuestre que para cualquier sucesión de números naturales $(a_k)_{k\in\mathbb{N}}$ (que en particular es una sucesión de números reales) y todo número natural k tenemos que $\prod_{i=0}^{n} k^{a_i} = k^{\sum_{i=0}^{n} a_i}$ (sugerencia: haga un argumento inductivo sobre la variable n).

Ejercicio 20.3.10. Sean $n, r \in \mathbb{N}$, con $0 \leq r \leq n$, y A un conjunto con n elementos distintos. Una *combinación* de A es simplemente un subconjunto de A. Una r-combinación de A es un subconjunto de A con r elementos. El número de r-combinaciones de un conjunto de n elementos es denotado por $\binom{n}{r}$ y corresponde, más precisamente, al número:

$$\binom{n}{r} = \frac{n!}{r!\,(n-r)!}.$$

Pruebe que

1. $\binom{n}{r} = \binom{n}{n-r}$,
2. $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$,
3. $\binom{n}{r} = \frac{n}{r}\binom{n-1}{r-1}$, siempre que $r \geq 1$.

Lección
veintiuno
Imágenes directa y recíproca

Consideremos de nuevo el conjunto de todas las personas P y la función F que asigna a cada persona x su fecha de nacimiento. Esta función contiene información que nos puede interesar como por ejemplo, si tenemos un interés histórico, las fechas de nacimiento de las mujeres matemáticas, o si tenemos un interés menos académico, las fechas de nacimiento de todos los deportistas que han estado en algunos juegos olímpicos representando nuestro país. Denotemos por M el conjunto de todas las mujeres matemáticas. Claramente todas las mujeres matemáticas son personas, esto es $M \subset P$. El conjunto de todas las fechas de nacimiento de las mujeres matemáticas puede ser escrito en notación de conjunto como

$$\begin{aligned}&\{y \in codom(F) \ : \ y = F(x) \text{ para algún } x \in M\}\\ &= \{F(x) \ : \ x \in M\} \subset codom(F).\end{aligned}$$

Lo que se está haciendo aquí es tomar un subconjunto del dominio de la función F, en este caso M conformado por todas las mujeres matemáticas, y determinar el correspondiente subconjunto del codominio cuyos elementos son exactamente todas las fechas de nacimiento de las mujeres matemáticas, es decir, las imágenes por la función F de cada $x \in M$.

Dado que la función F posee tanta información también puede ser muy interesante saber, por ejemplo, si hubo mujeres matemáticas nacidas antes del año 1500. Para mayor facilidad consideremos la función $G = F|_M$ que tiene dominio M y que simplemente asigna a cada mujer matemática su fecha de nacimiento. Ahora debemos ver cuáles son las mujeres matemáticas nacidas antes de 1500. Esta búsqueda nos determina un subconjunto del codominio de G, digamos Q, en el que están todas las fechas antes del año 1500. Así mismo, el subconjunto de $M = dom(G)$ correspondiente a todas las mujeres matemáticas que tienen fecha de nacimiento en Q será $\{x \in M \mid G(x) \in Q\} \subset M$. En resumen, tomamos un subconjunto Q del codominio de G y determinamos el correspondiente subconjunto de su dominio M conformado por todas las mujeres matemáticas con fecha de nacimiento en Q, es decir, nacidas antes del año 1500. Alguien podría pensar que $\{x \in M \mid G(x) \in Q\}$ es vacío, es decir, que no hubo mujeres matemáticas nacidas antes del año 1500, pero no es así. Es sabido que Hipatia nació alrededor del año 360 en Alejandría, Egipto. Aunque no sabemos su fecha de nacimiento con precisión, en nuestro ejemplo tenemos que $G(Hipatia) \in Q$, es decir la fecha de nacimiento de Hipatia fue antes del año 1500. Las Definiciones 21.1.1 y 21.2.1 generalizan los conjuntos descritos anteriormente.

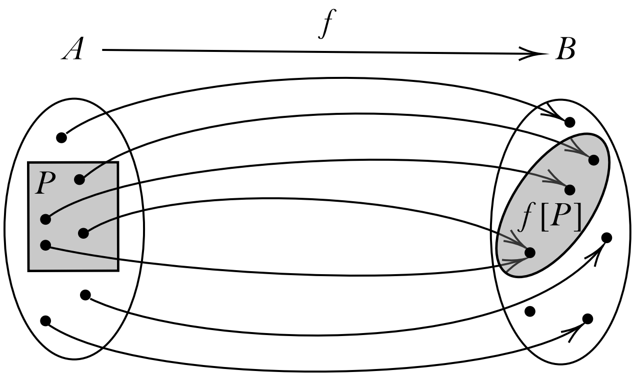
21.1. Imagen directa

Definición 21.1.1 (Imagen directa)**.** Sean $f : A \longrightarrow B$ una función y $P \subseteq A$. La *imagen directa* de P bajo f, denotada por $f[P]$, es el conjunto definido por

$$f[P] = \{b \in B : b = f(p) \text{ para algún } p \in P\}.$$

Observación 21.1.2. Sea $f : A \longrightarrow B$ una función. Note que el rango de f, que también es llamado imagen de f, es el conjunto $f[A]$.

La siguiente figura muestra una representación de la imagen directa de un conjunto $P \subseteq A$, bajo una función $f : A \longrightarrow B$, mediante un diagrama de flechas.



Una manera relajada de describir este conjunto $f[P]$ que aparece en la Definición 21.1.1 es

$$f[P] = \{f(p) : p \in P\}.$$

Ejemplo 21.1.3. Consideremos de nuevo la función parte entera que hemos estudiado en los Ejemplos 19.2.11 y 19.4.3,

$$\begin{aligned} f = \lfloor\cdot\rfloor : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \lfloor x \rfloor = n, \end{aligned}$$

donde n es el mayor de los números enteros menores o iguales a x. Por la Definición 21.1.1, vemos que la imagen directa del intervalo abierto $(1/2, 3/2)$, bajo la función $f = \lfloor\cdot\rfloor$, es:

$$\begin{aligned} f[(1/2, 3/2)] &= \{n \in \mathbb{Z} \,:\, \lfloor x \rfloor = n \text{ para algún } x \in (1/2, 3/2)\} \\ &= \{0, 1\}, \end{aligned}$$

porque el mayor de los números enteros menores o iguales a cualquiera de los números reales $x \in (1/2, 1)$ es 0, es decir $\lfloor x \rfloor = 0$ para todo $x \in (1/2, 1)$, y el mayor de los números enteros menores o iguales a cualquiera de los números reales $x \in [1, 3/2)$ es 1, en otras palabras $\lfloor x \rfloor = 1$ para todo $x \in [1, 3/2)$. También podemos ver que la imagen directa del intervalo cerrado $[0, 3]$, bajo la función $f = \lfloor\cdot\rfloor$, es:

$$f\big[[0, 3]\big] = \{n \in \mathbb{Z} \,:\, \lfloor x \rfloor = n \text{ para algún } x \in [0, 3]\} = \{0, 1, 2, 3\},$$

porque $\lfloor x \rfloor = 0$ para todo $x \in [0, 1)$, $\lfloor x \rfloor = 1$ para todo $x \in [1, 2)$, $\lfloor x \rfloor = 2$ para todo $x \in [2, 3)$ y finalmente $\lfloor 3 \rfloor = 3$.

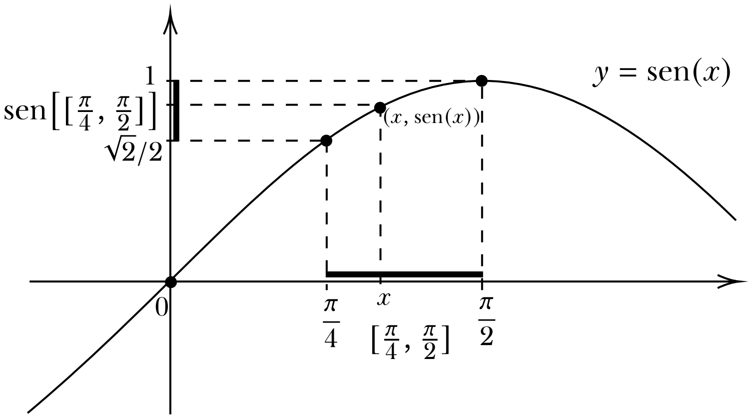
Ejemplo 21.1.4. Consideremos ahora la muy conocida función trigonométrica seno, denotada aquí simplemente por sen,

$$\begin{aligned} \operatorname{sen} : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \operatorname{sen}(x). \end{aligned}$$

Nuestro conocimiento de la función seno de los cursos de cálculo elemental nos permite afirmar que la imagen directa del intervalo cerrado $[\pi/4, \pi/2]$, bajo la función sen, es:

$$\begin{aligned} \operatorname{sen}\big[[\pi/4, \pi/2]\big] &= \{y \in \mathbb{R} \,:\, \operatorname{sen}(x) = y \text{ para algún } x \in [\pi/4, \pi/2]\} \\ &= \big[\sqrt{2}/2, 1\big], \end{aligned}$$

porque para todo $x \in [\pi/4, \pi/2]$, $\sqrt{2}/2 \leq \mathrm{sen}(x) \leq 1$. Para mayor claridad presentamos el siguiente gráfico de la función seno donde se pueden apreciar estos conjuntos



Otra notación ampliamente usada para $f[P]$, imagen directa de P bajo f, es simplemente "$f(P)$". No usamos esta notación debido a que escribir "$f(P)$" puede ser ambigüo porque se puede interpretar que la función f es evaluada en el subconjunto P, lo cual no tiene sentido, y se indicó que f solo debe evaluarse en elementos de su dominio y no en subconjuntos de él. Este es un ejemplo de lo que es referido como *abuso de notación*. Sin embargo, reconocer qué tipo de objeto está dentro del paréntesis en el símbolo: $f(\square)$, si $\square$ es subconjunto de $dom(f)$ o si $\square$ es elemento de $dom(f)$, no siempre es absolutamente claro. Consideremos la función $id_{\mathscr{P}(\varnothing)}$. Sabemos que $\varnothing \in \mathscr{P}(\varnothing)$ y $\varnothing \subseteq \mathscr{P}(\varnothing)$. Es decir, $\varnothing$ es elemento y subconjunto de $\mathscr{P}(\varnothing)$, por lo tanto, el término "$id_{\mathscr{P}(\varnothing)}(\varnothing)$" no es claro si se refiere a la función $id_{\mathscr{P}(\varnothing)}$ evaluada en el elemento $\varnothing$ o si se refiere a la imagen directa del subconjunto $\varnothing$ bajo la función $id_{\mathscr{P}(\varnothing)}$. No obstante, en algunos contextos, como lo son los cursos de cálculo y análisis, es posible reconocer de manera clara qué tipo de objeto está dentro del paréntesis en $f(\square)$. Esto nos permitirá entender a qué se refiere esta notación y, por lo tanto, esta manera de escribir no sería inconveniente de usar ni debería causar problemas. En los casos en los que esta notación genera ambigüedades se recurre al contexto para mantener con interpretación única al término "$f(P)$".

Exploremos una visión un poco más abstracta. Sea $f : A \longrightarrow B$ una función. Vimos que si $P \subseteq A$, entonces $f[P] \subseteq B$. Esto es, a cualquier elemento $P \in \mathcal{P}(A)$ le corresponde un elemento $f[P] \in \mathcal{P}(B)$. Por lo tanto, el proceso de tomar imágenes directas de subconjuntos arbitrarios de A tiene el efecto de inducir una nueva función a partir de la función f. Tal función es denotada por $f_* : \mathcal{P}(A) \longrightarrow \mathcal{P}(B)$ y es definida por $f_*(P) = f[P]$. Vale la pena mencionar que la notación "$f_*(P)$" no significa otra cosa que la imagen del elemento $P \in dom(f_*) = \mathcal{P}(A)$ por la función f_*.

Ejemplo 21.1.5. Consideremos la función f de $A = \{1, 2, 3\}$ en $B = \{a, e, i, o, u\}$ dada por

$$\begin{aligned} f : \{1, 2, 3\} &\longrightarrow \{a, e, i, o, u\} \\ 1 &\longmapsto u \\ 2 &\longmapsto a \\ 3 &\longmapsto u. \end{aligned}$$

Vemos que $f[\{1\}] = \{u\}$ porque el único elemento que está en $\{1\}$ es 1 y $f(1) = u$. Así mismo, $f[\{2\}] = \{a\}$ y $f[\{3\}] = \{u\}$. Como $f(1) = u$ y $f(3) = u$, consecuentemente $f[\{1, 3\}] = \{u\}$. También $f[\{1, 2\}] = \{a, u\}$. Vista como relación,

$$\begin{aligned} f_* =&\{(\varnothing, \varnothing), (\{1\}, \{u\}), (\{2\}, \{a\}), (\{3\}, \{u\}), (\{1, 2\}, \{a, u\}), \\ &(\{1, 3\}, \{u\}), (\{2, 3\}, \{a, u\}), (\{1, 2, 3\}, \{a, u\})\}. \end{aligned}$$

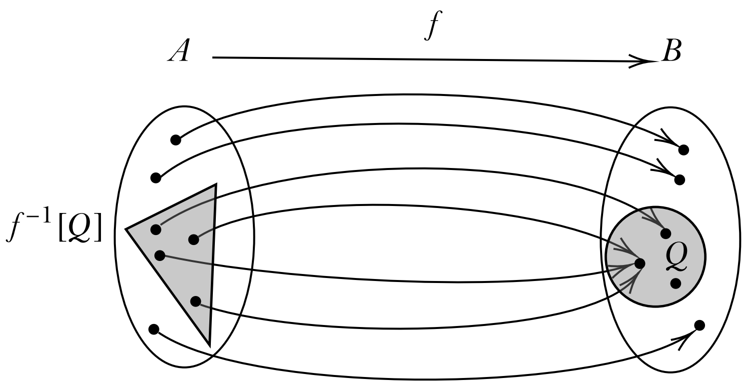
El hecho $f_*(\varnothing) = f[\varnothing] = \varnothing$ es válido para cualquier función f. Tal afirmación es enunciada en el Teorema 21.3.1.

21.2. Imagen recíproca

Definición 21.2.1. Sean $f : A \longrightarrow B$ una función y $Q \subseteq B$. La *imagen recíproca* de Q bajo f, denotada por $f^{-1}[Q]$, es el conjunto definido por

$$f^{-1}[Q] = \{a \in A : f(a) \in Q\}.$$

La siguiente figura muestra una representación mediante diagrama de flechas de la imagen recíproca de un conjunto $Q \subseteq B$ bajo la función $f : A \to B$.



Una forma alternativa de describir este conjunto que aparece en la Definición 21.2.1 es

$$f^{-1}[Q] = \{a \in A \,:\, f(a) = q \text{ para algún } q \in Q\}.$$

Ejemplo 21.2.2. Consideremos de nuevo la función parte entera

$$\begin{aligned} f = \lfloor\cdot\rfloor : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \lfloor x \rfloor = n, \end{aligned}$$

donde $n \in \mathbb{Z}$ satisface que $n \leq x < n+1$. Nótese que $f^{-1}[\{j\}] = [j, j+1)$ para cualquier $j \in \mathbb{Z}$ porque $\lfloor x \rfloor = j$ para cualquier $x \in [j, j+1)$ por la misma definición de la función $\lfloor\cdot\rfloor$, ver Ejemplo 19.2.11. También vale que $f^{-1}[(j, j+1)] = \varnothing$ para cualquier $j \in \mathbb{Z}$ porque $(j, j+1) \cap rango(\lfloor\cdot\rfloor) = \varnothing$.

Supongamos que deseamos determinar la imagen recíproca del intervalo abierto $(3/2, 5/2)$, bajo la función $f = \lfloor\cdot\rfloor$. Como $rango(\lfloor\cdot\rfloor) = \mathbb{Z}$, vea el Ejercicio 19.5.6, basta calcular la imagen recíproca del conjunto $(3/2, 5/2) \cap \mathbb{Z} = \{2\}$, así que $f^{-1}[(3/2, 5/2)] = f^{-1}[\{2\}] = [2, 3)$.

Puesto que tenemos que $(-1/2, 3] \cap \mathbb{Z} = \{0, 1, 2, 3\}$, podemos decir que $f^{-1}\big[(-1/2, 3]\big] = f^{-1}[\{0, 1, 2, 3\}] = [0, 4)$ porque para cualquier $x \in [0, 4)$ se cumple que $\lfloor x \rfloor = n$ donde $n \in \{0, 1, 2, 3\}$.

Ejemplo 21.2.3. Respecto a la función seno considerada en el Ejemplo 21.1.4 se tiene que la imagen recíproca del intervalo cerrado $\big[\sqrt{2}/2, 1\big]$, por Definición 21.2.1, corresponde al conjunto

$$\operatorname{sen}^{-1}\big[[\sqrt{2}/2, 1]\big] = \{x \in \mathbb{R} \,:\, \operatorname{sen}(x) \in [\sqrt{2}/2, 1]\}.$$

Note que el intervalo $\big[\pi/4, 3\pi/4\big] \subset \operatorname{sen}^{-1}\big[[\sqrt{2}/2, 1]\big]$ porque para todo $x \in \big[\pi/4, 3\pi/4\big]$ se cumple que $\operatorname{sen}(x) \in [\sqrt{2}/2, 1]$. Sin embargo, existen otros $x \in \mathbb{R}$ que también cumplen esta condición porque la función seno es una función periódica de periodo 2π, es decir

$$\operatorname{sen}(x + 2\pi) = \operatorname{sen}(x) \quad \text{para todo} \quad x \in \mathbb{R}.$$

Por lo tanto, para todo $x \in \big[\pi/4 \pm 2\pi, 3\pi/4 \pm 2\pi\big]$ se cumple que $\operatorname{sen}(x) \in [\sqrt{2}/2, 1]$ y para todo $x \in \big[\pi/4 \pm 4\pi, 3\pi/4 \pm 4\pi\big]$ vale que $\operatorname{sen}(x) \in [\sqrt{2}/2, 1]$ y así sucesivamente. Más precisamente, para cualquier $k \in \mathbb{Z}$ se tiene que para todo $x \in \big[\pi/4 + 2k\pi, 3\pi/4 + 2k\pi\big]$ es válido que $\operatorname{sen}(x) \in [\sqrt{2}/2, 1]$. Esto implica que

$$\operatorname{sen}^{-1}\big[[\sqrt{2}/2, 1]\big] = \bigcup_{k \in \mathbb{Z}} \big[\pi/4 + 2k\pi, 3\pi/4 + 2k\pi\big].$$

Desafortunadamente, no se puede decir que la notación “$f^{-1}[Q]$” no causa problemas. En efecto, si una función $f : A \longrightarrow B$ tiene una función inversa respecto a la composición de funciones (esto será estudiado en la próxima lección) entonces la función inversa será denotada por $f^{-1} : B \longrightarrow A$ y así el término “$f^{-1}[Q]$” tendrá dos significados. Un significado es el que hemos estado estudiando que es la imagen recíproca de $Q \subseteq B$ bajo f y el otro significado de $f^{-1}[Q]$ es que es la imagen directa de $Q \subseteq B$ bajo f^{-1}. El problema de fondo es que la función f^{-1} no siempre existe. Por lo tanto, es muy importante tener presente que la notación $f^{-1}[Q]$ no necesariamente significa la imagen directa de $Q \subseteq B$ bajo f^{-1} porque $f^{-1}[Q]$ es usado inclusive cuando no existe la función inversa de f. Adicionalmente, si la función f^{-1} existe, los dos significados para $f^{-1}[Q]$ coinciden.

Sean $f : A \longrightarrow B$ una función, $P \subseteq A$ y $Q \subseteq B$. Notemos que los términos "$f\left[f^{-1}[Q]\right]$" y "$f^{-1}\left[f[P]\right]$" tienen todo el sentido porque $Q \subseteq B$, $f^{-1}[Q] \subseteq A$ y, por lo tanto, la imagen directa de este subconjunto de A bajo la función f es $f\left[f^{-1}[Q]\right]$. Del mismo modo, $f^{-1}\left[f[P]\right]$ corresponde a la imagen recíproca del subconjunto $f[P]$ que está contenido en B porque $P \subseteq A$. En este contexto debemos tener mucha precaución porque no siempre es válido que $f\left[f^{-1}[Q]\right] = Q$ ni que $f^{-1}\left[f[P]\right] = P$. El siguiente ejemplo muestra porque no siempre es verdad.

Ejemplo 21.2.4. Sea $f : \mathbb{R} \longrightarrow \mathbb{R}$ la función definida por $f(x) = x^2$ para todo $x \in \mathbb{R}$. Se puede probar que $f[(0,2)] = (0,4)$ y $f^{-1}\left[f[(0,2)]\right] = f^{-1}[(0,4)] = (-2,0) \cup (0,2) \neq (0,2)$. Similarmente, como $f^{-1}[(-4,4)] = (-2,2)$,

$$\begin{aligned} f\left[f^{-1}[(-4,4)]\right] &= f[(-2,2)] \\ &= [0,4) \\ &\neq (-4,4). \end{aligned}$$

Ejemplo 21.2.5. Sea $f : \mathbb{R} \longrightarrow \mathbb{R}$ la función definida por $f(x) = x^4 - 2x^2$ para cualquier $x \in \mathbb{R}$. Se puede ver que $f\left[[-1,1]\right] = [-1,0]$ y que $rango(f) = f[\mathbb{R}] = [-1,+\infty)$. También se puede obtener que $f^{-1}\left[[0,4]\right] = \left[-\sqrt{1+\sqrt{5}}, -\sqrt{2}\right] \cup \left[\sqrt{2}, \sqrt{1+\sqrt{5}}\right] \cup \{0\}$ y que $f^{-1}\left[[-4,-2]\right] = \varnothing$. Los detalles de las pruebas de estas igualdades de conjuntos son dejadas como ejercicios para el lector.

Sea $f : A \longrightarrow B$ una función. Así como construimos la función $f_* : \mathscr{P}(A) \longrightarrow \mathscr{P}(B)$ basados en la imagen directa de cualquier subconjunto de A bajo f, a todo elemento $Q \in \mathscr{P}(B)$ le corresponde un único elemento $f^{-1}[Q] \in \mathscr{P}(A)$. Por lo tanto, este proceso de tomar imágenes recíprocas de subconjuntos de B tiene el efecto de inducir una nueva función denotada por $f^* : \mathscr{P}(B) \longrightarrow \mathscr{P}(A)$ a partir de la función f. Esta función f^* es definida por $f^*(Q) = f^{-1}[Q]$. Las funciones f_* y f^* nos permiten dar una mirada más abstracta a las imágenes directas y recíprocas de conjuntos bajo la función f pero en estas notas solo serán usadas en algunos ejercicios. Esta visión le permitirá a los estudiantes entender con mayor facilidad conceptos más abstractos que aparecen en cursos superiores como topología o teoría de la medida.

21.3. Propiedades

El siguiente teorema presenta algunas de las propiedades más básicas de las imágenes directas y recíprocas de funciones.

Teorema 21.3.1. *Sean A, B conjuntos, sean $P, S \subseteq A$ y $Q, T \subseteq B$ subconjuntos y sea $f : A \longrightarrow B$ una función. Sean J y K conjuntos no vacíos, sea $\{A_j\}_{j\in J}$ una familia de subconjuntos de A indexados por J, y sea $\{B_k\}_{k\in K}$ una familia de subconjuntos de B indexados por K. Entonces, valen las siguientes propiedades:*

1. $f[\varnothing] = \varnothing$ *y* $f^{-1}[\varnothing] = \varnothing$.
2. $f^{-1}[B] = A$.
3. $f[P] \subseteq Q$ *si y solo si* $P \subseteq f^{-1}[Q]$.
4. *Si* $P \subseteq S$, *entonces* $f[P] \subseteq f[S]$.
5. *Si* $Q \subseteq T$, *entonces* $f^{-1}[Q] \subseteq f^{-1}[T]$.
6. $f\left[\bigcup_{j\in J} A_j\right] = \bigcup_{j\in J} f[A_j]$.
7. $f\left[\bigcap_{j\in J} A_j\right] \subseteq \bigcap_{j\in J} f[A_j]$.
8. $f^{-1}\left[\bigcup_{k\in K} B_k\right] = \bigcup_{k\in K} f^{-1}[B_k]$.
9. $f^{-1}\left[\bigcap_{k\in K} B_k\right] = \bigcap_{k\in K} f^{-1}[B_k]$.

Para demostrar este teorema se debe tener en cuenta que objetos de la forma $f[P]$ o $f^{-1}[Q]$ son conjuntos, y para probar que ellos son subconjuntos de otro conjunto X se procede de la manera estándar, que es tomar cualquier elemento b de estos y probar que tal b es también elemento del conjunto X. Para probar la igualdad entre dos de estos conjuntos se debe probar que cada conjunto es subconjunto del otro. Adicionalmente, una afirmación de la forma "$b \in f[P]$" es equivalente, debido a la Definición 21.1.1, a decir que existe $a \in P$ tal que $b = f(a)$; similarmente, la afirmación "$y \in f^{-1}[Q]$" es equivalente, debido a la Definición 21.2.1, a decir $f(y) \in Q$.

Demostración. A continuación, se realizarán las demostraciones de tres afirmaciones del teorema. El resto de las pruebas son dejadas como ejercicios para el lector.

1. Como $\varnothing$ es subconjunto de todo conjunto, entonces $\varnothing \subseteq f[\varnothing]$ y también $\varnothing \subseteq f^{-1}[\varnothing]$. Razonemos por reducción al absurdo. Supongamos que $f[\varnothing] \nsubseteq \varnothing$. Esto significa que existiría $b \in f[\varnothing]$. Por definición de imagen directa existiría $a \in \varnothing$ tal que $f(a) = b$. Esto es absurdo porque $\varnothing$ no tiene elementos. Por lo tanto, $f[\varnothing] \subseteq \varnothing$. En conclusión $f[\varnothing] = \varnothing$ porque también vimos que $\varnothing \subseteq f[\varnothing]$.
   Del mismo modo, por reducción al absurdo, supongamos que $f^{-1}[\varnothing] \nsubseteq \varnothing$. Esto significa que existiría $a \in f^{-1}[\varnothing]$. Por definición de imagen recíproca $f(a) \in \varnothing$. Esto es absurdo porque $\varnothing$ no tiene elementos. Por lo tanto, $f^{-1}[\varnothing] \subseteq \varnothing$. Como también $\varnothing \subseteq f^{-1}[\varnothing]$, concluímos que $f^{-1}[\varnothing] = \varnothing$.

2., 3., 4., 5. y 6. Ejercicios para el lector.

7. Sea $b \in f\left[\bigcap_{j\in J} A_j\right]$ cualquiera. Por Definición 21.1.1 de imagen directa, podemos afirmar que existe $a \in \bigcap_{j\in J} A_j$ tal que $b = f(a)$. Sea $k \in J$ arbitrario pero fijo. Como $a \in \bigcap_{j\in J} A_j$, entonces $a \in A_j$ para todo $j \in J$; en particular $a \in A_k$. Por lo tanto, por definición de imagen directa tenemos que $b := f(a) \in f[A_k]$. Como $k \in J$ lo hemos tomado arbitrario, entonces podemos decir que para todo $j \in J$ tenemos que $b \in f[A_j]$, es decir, $b \in \bigcap_{j\in J} f[A_j]$. Esto prueba que $f\left[\bigcap_{j\in J} A_j\right] \subseteq \bigcap_{j\in J} f[A_j]$.

8. Sea $a \in f^{-1}\left[\bigcup_{k\in K} B_k\right]$ cualquiera, es decir, $f(a) \in \bigcup_{k\in K} B_k$ por Definición 21.2.1 de imagen recíproca. Esto es equivalente a que existe $k \in K$ tal que $f(a) \in B_k$, o mejor, usando de nuevo la Definición 21.2.1 de imagen recíproca, existe $k \in K$ tal que $a \in f^{-1}[B_k]$, que es lo mismo que, $a \in \bigcup_{k\in K} f^{-1}[B_k]$. Como en esta prueba todas las afirmaciones son equivalentes, podemos concluir la doble contenencia de los conjuntos $f^{-1}\left[\bigcup_{k\in K} B_k\right]$ y $\bigcup_{k\in K} f^{-1}[B_k]$, probando así lo que queríamos.

9. Ejercicio para el lector.

☑

21.4. Ejercicios

Ejercicio 21.4.1. Sean $A = \{a, b, c, d\}$, $B = \{1, 2, 3\}$ conjuntos, y $f = \{(a, 2), (b, 2), (c, 1), (d, 2)\}$ función de A en B. Halle $f[\{a, b, d\}]$, $f[\{a, c\}]$, $f^{-1}[\{3\}]$ y $f^{-1}[\{1, 2\}]$.

Ejercicio 21.4.2. Sean A y B conjuntos, $P, Q \subseteq A$ y $f : A \longrightarrow B$ una función.

1. Pruebe que $f[P] - f[Q] \subseteq f[P - Q]$.
2. ¿Es necesario que $f[P-Q] \subseteq f[P]-f[Q]$? Dé una demostración o un contraejemplo.

Ejercicio 21.4.3. Sean A y B conjuntos, $U, V \subseteq B$ y $f : A \longrightarrow B$ una función. Pruebe que $f^{-1}[U - V] = f^{-1}[U] - f^{-1}[V]$.

Ejercicio 21.4.4. En el contexto del Teorema 21.3.1, encuentre un contraejemplo en el que sea claro que $f\left[\bigcap_{i\in I} U_i\right] \not\supseteq \bigcap_{i\in I} f[U_i]$.

Ejercicio 21.4.5. Sean A, B conjuntos, $P \subseteq A, Q \subseteq B$ y $f : A \to B$ una función. Pruebe que:

1. $P \subseteq f^{-1}[f[P]]$.
2. $f[f^{-1}[Q]] \subseteq Q$.
3. $f[P] = f[f^{-1}[f[P]]]$.
4. $f^{-1}[f[f^{-1}[Q]]] = f^{-1}[Q]$.

Ejercicio 21.4.6. Sea $f : A \to B$ una función. Considere la relación $\mathcal{F} \subseteq \mathcal{P}(A) \times \mathcal{P}(B)$ dada por:

$$(P, Q) \in \mathcal{F} \quad \text{si y solo si} \quad Q = f[P],$$

para cualesquiera $P \in \mathcal{P}(A)$ y $Q \in \mathcal{P}(B)$. Pruebe que $\mathcal{F}$ es función de $\mathcal{P}(A)$ en $\mathcal{P}(B)$. En efecto, $\mathcal{F} = f_*$. Si además $g : A \to B$ es también una función, pruebe que:

$$f = g \quad \text{si y solo si} \quad f_* = g_*.$$

Ejercicio 21.4.7. Sea $f : A \to B$ una función. Considere la relación $\mathfrak{F} \subseteq \mathscr{P}(B) \times \mathscr{P}(A)$ dada por:

$$(Q, P) \in \mathfrak{F} \quad \text{si y solo si} \quad P = f^{-1}[Q],$$

para cualesquiera $Q \in \mathscr{P}(B)$ y $P \in \mathscr{P}(A)$. Pruebe que $\mathfrak{F}$ es función de $\mathscr{P}(B)$ en $\mathscr{P}(A)$. En efecto, $\mathfrak{F} = f^*$. Si además $g : A \to B$ es también una función, pruebe que:

$$f = g \quad \text{si y solo si} \quad f^* = g^*.$$

Ejercicio 21.4.8. Para cada una de las expresiones de las siguientes funciones $f : \mathbb{R} \to \mathbb{R}$ y cada uno de los siguientes conjuntos $X \subseteq \mathbb{R}$ determine $f[X]$, $f^{-1}[X]$, $f^{-1}[f[X]]$ y $f[f^{-1}[X]]$.

1. $f(x) = \sqrt{|x|}$ y $X = [1, 2]$.
2. $f(x) = \sqrt{|x|}$ y $X = [1/2, 1]$.
3. $f(x) = \lfloor x \rfloor$ y $X = (1/2, 5]$.
4. $f(x) = x^3 - 3x$ y $X = [-1, 2]$.

Lección

veintidós

Composición de funciones. Inversa de una función

Hay diferentes maneras de "combinar" funciones de tal manera que se puedan obtener (posiblemente) otras nuevas. Una forma simple de hacerlo es como se hace en los cursos de cálculo. Veamos la siguiente definición:

Definición 22.0.1. Sean $f, g : \mathbb{R} \longrightarrow \mathbb{R}$ funciones. La *suma* y el *producto* entre f y g corresponde a las funciones $f + g : \mathbb{R} \longrightarrow \mathbb{R}$ y $f \cdot g : \mathbb{R} \longrightarrow \mathbb{R}$ definidas por

$$(f+g)(x) = f(x) + g(x) \quad \text{para todo} \quad x \in \mathbb{R}, \tag{22.1}$$

$$\text{y} \qquad (f \cdot g)(x) = f(x) \cdot g(x) \quad \text{para todo} \quad x \in \mathbb{R}, \tag{22.2}$$

respectivamente.

Es dejado como ejercicio para el lector probar que $f+g$ y $f \cdot g$ son en efecto funciones. Moralmente, se definieron dos nuevas funciones, llamadas $f+g$ y $f \cdot g$, a partir de las funciones f y g. Nótese que la función suma $f + g$, evaluada en $x \in \mathbb{R}$, está definida en términos de la adición de los números reales $f(x)$ y $g(x)$; y del mismo modo la función producto $f \cdot g$, evaluada en $x \in \mathbb{R}$, está definida en términos de la multiplicación entre los números reales $f(x)$ y $g(x)$. Justamente la estructura de $\mathbb{R}$ va a implicar que la adición y multiplicación de funciones hereden prácticamente las mismas propiedades de los números reales. Es así como la adición de funciones, por ejemplo, tiene elemento neutro (o elemento identidad) puesto que la función $\mathbf{0} : \mathbb{R} \longrightarrow \mathbb{R}$, dada por $\mathbf{0}(x) := 0$ para todo $x \in \mathbb{R}$, satisface que $f + \mathbf{0} = \mathbf{0} + f = f$ para toda función $f : \mathbb{R} \longrightarrow \mathbb{R}$ porque

$$(f + \mathbf{0})(x) = f(x) + \mathbf{0}(x) = f(x) + 0 = f(x)$$

y

$$(\mathbf{0} + f)(x) = \mathbf{0}(x) + f(x) = 0 + f(x) = f(x),$$

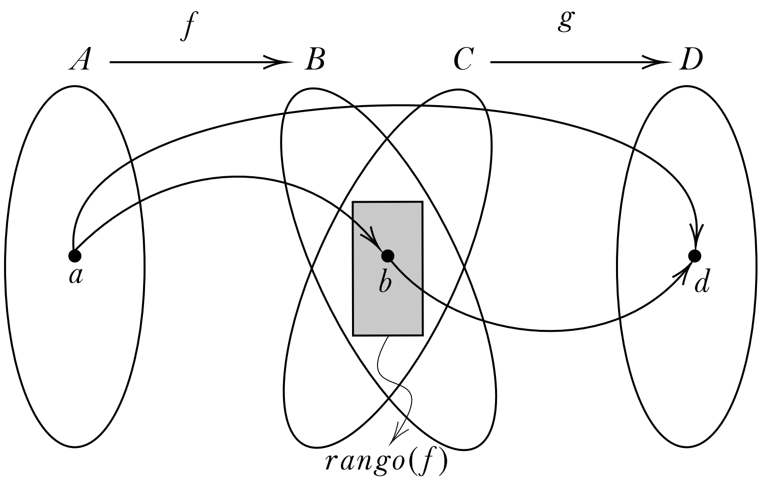
para todo $x \in \mathbb{R}$. Sin embargo, el hecho de que el número cero no tenga inverso multiplicativo va a impedir que todas las funciones que tengan raíces reales no tengan función inversa multiplicativa con dominio $\mathbb{R}$. En efecto, la función inverso multiplicativo de una función f (ver Observación 22.4.5), que es denotada por $\frac{1}{f}$ y definida por $\left(\frac{1}{f}\right)(x) := \frac{1}{f(x)}$, no tendrá en su dominio los $x \in \mathbb{R}$ para los cuales la función f se anula, es decir, los $x \in \mathbb{R}$ para los cuales $f(x) = 0$. Por lo tanto,

$$dom\left(\frac{1}{f}\right) = \{x \in \mathbb{R} \,:\, f(x) \neq 0\}.$$

El hecho de obtener nuevas funciones a partir de dos funciones arbitrarias f y g, mediante la adición y la multiplicación, no siempre es posible debido a que no todos los conjuntos tienen la misma estuctura de $\mathbb{R}$ donde se puede sumar y multiplicar.

22.1. Composición de funciones

Una manera más amplia de operar funciones es por medio de la composición. Realizar la composición de dos funciones no es, a esta altura, una operación desconocida debido a que las funciones por definición son relaciones y en la Lección 14 se introdujo la composición de relaciones.



Sean A, B, C, D conjuntos y sean $f : A \longrightarrow B$ y $g : C \longrightarrow D$ funciones tales que $rango(f) \subseteq dom(g) = C$. Como f y g son relaciones, recordemos que la composición de g y f, denotada por $g \circ f$, es una relación de A en D cuyos elementos son las parejas $(a, d) \in A \times D$ para las cuales existe $b \in rango(f) \subseteq dom(g) = C$ tal que $(a, b) \in f$ y $(b, d) \in g$, es decir, $f(a) = b$ y $g(b) = d$. Más precisamente, la relación $g \circ f \subseteq A \times D$ corresponde al conjunto:

$\{(a, d) \in A \times D \ : \ (a, b) \in f \ \text{ y } \ (b, d) \in g \ \text{ para algún } b \in rango(f)\}.$

En otras palabras, la pareja $(a, d) \in g \circ f$ si y solo si existe $b \in rango(f) \subseteq C$ tal que $(a, b) \in f$ y $(b, d) \in g$.

Dado que f y g son funciones, una pregunta que surge naturalmente es: ¿la relación $g \circ f$ es función? Veamos:

i. Como $g \circ f$ es una relación de A en D, sabemos por definición que $dom(g \circ f) \subseteq A$. Sea $a \in A$ cualquiera. Como $f : A \longrightarrow B$ es función, se tiene que $dom(f) = A$. Dado que $a \in A = dom(f)$, existe un único elemento $f(a) \in B$ tal que $(a, f(a)) \in f$. El supuesto $rango(f) \subseteq dom(g) = C$ y el hecho de que $f(a) \in rango(f)$ implican que $f(a) \in dom(g)$. Como $g : C \longrightarrow D$ es función, existe un único elemento $g(f(a)) \in D$ tal que $(f(a), g(f(a))) \in g$. Por lo tanto, $(a, g(f(a))) \in g \circ f$. Es decir, $a \in dom(g \circ f)$. En conclusión, $dom(g \circ f) = A$.

ii. Sean $a \in A = dom(g)$ y $d, d' \in D$ tales que $(a, d), (a, d') \in g \circ f$. Veamos que $d = d'$. Como $(a, d) \in g \circ f$, existe $b \in B$ tal que $(a, b) \in f$ y $(b, d) \in g$. El hecho de ser f y g funciones nos permite escribir $b = f(a)$ y $d = g(b) = g(f(a))$. Como hemos supuesto que $(a, d') \in g \circ f$, entonces existe $b' \in B$ tal que $(a, b') \in f$ y $(b', d') \in g$. De nuevo, como f y g son funciones, por hipótesis, podemos escribir $b' = f(a)$ y $d' = g(b') = g(f(a))$. Por lo tanto, $d = g(f(a)) = d'$.

En conclusión, de i y ii, por la Definición 19.1.1, concluímos que $g \circ f$ es función. Además, si $(a, d) \in g \circ f$, se tiene que $d = g(f(a))$. Esta discusión nos permite presentar la definición de composición de funciones de manera más concreta.

Definición 22.1.1. Sean A, B, C, D conjuntos y sean $f : A \longrightarrow B$ y $g : C \longrightarrow D$ funciones tales que $rango(f) \subseteq dom(g)$. La *composición* de g y f es la función

$$\begin{aligned} g \circ f : A &\longrightarrow D \\ x &\longmapsto (g \circ f)(x) := g(f(x)) \quad \text{para todo } x \in A. \end{aligned}$$

Obsérvese que el símbolo "$g \circ f$" en la anterior definición es el nombre de la función de A en D, que fue construída a partir de las funciones f y g. Nótese además que "$(g \circ f)(x)$" denota al elemento del conjunto D que es la única imagen de $x \in A$ por medio de la función $g \circ f$. La función f, que es la primera función que actúa, es conocida como *función interna* de esa composición y, consecuentemente, la función g es la *función externa*. En general, no es correcto escribir "$g \circ f(x)$" porque $\circ$ es una "operación"[1] entre dos funciones y "$f(x)$" es un elemento del conjunto B y no es una función; a menos que B sea un conjunto cuyos elementos sean funciones. Téngase siempre en cuenta que para poder definir la composición de dos funciones el rango de la función interna debe estar contenido en el dominio de la función externa.

Ejemplo 22.1.2.

1. Sea P el conjunto de todas las personas y sea $m : P \longrightarrow P$ la función que asigna a cada persona su madre biológica. Entonces $m \circ m$ es la función que asigna a cada persona la madre de su madre, es decir, su abuela materna.

2. Sean $f, g : \mathbb{R} \longrightarrow \mathbb{R}$ funciones definidas por $f(x) = x^2$ y $g(x) = \operatorname{sen} x$, para todo $x \in \mathbb{R}$. Entonces, $f \circ g$ y $g \circ f$ están dadas por

$$\begin{aligned}(f \circ g)(x) &= f(g(x)) = f(\operatorname{sen} x) = (\operatorname{sen} x)^2 = \operatorname{sen}^2 x,\\ (g \circ f)(x) &= g(f(x)) = g(x^2) = \operatorname{sen}(x^2),\end{aligned}$$

   para todo $x \in \mathbb{R}$.

3. Sean

$$\begin{aligned} f : (0, +\infty) &\longrightarrow \mathbb{R} \\ x &\longmapsto f(x) = \ln x \end{aligned} \qquad \text{y} \qquad \begin{aligned} g : (0, +\infty) &\longrightarrow \mathbb{R} \\ x &\longmapsto g(x) = \sqrt{x}, \end{aligned}$$

   para todo $x \in (0, +\infty)$, funciones. Entonces,

$$\begin{aligned} f \circ g : (0, +\infty) &\longrightarrow \mathbb{R} \\ x &\longmapsto (f \circ g)(x) = f(g(x)) = f(\sqrt{x}\,) = \ln(\sqrt{x}), \end{aligned}$$

[1] Aquí no usamos el término *operación* en el sentido estricto usual, sino apenas para indicar que lo que se obtiene de componer dos funciones es también una función, sin importar su dominio ni codominio.

para todo $x \in (0, +\infty)$. Sin embargo, como $rango(f) = \mathbb{R}$ y $dom(g) = (0, +\infty)$, no se puede realizar la composición $g \circ f$ porque no es válido que $rango(f) \subseteq dom(g)$, es decir, $\sqrt{\ln x}$ no está definida para todo $x \in (0, +\infty)$.

22.2. Propiedades de la composición

Como fue discutido antes de la Definición 22.1.1, la composición $g \circ f$ de las funciones $f : A \longrightarrow B$ y $g : C \longrightarrow D$ tales que $rango(f) \subseteq dom(g) = C$ es también una función. Esto nos permite afirmar que la composición de funciones es en cierto sentido "clausurativa" (no en el sentido de que obtengamos siempre funciones con el mismo dominio y mismo codominio, sino que lo obtenido es también función).

Los numerales 2 y 3 en el Ejemplo 22.1.2 nos muestran que la composición de funciones *no es conmutativa*, porque algunas veces, como en 3, ni siquiera es posible definir alguna de las composiciones. En el caso que fuera posible realizar las dos composiciones, $f \circ g$ y $g \circ f$, como en 2, no necesariamente vale que $f(g(x)) = g(f(x))$ para todo x del respectivo dominio.

Ejemplo 22.2.1. Consideremos las funciones de $\mathbb{R}$ en $\mathbb{R}$ dadas por las fórmulas algebraicas $f(x) = x^3$ y $g(x) = x+1$ para cualquier $x \in \mathbb{R}$. Es claro que $rango(f) \subseteq \mathbb{R} = dom(g)$ y $rango(g) \subseteq \mathbb{R} = dom(f)$. Esto nos garantiza que podemos hacer las dos composiciones $g \circ f$ y $f \circ g$. La función $g \circ f : \mathbb{R} \longrightarrow \mathbb{R}$ es dada por $(g \circ f)(x) = g(f(x)) = g(x^3) = x^3 + 1$ para todo $x \in \mathbb{R}$. La función $f \circ g : \mathbb{R} \longrightarrow \mathbb{R}$ es dada por $(f \circ g)(x) = f(g(x)) = f(x + 1) = (x + 1)^3$ para todo $x \in \mathbb{R}$. Nótese que $dom(g \circ f) = dom(f \circ g) = \mathbb{R}$ y $codom(g \circ f) = codom(f \circ g) = \mathbb{R}$. Vemos que las expresiones algebraicas $x^3 + 1$ y $(x + 1)^3$ no tienen la misma forma. Sin embargo, esto podría no ser suficiente para concluir que $g \circ f \neq f \circ g$, porque hay muchas expresiones algebraicas con apariencias distintas que acaban siendo iguales, por ejemplo $(x + 1)^2$ y $x^2 + 2x + 1$. Así que para dejar todo lo más claro posible, evaluamos en un cierto número real y veamos si coinciden, $(g \circ f)(1) = 1^3 + 1 = 2$ pero $(f \circ g)(1) = (1 + 1)^3 = 8$. Como es válido que existe al menos un $x \in \mathbb{R}$ tal que $(g \circ f)(x) \neq (f \circ g)(x)$, entonces podemos afirmar que $g \circ f \neq f \circ g$.

Proposición 22.2.2. *Sean A, B, C, D, E, K conjuntos, y sean $f : A \longrightarrow B$, $g : C \longrightarrow D$ y $h : E \longrightarrow K$ funciones tales que $rango(f) \subseteq dom(g) = C$ y $rango(g) \subseteq dom(h) = E$. Entonces,*

$$(h \circ g) \circ f = h \circ (g \circ f).$$

Demostración. Se deja como ejercicio para el lector probar que tanto $(h \circ g) \circ f$ como $h \circ (g \circ f)$ son funciones de A en K. Esto implica que estas funciones tienen el mismo dominio, el conjunto A, y el mismo codominio, el conjunto K.

Ahora, sea $x \in A$ cualquiera. Usando el hecho de que $h \circ g$ y $g \circ f$ son también funciones, debido a que por hipótesis f, g y h son funciones, y la Definición 22.1.1 de composición de funciones en cada una de las siguientes igualdades tenemos que:

$$\begin{aligned}
((h \circ g) \circ f)(x) &= (h \circ g)(f(x)) \\
&\quad \text{(Definición 22.1.1 de composición } h \circ g \text{ y } f) \\
&= h(g(f(x))) \\
&\quad \text{(Definición 22.1.1 de composición de } h \text{ y } g) \\
&= h((g \circ f)(x)) \\
&\quad \text{(Definición 22.1.1 de composición } g \text{ y } f) \\
&= (h \circ (g \circ f))(x). \\
&\quad \text{(Definición 22.1.1 de composición de } h \\
&\quad \text{y } g \circ f).
\end{aligned}$$

Por lo tanto, $(h \circ g) \circ f = h \circ (g \circ f)$. ☑

22.3. Neutros de la composición de funciones

Consideremos la función constante $\mathbb{1} : \mathbb{R} \longrightarrow \mathbb{R}$, dada por $\mathbb{1}(x) = 1$ para todo $x \in \mathbb{R}$. Notemos que para toda función $f : \mathbb{R} \longrightarrow \mathbb{R}$

$$f \cdot \mathbb{1} = \mathbb{1} \cdot f = f,$$

porque

$$(f \cdot \mathbb{1})(x) = f(x) \cdot \mathbb{1}(x) = f(x) \cdot 1 = f(x)$$

y

$$(\mathbb{1} \cdot f)(x) = \mathbb{1}(x) \cdot f(x) = 1 \cdot f(x) = f(x),$$

para todo $x \in \mathbb{R}$. En efecto, la función $\mathbb{1}$ es la función identidad respecto a la multiplicación de funciones. Lo que vamos a estudiar en esta subsección es si es posible encontrar una función identidad pero respecto a la composición de funciones.

Como vimos en el Ejemplo 22.1.2 numeral 3, es factible que a pesar de que la composición $f \circ g$ esté definida, $g \circ f$ no lo esté. Esto tiene implicaciones serias cuando queremos hallar, por ejemplo, una función que sea elemento neutro o identidad de esta operación entre funciones. Debemos entonces tener un poco más de cuidado al hablar de elementos identidad respecto a la composición, pues como veremos a continuación, en general no tendremos una misma función que al componer a izquierda y a derecha deje invariante la función con la que estemos componiendo.

Proposición 22.3.1. *Sea $f : A \longrightarrow B$ función arbitraria.*

1. $f \circ id_A = f$.
2. $id_B \circ f = f$.
3. *Si $A = B$, entonces $id_A = id_B$ y*

$$f \circ id_A = f = id_A \circ f.$$

Demostración.

1. Sean $f : A \longrightarrow B$ función arbitraria y $id_A : A \longrightarrow A$ la función identidad en A. El rango de la función id_A es justamente $A = dom(f)$. Por lo tanto, $f \circ id_A : A \longrightarrow B$ es una función con dominio A y codominio B. Ahora sea $a \in A = dom(f) = dom(f \circ id_A)$ cualquiera. Por Definición 22.1.1 de composición de funciones se tiene que $(f \circ id_A)(a) = f(id_A(a))$ y por Definición 19.2.2 de la función identidad en A se tiene que $f(id_A(a)) = f(a)$, es decir $(f \circ id_A)(a) = f(a)$. Como $a \in A$ es arbitraria concluímos lo que se quería.

2, 3. Ejercicios para el lector.

☑

Observación 22.3.2. Note que $id_A \circ f$ no necesariamente está definida; a no ser que $B \subseteq A$ y, similarmente, $f \circ id_B$ no necesariamente está definida; a no ser que $A \subseteq B$. También, como consecuencia de esta última Proposición 22.3.1, diremos que, para cualquier función $f : A \longrightarrow B$, respecto a la composición de funciones, la función id_A es *elemento neutro a la derecha* de f y, del mismo modo, id_B es *elemento neutro a la izquierda* de f. Y en el caso en que $A = B$, para cualquier función $f : A \longrightarrow A$ se dice que id_A es *elemento neutro* de f porque

$$f \circ id_A = id_A \circ f = f. \tag{22.3}$$

22.4. Inversa de una función

Una pregunta que surge naturalmente en este momento es si dada una función f, ¿existe otra función que sea inversa de la función f respecto a la composición de funciones? Recordemos lo que ocurre en los conjuntos numéricos $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$. Se sabe que dado cualquier número x existe un número y tal que $x + y = y + x = 0$, donde 0 es el elemento identidad de la adición. Este número y es único, es denotado por $y = -x$ y es llamado el opuesto, o el inverso, aditivo de x. También en $\mathbb{Q}$ y $\mathbb{R}$ vale que para cualquier número x no nulo existe un número y tal que $x \cdot y = y \cdot x = 1$, donde 1 es el elemento identidad de la multiplicación. Tal número y es único, es denotado por $y = x^{-1} = \frac{1}{x}$ y es llamado el inverso multiplicativo de x. En estos ejemplos se tiene que las operaciones adición y multiplicación son conmutativas. No es así en el caso de la composición de funciones. Vea el Ejemplo 22.2.1 y la discusión desarrollada.

Como no tenemos además un concepto de función que sea en general neutro a izquierda y a derecha simultáneamente (vea Observación 22.3.2); esto debido a que el dominio de una función dada puede diferir de su codominio, entonces definimos a continuación los conceptos de función *inversa a derecha* y función *inversa a izquierda* de una función.

Definición 22.4.1. Sea $f : A \longrightarrow B$ cualquier función.

1. Una función $g : B \longrightarrow A$ se dice una *inversa a derecha* de f si y solo si $f \circ g = id_B$.

2. Una función $g : B \longrightarrow A$ se dice una *inversa a izquierda* de f si y solo si $g \circ f = id_A$.

3. Una función g se dice una *inversa* de f si y solo si g es inversa a derecha y también inversa a izquierda de f.

En caso de que exista, aunque se ha usado el término *una inversa* en la Definición 22.4.1(3), vemos de la siguiente proposición que de ahora en adelante podremos escribir *la inversa*, puesto que demostraremos que en caso de existir dicha inversa, esta debe ser única.

Proposición 22.4.2. *Sea $f : A \longrightarrow B$ cualquier función.*

1. *Si $g : B \longrightarrow A$ es una inversa a derecha de f y $h : B \longrightarrow A$ es una inversa a izquierda de f, entonces $g = h$.*

2. *Si f tiene inversa, entonces tal inversa es única.*

3. *Si $g : B \longrightarrow A$ es inversa de f, entonces f es inversa de g.*

Demostración.

1. Sea $f : A \longrightarrow B$ cualquier función. Supongamos que $g : B \longrightarrow A$ es una inversa a izquierda de f y que $h : B \longrightarrow A$ es una inversa a derecha de f. Por Definición 22.4.1, esto implica que $f \circ g = id_B$ y $id_A = h \circ f$. Aplicando los resultados 1 y 2 de la Proposición 22.3.1 tenemos que $h \circ id_B = h$ y $g = id_A \circ g$. Por lo tanto, usando la Proposición 22.2.2 que nos dice que la composición de funciones es asociativa, concluímos que
$$g = id_A \circ g = (h \circ f) \circ g = h \circ (f \circ g) = h \circ id_B = h.$$

2. Sea $f : A \longrightarrow B$ cualquier función. Supongamos que $g, h : B \longrightarrow A$ son funciones inversas de f. Por la Definición 22.4.1(3), en particular, g es inversa a derecha de f y h es inversa a izquierda de f. Entonces, por 1, se concluye que $g = h$.

3. Sea $f : A \longrightarrow B$ cualquier función. Supongamos que $g : B \longrightarrow A$ es inversa de f. Por Definición 22.4.1(3), esto significa que g es inversa a izquierda y a derecha de f. Más precisamente, $g \circ f = id_A$ y $f \circ g = id_B$. Esto es equivalente a decir que f es inversa a derecha y a izquierda de g. De nuevo por la Definición 22.4.1(3) de función inversa, concluímos que f es inversa de g.

☑

Observación 22.4.3. Sea $f : A \longrightarrow B$ una función. Fue probado en la anterior Proposición 22.4.2 que la inversa de la función f es única siempre y cuando exista. Esta unicidad de la inversa de la función f, en el caso de existir, la hace merecedora de una notación especial para referirnos a ella. Así que, si $f : A \longrightarrow B$ tiene inversa entonces la denotaremos por $f^{-1} : B \longrightarrow A$.

Ejemplo 22.4.4. Consideremos la funciones

$$\begin{aligned} f : [0,+\infty) &\longrightarrow [0,+\infty) \\ x &\longmapsto f(x) = x^2 \end{aligned} \qquad \text{y} \qquad \begin{aligned} g : [0,+\infty) &\longrightarrow [0,+\infty) \\ x &\longmapsto g(x) = \sqrt{x}, \end{aligned}$$

para todo $x \in [0,+\infty)$. Entonces,

$$\begin{aligned} f \circ g : [0,+\infty) &\longrightarrow [0,+\infty) \\ x &\longmapsto (f \circ g)(x) = f(g(x)) = \left(\sqrt{x}\right)^2 = x = id_{[0,+\infty)}(x), \end{aligned}$$

para todo $x \in [0,+\infty)$, y

$$\begin{aligned} g \circ f : [0,+\infty) &\longrightarrow [0,+\infty) \\ x &\longmapsto (g \circ f)(x) = g(f(x)) = \sqrt{x^2} = x = id_{[0,+\infty)}(x), \end{aligned}$$

para todo $x \in [0,+\infty)$. Por lo tanto,

$$f \circ g = g \circ f = id_{[0,+\infty)}.$$

Es decir, $g = f^{-1}$ es la inversa de la función f.

Observación 22.4.5. Sea $f : \mathbb{R} \longrightarrow \mathbb{R}$ una función. Nótese que $f^{-1} : \mathbb{R} \longrightarrow \mathbb{R}$ la inversa de la función f, en caso de existir, no coincide con la función inversa multiplicativa de f que es

$$\begin{aligned}\frac{1}{f} : D &\longrightarrow \mathbb{R}\\ x &\longmapsto \left(\frac{1}{f}\right)(x) = \frac{1}{f(x)} \quad \text{para todo } \ x \in D,\end{aligned}$$

donde

$$D = dom\left(\frac{1}{f}\right) = \{x \in \mathbb{R} \ : \ f(x) \neq 0\}.$$

Obsérvese que $\frac{1}{f}$ es la inversa multiplicativa de f porque

$$\frac{1}{f} \cdot f = f \cdot \frac{1}{f} = \mathbb{1}|_D.$$

Más precisamente, para todo $x \in D$ se tiene que

$$\left(\frac{1}{f} \cdot f\right)(x) = \left(\frac{1}{f}\right)(x) \cdot f(x) = 1 = f(x) \cdot \left(\frac{1}{f}\right)(x) = \left(f \cdot \frac{1}{f}\right)(x).$$

Ejemplo 22.4.6. Consideremos las funciones

$$\begin{aligned}\tan : \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) &\longrightarrow \mathbb{R} & \arctan : \mathbb{R} &\longrightarrow \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)\\ x &\longmapsto \tan(x), & x &\longmapsto \arctan(x),\end{aligned}$$

$$\text{y} \qquad \begin{aligned}\cot : \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) - \{0\} &\longrightarrow \mathbb{R}\\ x &\longmapsto \cot(x) = \frac{1}{\tan(x)},\end{aligned}$$

definidas para todo x de su correspondiente dominio. Entonces,

$$\tan \circ \arctan = id_{\mathbb{R}} \quad \text{y} \quad \arctan \circ \tan = id_{(-\pi/2,\pi/2)}.$$

Es decir, arctan es la inversa de la función tan respecto a la composición de funciones, en cambio cot es la inversa multiplicativa de la función tan porque

$$\tan \cdot \cot = \cot \cdot \tan = \mathbb{1}|_{dom(\cot)}.$$

Más precisamente,

$$(\tan \cdot \cot)(x) = \tan(x) \cdot \cot(x) = \cot(x) \cdot \tan(x) = (\cot \cdot \tan)(x) = 1$$

para todo $x \in dom(\cot) = (-\pi/2, \pi/2) - \{0\}$. En resumen,

$$\arctan = \tan^{-1} \quad \text{y} \quad \cot = \frac{1}{\tan}.$$

Ejemplo 22.4.7. Consideremos de nuevo el Ejemplo 22.1.2(1) en el que P es el conjunto de todas las personas y $m : P \longrightarrow P$ es la función que asigna a cada persona su madre biológica. Una candidata a ser inversa de la función m sería la relación $h \subseteq P \times P$ tal que a cada madre le corresponda sus hijos. Esta relación no llega a tener el estatus de función porque por ejemplo no todas las personas son madres, es decir $dom(h)$ no es P. Este inconveniente puede ser dejado de lado si cambiamos el codominio de la función m, es decir, consideremos $m : P \longrightarrow M$ donde M es el conjunto de todas las personas que son madres y así consideremos h como una relación de M en P. A pesar de esta modificación, sabemos que existen madres que tienen varios hijos, es decir existen $x \in dom(h) = M$ y $y, y' \in P$ tales que (x, y), $(x, y') \in h$ y $y \neq y'$, esto es y y y' son hermanos. Esto significa que h definitivamente no es función.

Como podemos notar del anterior ejemplo la inversa de una función no siempre existe, es decir, la inversa de una función algunas veces existe y otras veces no, por lo tanto, la pregunta que queda por responder es la siguiente: ¿cuando existe la inversa de una función? Esta pregunta será respondida en la siguiente lección.

22.5. Ejercicios

En los siguientes ejercicios tenga en cuenta que: dados A y B conjuntos cualesquiera, denotamos por B^A al conjunto de todas las funciones de A en B. Más precisamente,

$$B^A = \{f \in \mathcal{P}(A \times B) \; : \; f \text{ es función de } A \text{ en } B\}.$$

Ejercicio 22.5.1. Pruebe que la adición de funciones de $\mathbb{R}^{\mathbb{R}}$, tal y como fue definida en (22.1), es clausurativa en $\mathbb{R}^{\mathbb{R}}$, asociativa, conmutativa, tiene elemento neutro y opuestos aditivos. ¿Qué propiedades satisface la adición de funciones de $\mathbb{Q}^{\mathbb{Q}}$? ¿Y las de $\mathbb{Z}^{\mathbb{Z}}$? ¿Y las de $\mathbb{N}^{\mathbb{N}}$?

Ejercicio 22.5.2. Pruebe que la multiplicación de funciones de $\mathbb{R}^{\mathbb{R}}$, tal y como fue definida en (22.2), es clausurativa en $\mathbb{R}^{\mathbb{R}}$, asociativa, conmutativa, tiene elemento neutro pero no necesariamente tiene inversos multiplicativos en $\mathbb{R}^{\mathbb{R}}$. ¿Qué propiedades satisface la multiplicación de funciones de $\mathbb{Q}^{\mathbb{Q}}$? ¿Y las de $\mathbb{Z}^{\mathbb{Z}}$? ¿Y las de $\mathbb{N}^{\mathbb{N}}$?

Ejercicio 22.5.3. Determine en cada caso las funciones $f \circ g$ y $g \circ f$ donde $f, g \in \mathbb{R}^{\mathbb{R}}$ y están dadas por las siguientes expresiones, para cada $x \in \mathbb{R}$,

- $f(x) = \cos x$ y $g(x) = \operatorname{sen} x$.
- $f(x) = 2x^3 - 1$ y $g(x) = 2(x-1)^2$.
- $f(x) = \frac{1}{x^2+2}$ y $g(x) = 2x - 1$.

Simplifique siempre que sea posible.

Ejercicio 22.5.4. Sea $A = \mathbb{R} - \{1\}$ y sea $f : A \to A$ la función definida por la fórmula algebraica

$$f(x) = \frac{x+1}{x-1},$$

para todo $x \in \mathbb{R}$. ¿Es f la inversa de f? Justifique su respuesta.

Ejercicio 22.5.5. Dada $f : A \longrightarrow A$ una función, denotamos por f^2 la función $f \circ f$. Similarmente, también se denota por f^3 a la función $f \circ f \circ f$. Defina rigurosamente para cada $n \in \mathbb{Z}^+$, usando recursividad, la función f^n que correspondería informalmente a la función que se obtiene al componer n veces la función f, es decir, la función $f \circ f \circ \cdots \circ f$ (n veces).

Ejercicio 22.5.6. Sea $f : A \longrightarrow B$ una función que tiene inversa. Demuestre que $f^{-1} : B \longrightarrow A$ como relación es la relación inversa de f.

Ejercicio 22.5.7. Sean A, B y C conjuntos, con $U \subseteq A$, $V \subseteq C$. Además, sean $f : A \longrightarrow B$ y $g : B \longrightarrow C$ funciones. Pruebe que

$$(g \circ f)[U] = g[f[U]] \quad \text{y} \quad (g \circ f)^{-1}[V] = f^{-1}[g^{-1}[V]].$$

Ejercicio 22.5.8. Sean A conjunto no vacío y $f : A \rightarrow A$ una función. Suponga que existe $a \in A$ tal que $f(x) = a$ para todo $x \in A$. Pruebe que para toda función $g : A \rightarrow A$, $f \circ g = f$. ¿Es válida la recíproca de esta afirmación? Es decir, ¿es válido que para cualquier función $g : A \rightarrow A$ tal que $f \circ g = f$, se cumple que f es constante? Justifique su respuesta.

Lección *veintitrés*

Funciones biyectivas

Al final de la Lección 22 se dejó abierta la pregunta: ¿cuando existe la función inversa de una función dada? Esta pregunta surgió naturalmente de observar que algunas funciones sí tienen inversa, pero otras no tienen. El propósito en esta lección es justamente responder esta pregunta. Desafortunadamente, no es simple determinar si una función tiene inversa o no; o al menos verificar si tiene inversa a izquierda o inversa a derecha. La dificultad radica en que se debe encontrar una candidata adecuada que sea función y que satisfaga la condición de ser el tipo de inversa buscado. Esto en algunas ocasiones es prácticamente imposible. Dada la importancia que tienen en todas las matemáticas las funciones inversas, sería maravilloso tener criterios que nos permitieran chequear rápidamente si una función tiene inversa a derecha o inversa a izquierda o ambas sin necesidad de hallar explícitamente la función deseada.

En el siguiente ejemplo identificaremos algunos problemas que puede tener una función para no tener inversa.

Ejemplo 23.0.1. Consideremos la conocidísima función $f : \mathbb{R} \longrightarrow \mathbb{R}$ dada por $f(x) = x^2$ para todo $x \in \mathbb{R}$, es decir, f asigna a cada real x su cuadrado x^2. ¿Esta función tiene una inversa a derecha o una inversa a izquierda?

Supongamos que $h : \mathbb{R} \longrightarrow \mathbb{R}$ es una inversa a izquierda de f, es decir, $h \circ f = id_{\mathbb{R}}$, por lo tanto, $h(f(x)) = x$ para todo $x \in \mathbb{R}$. Es sabido que $(-3)^2 = 3^2$, luego $f(-3) = f(3)$ y $h(f(-3)) = h(f(3))$ puesto que h es función. Como $h(f(x)) = x$ para todo $x \in \mathbb{R}$, se deduce que $-3 = 3$, lo que es una contradicción. Entonces, f no tiene inversa a izquierda. El problema que se tiene aquí para hallar una inversa a izquierda de f es que hay distintos objetos en su dominio que tienen la misma imagen en el codominio.

Ahora, supongamos que $g : \mathbb{R} \longrightarrow \mathbb{R}$ es una inversa a derecha para f. Esto sería que $f \circ g = id_{\mathbb{R}}$, es decir, $f(g(x)) = x$ para todo $x \in \mathbb{R}$. En particular, $f(g(-3)) = -3$, lo que significaría que el cuadrado del real $g(-3)$ es -3 lo cual no es posible dado que -3 es negativo y $(g(-3))^2$ no lo puede ser. Por lo tanto, f no tiene inversa a derecha. Nótese que el principal problema para hallar una inversa a derecha de f es que hay objetos en su codominio, los reales negativos, que no están en el rango de f.

En las siguientes definiciones daremos nombres a las funciones que no tienen los problemas que se vieron en el ejemplo anterior.

23.1. Funciones inyectivas

Definición 23.1.1. Sea $f : A \longrightarrow B$ una función. La función f se dice *inyectiva* (también llamada *uno a uno*) si y solo si dados $x, y \in A$ cualesquiera se satisface que

$$f(x) = f(y) \qquad \text{implica} \qquad x = y.$$

Equivalentemente, para cualesquiera $x, y \in A$,

$$x \neq y \qquad \text{implica} \qquad f(x) \neq f(y).$$

Observación 23.1.2. Sea $f : A \longrightarrow B$ una función. f no es inyectiva si y solo si existen $x, y \in A$ tales que $f(x) = f(y)$ pero $x \neq y$.

Ejemplo 23.1.3. Consideremos las siguientes funciones que se diferencian en sus dominios.

1. La función $h : [0, +\infty) \longrightarrow [0, +\infty)$ definida por $h(x) = x^2$ para todo $x \in [0, +\infty)$. Veamos que h es inyectiva. Sean x, $y \in [0, +\infty)$ tales que $h(x) = h(y)$. Es decir, $x^2 = y^2$. Como x y y son no negativos, se deduce que $x = |x| = \sqrt{x^2} = \sqrt{y^2} = |y| = y$. Esto prueba que h es inyectiva.

2. Ahora, sea $g : \mathbb{R} \longrightarrow [0, +\infty)$ definida por $g(x) = x^2$ para todo $x \in \mathbb{R}$. Esta función no es inyectiva. Una razón por la que g no es inyectiva es porque $g(-3) = 9 = g(3)$ y $-3 \neq 3$.

Ejemplo 23.1.4. Sean $a, b \in \mathbb{R}$, con $a \neq 0$. La función

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto f(x) = ax + b \quad \text{para todo} \quad x \in \mathbb{R}, \end{aligned}$$

es inyectiva. Sean x, $x' \in \mathbb{R}$ cualesquiera tales que $f(x) = f(x')$, es decir $ax + b = ax' + b$. Veamos que $x = x'$. Usando los axiomas de los números reales tenemos que

$$\begin{aligned}
x &= 1x = \frac{a}{a}x = \frac{ax}{a} = \frac{ax+0}{a} = \frac{ax+[b+(-b)]}{a} \\
&= \frac{(ax+b)+(-b)}{a} = \frac{(ax'+b)+(-b)}{a} = \frac{ax'+[b+(-b)]}{a} \\
&= \frac{ax'+0}{a} = \frac{ax'}{a} = \frac{a}{a}x' = 1\,x' = x'.
\end{aligned}$$

Dejamos como ejercicio para el lector justificar cada una de las anteriores igualdades.

Por lo tanto, f es inyectiva.

23.2. Funciones sobreyectivas

Definición 23.2.1. Sea $f : A \longrightarrow B$ una función. La función f se dice *sobreyectiva* (también llamada simplemente *sobre*) si y solo si para todo $b \in B$ existe algún $a \in A$ tal que $f(a) = b$, es decir $B \subseteq f[A] = rango(f)$. Como $f[A] \subseteq B$, equivalentemente, f se dice sobreyectiva si y solo si $rango(f) = f[A] = B$.

Observación 23.2.2. Sea $f : A \longrightarrow B$ una función. f no es sobreyectiva si y solo si existe $b \in B$ tal que para todo $a \in A$ se tiene que $f(a) \neq b$. Es decir, $rango(f) = f[A] \subsetneq B$.

Ejemplo 23.2.3. Consideremos de nuevo las funciones del Ejemplo 23.1.3.

1. La función $h : [0, +\infty) \longrightarrow [0, +\infty)$ definida por $h(x) = x^2$ para todo $x \in [0, +\infty)$ es sobreyectiva. Sea $b \in [0, +\infty)$ cualquiera. Tomemos $a := \sqrt{b} \in [0, +\infty) = dom(h)$ (ver apéndice). Así $h(a) = h(\sqrt{b}) = (\sqrt{b})^2 = b$. Entonces, h es sobreyectiva.

2. La función $g : \mathbb{R} \longrightarrow [0, +\infty)$ definida por $g(x) = x^2$ para todo $x \in \mathbb{R}$ es sobreyectiva. La prueba de que g es sobreyectiva coincide con la prueba de la sobreyectividad de h en 1.

3. La función $j : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $j(x) = x^2$ para todo $x \in \mathbb{R}$ *no* es sobreyectiva, puesto que si tomamos $-1 \in \mathbb{R}$, ningún real

x satisface $j(x) = x^2 = -1$ (ningún cuadrado de un número real es negativo).

Notemos que a pesar de que las funciones dadas en los numerales 1, 2 y 3 en este ejemplo son iguales como conjunto de parejas ordenadas, la sobreyectividad de ellas depende del conjunto que estemos tomando como codominio.

Ejemplo 23.2.4. Sean $a, b \in \mathbb{R}$, con $a \neq 0$. La función $f : \mathbb{R} \longrightarrow \mathbb{R}$ considerada en el Ejemplo 23.1.4 dada por $f(x) = ax + b$ para todo $x \in \mathbb{R}$ es sobreyectiva. Sea $y \in \mathbb{R}$ cualquiera. Tomemos $x = \frac{y-b}{a}$. Usando los axiomas de los reales tenemos que

$$\begin{aligned} f(x) &= ax + b = a\left(\frac{y-b}{a}\right) + b = \frac{a}{a}(y-b) + b \\ &= (y-b) + b = y + [(-b) + b] = y + 0 = y. \end{aligned}$$

Dejamos de nuevo como ejercicio justificar cada una de las anteriores igualdades. Esto muestra que f es sobreyectiva.

23.3. Funciones biyectivas

Definición 23.3.1. Sea $f : A \longrightarrow B$ una función. La función f se dice *biyectiva* si y solo si f es inyectiva y sobreyectiva.

Ejemplo 23.3.2. Consideremos de nuevo las funciones h y g de los Ejemplos 23.1.3 y 23.2.3 y la función f de los Ejemplos 23.1.4 y 23.2.4,

1. h es biyectiva pero g no lo es porque a pesar de ser sobreyectiva no es inyectiva.

2. f es biyectiva.

Lema 23.3.3. *Sean $f : A \longrightarrow B$ y $g : B \longrightarrow C$ funciones.*

1. *Si f y g son inyectivas, entonces $g \circ f$ es inyectiva.*

2. *Si f y g son sobreyectivas, entonces $g \circ f$ es sobreyectiva.*

3. *Si f y g son biyectivas, entonces $g \circ f$ es biyectiva.*

Demostración. Sean $f : A \longrightarrow B$ y $g : B \longrightarrow C$ funciones. Vemos que $g \circ f : A \longrightarrow C$ es función porque tanto f como g son funciones y $rango(f) \subseteq dom(g) = B$.

1. Supongamos que f y g son funciones inyectivas. Veamos que $g \circ f$ es también inyectiva. Sean $x, y \in A$ cualesquiera. Supongamos que $(g \circ f)(x) = (g \circ f)(y)$. Por Definición 22.1.1 de composición de funciones tenemos que $g(f(x)) = g(f(y))$. Como por hipótesis g es inyectiva, se concluye que $f(x) = f(y)$, y finalmente, como f es inyectiva, se deduce que $x = y$. Esto prueba que $g \circ f$ es inyectiva.

2. Supongamos que f y g son funciones sobreyectivas. Veamos que $g \circ f$ es también sobreyectiva. Sea $c \in C$ cualquiera. Por hipótesis sabemos que $g : B \longrightarrow C$ es sobreyectiva, entonces existe $b \in B$ tal que $g(b) = c$. Como $f : A \longrightarrow B$ también es sobreyectiva, existe $a \in A$ tal que $f(a) = b$. En conclusión, existe $a \in A$ tal que $(g \circ f)(a) = g(f(a)) = g(b) = c$. Esto prueba que $g \circ f$ es sobreyectiva.

3. Esta parte es consecuencia directa de las anteriores.

☑

23.4. Existencia de funciones inversas

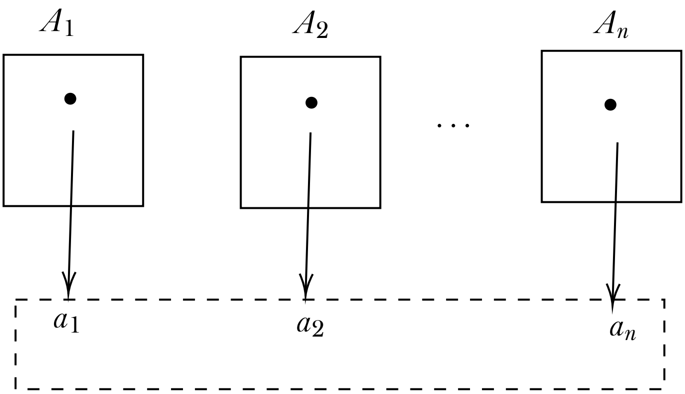
El siguiente teorema aborda la cuestión planteada al inicio de esta lección, en la que se indagaba por la existencia de funciones inversas. Este teorema nos dice cuando una función dada posee una inversa a derecha, una inversa a izquierda, o una inversa.

Teorema 23.4.1. *Sean A y B conjuntos no vacíos y sea $f : A \longrightarrow B$ una función.*

1. *La función f tiene una inversa a derecha si y solo si f es sobreyectiva.*
2. *La función f tiene una inversa a izquierda si y solo si f es inyectiva.*
3. *La función f tiene una inversa si y solo si f es biyectiva.*

Antes de dar una demostración de estas equivalencias tenemos que hablar de, uno de los axiomas de la Teoría de conjuntos, el conocido *axioma de elección*. En estas notas no pretendemos profundizar en este tema, ampliamente estudiado en el curso Introducción a la Teoría de Conjuntos, pero sí vale la pena acercarnos intuitivamente a lo que nos dice este axioma puesto que la demostración de la equivalencia 1 del Teorema 23.4.1 requiere de este.[1]

Dado un conjunto $A \neq \emptyset$, sabemos que por lo menos tiene un elemento; así que si lo necesitamos podemos escoger un elemento $a \in A$. Dentro de la *axiomática de Zermelo-Fraenkel*, si tenemos finitos conjuntos no vacíos $A_1, \cdots, A_n$ ($n \in \mathbb{N} - \{0\}$), podemos escoger *al tiempo* un elemento de cada uno de estos conjuntos $a_i \in A_i$ ($i \in \{1, \cdots, n\}$).



Aunque parezca intuitivamente hablando "trivial", existen universos de la Teoría de conjuntos de Zermelo-Fraenkel en los que si tenemos una familia *infinita* de conjuntos no vacíos $\mathcal{F} := \{A_i : i \in I\}$, no podemos escoger *al tiempo* un elemento $a_j \in A_j$ para cada $j \in I$. Afortunadamente, sí existen universos de la Teoría de conjuntos de Zermelo-Fraenkel en los que sí podemos hacer esta elección simultánea infinita. Suponer que podemos hacerlo es lo que se conoce como *axioma de elección*. Este axioma es ampliamente estudiado en

[1]Más aún, 1 es equivalente al axioma de elección (AE). El hecho de que AE implica 1 puede ser visto en la demostración abajo. Sin embargo, el hecho de que 1 implica AE no será estudiado en estas notas.

textos como [6] por lo que los lectores curiosos pueden remitirse a este texto para profundizar al respecto. Rigurosamente, el enunciado del axioma de elección es el siguiente:

(AE) Dada una familia indexada de conjuntos no vacíos $\mathscr{F} := \{A_i : i \in I\}$ $(I \neq \emptyset)$, existe una función $g : I \to \bigcup_{i \in I} A_i$ tal que para todo $j \in I$ tenemos que $g(j) \in A_j$. Dicha función g se denomina **función de elección** para $\mathscr{F}$.

Vale la pena notar que la función g está *eligiendo* simultáneamente un elemento $g(j)$ de cada conjunto A_j $(j \in I)$.

Demostración del Teorema 23.4.1. Sea $f : A \longrightarrow B$ una función.

1. Supongamos que f tiene una inversa a derecha $g : B \longrightarrow A$, esto es, $f \circ g = id_B$. Veamos que $f : A \longrightarrow B$ es sobreyectiva. Sea $b \in B$ cualquiera. Tomemos $a = g(b) \in A$. Entonces, como f es función, $f(a) = f(g(b))$, y por Definición 22.1.1 de composición de funciones $f(g(b)) = (f \circ g)(b)$. Dado que $f \circ g = id_B$, se tiene que $(f \circ g)(b) = id_B(b) = b$. Es decir, existe $a \in A$ tal que $f(a) = b$. Esto prueba que f es sobreyectiva.

   Ahora supongamos que f es sobreyectiva. Veamos que existe una función $h : B \longrightarrow A$ tal que $f \circ h = id_B$. Como $f : A \longrightarrow B$ es sobreyectiva, dado cualquier $b \in B$ existe $a \in A$ tal que $f(a) = b$. Más específicamente, la imagen recíproca de $\{b\}$ bajo f, es decir, $f^{-1}[\{b\}]$, es un conjunto no vacío. Entonces $\left\{f^{-1}[\{b\}]\right\}_{b \in B}$ es una familia de conjuntos no vacíos. El propósito es construir una función h tal que $h(b) \in f^{-1}[\{b\}]$ para todo $b \in B$. AE nos garantiza la existencia de una función $h : B \longrightarrow \bigcup_{b \in B} f^{-1}[\{b\}]$ tal que $h(b) \in f^{-1}[\{b\}]$ para todo $b \in B$. Es decir, esta función nos da una elección de un elemento $a \in f^{-1}[\{b\}]$ para cada $b \in B$ de tal manera que $h(b) = a$. Como para cada $b \in B$ tenemos que $f^{-1}[\{b\}] \subseteq A$, podemos tomar la función h con codominio A. Consecuentemente, por la Definición 22.1.1 y la construcción de h se tiene que $(f \circ h)(b) = f(h(b)) = b$ para todo $b \in B$. Por lo tanto, $f \circ h = id_B$.

2. Supongamos que f tiene una inversa a izquierda $g : B \longrightarrow A$, esto es, $g \circ f = id_A$. Veamos que f es inyectiva. Sean x,

$y \in A$ cualesquiera. Supongamos que $f(x) = f(y)$. Como g es función, se tiene que $g(f(x)) = g(f(y))$ y, por Definición 22.1.1, podemos escribir esta igualdad así $(g \circ f)(x) = (g \circ f)(y)$. Como por hipótesis $g \circ f = id_A$, es decir $g(f(a)) = a$ para todo $a \in A$, se deduce que $x = y$. Esto prueba que f es inyectiva.

Ahora supongamos que f es inyectiva. Veamos que existe una función $h : B \longrightarrow A$ tal que $h \circ f = id_A$. El propósito es describir cómo *actúa* la función h en cada elemento de B. Como $rango(f) \subseteq B$ entonces para cada $b \in B$ hay solo dos posibles opciones: $b \in rango(f)$ o $b \notin rango(f)$.

Si $b \in rango(f) = f[A]$, entonces existe $a_b \in A$ tal que $b = f(a_b)$. Tal a_b es único porque si existiese otro $a \in B$ tal que $b = f(a)$, tendríamos que $f(a_b) = f(a)$, pero como f es inyectiva, se deduciría que $a_b = a$. En este caso, definimos $h(b) = a_b$. Si por el contrario $b \notin rango(f) = f[A]$ entonces definimos $h(b) = \alpha$, donde α es algún elemento fijo de A. En resumen, consideramos

$$
\begin{aligned}
&h : B \longrightarrow A\\
&\qquad b \longmapsto h(b) = \begin{cases} a_b, & \text{si} \quad b \in f[A]; \;\; \text{donde} \;\; f(a_b) = b, \\ \alpha, & \text{si} \quad b \notin f[A]. \end{cases}
\end{aligned}
$$

Consecuentemente, por la Definición 22.1.1 y la construcción de h se tiene que, $h : B \longrightarrow A$ es función y $(h \circ f)(a) = h(f(a)) = a_{f(a)} = a$ para todo $a \in A$, porque $f(a_{f(a)}) = f(a)$. Por lo tanto, $h \circ f = id_A$.

3. Esta parte es consecuencia inmediata de las partes (1) y (2) de este teorema junto con el Lema 23.3.3.

☑

El siguiente teorema nos muestra una aplicación directa del Teorema 23.4.1, en la cual, esencialmente, se “cancelan” las funciones por la derecha o por la izquierda, dependiendo de si la función es inyectiva o sobreyectiva.

Teorema 23.4.2. *Sean A, B conjuntos no vacíos y sea $f : A \longrightarrow B$ una función.*

1. *La función f es inyectiva si y solo si $f \circ g = f \circ h$ implica $g = h$ para cualesquiera funciones g, $h : Y \longrightarrow A$ donde Y es cualquier conjunto.*

2. *La función f es sobreyectiva si y solo si $g \circ f = h \circ f$ implica $g = h$ para cualesquiera funciones g, $h : B \longrightarrow X$ donde X es cualquier conjunto.*

Demostración. Sean A, B conjuntos no vacíos y sea $f : A \longrightarrow B$ una función.

1. Supongamos que f es inyectiva. Sean Y cualquier conjunto y g, $h : Y \longrightarrow A$ funciones tales que $f \circ g = f \circ h$. Por la parte 2 del Teorema 23.4.1, la función f posee una inversa a izquierda, digamos $k : B \longrightarrow A$. Así, $k \circ (f \circ g) = k \circ (f \circ h)$, porque k es función. Como la composición de funciones es asociativa y k es una inversa a izquierda de f, es decir $k \circ f = id_A$, se deduce que

$$g = id_A \circ g = (k \circ f) \circ g = (k \circ f) \circ h = id_A \circ h = h.$$

La implicación que falta es dejada como ejercicio para el lector.

2. Supongamos que f es sobreyectiva. Sean X cualquier conjunto y $g, h : B \longrightarrow X$ funciones tales que $g \circ f = h \circ f$. Por la parte 1 del Teorema 23.4.1, la función f posee un inversa a derecha, digamos $k : B \longrightarrow A$. Entonces $(g \circ f) \circ k = (h \circ f) \circ k$. Como la composición de funciones es asociativa y k es una inversa a derecha de f, es decir $f \circ k = id_B$, se deduce que

$$g = g \circ id_B = g \circ (f \circ k) = h \circ (f \circ k) = h \circ id_B = h.$$

Ahora supongamos que f no es sobreyectiva. Veamos que existe un conjunto X y existen funciones $g, h : B \longrightarrow X$ tales que $g \circ f = h \circ f$ pero $g \neq h$. Sea $c \in B$ tal que $c \notin rango(f)$. Tomemos $X = \{1, 2\}$ y $g, h : B \longrightarrow X$ definidas por $g(b) = 1$ para todo $b \in B$, $h(b) = 1$ para todo $b \in B - \{c\}$ y $h(c) = 2$. Nótese que $g \circ f = h \circ f$ a pesar de que $g \neq h$. Esto prueba la afirmación contrarrecíproca de la implicación que nos faltaba por probar del numeral 2.

☑

23.5. Ejercicios

Ejercicio 23.5.1. Sean A y B conjuntos, $P, Q \subseteq A$ y $f : A \longrightarrow B$ una función inyectiva. Pruebe que $f[P - Q] = f[P] - f[Q]$. ¿Qué puede concluir si f no es inyectiva?

Ejercicio 23.5.2. Sean $a, b \in \mathbb{N}$ tales que $a < b$. Denotemos $[a, b]_{\mathbb{N}} := \{x \in \mathbb{N} : a \leq x \leq b\}$.

1. Sea $k \in \mathbb{N}$. Pruebe que existe una función biyectiva $[a, b]_{\mathbb{N}} \longrightarrow [a + k, b + k]_{\mathbb{N}}$.
2. Sea $m \in \mathbb{Z}^+$ el único elemento tal que $a + m = b$. Pruebe que existe una función biyectiva $[a, b]_{\mathbb{N}} \longrightarrow [1, m + 1]_{\mathbb{N}}$.

Ejercicio 23.5.3. En el enunciado del Teorema 23.4.1, analice cuáles de los numerales siguen siendo verdaderos en los casos en que $A = \varnothing$ o $B = \varnothing$.

Ejercicio 23.5.4. Dada $f : A \to B$ función, si f tiene inversa entonces $\left(f^{-1}\right)^{-1} = f$.

Ejercicio 23.5.5. Sean A, B conjuntos y $f : A \to B$ una función. Consideremos las funciones $f_* : \mathcal{P}(A) \to \mathcal{P}(B)$ y $f^* : \mathcal{P}(B) \to \mathcal{P}(A)$. Pruebe o refute que:

1. f_* es inyectiva si y solo si f es inyectiva.
2. f_* es sobreyectiva si y solo si f es sobreyectiva.
3. f^* es sobreyectiva si y solo si f es sobreyectiva.
4. Si f es biyectiva entonces $(f_*)^{-1} = f^*$ y $(f^*)^{-1} = f_*$.

Ejercicio 23.5.6. Dada $f : A \to B$ función, demuestre o refute: si f es inyectiva, cualquier inversa a izquierda de f es sobreyectiva.

Ejercicio 23.5.7 (AE)**.** Dada $f : A \to B$ función, demuestre o refute: si f es sobreyectiva, cualquier inversa a derecha de f es inyectiva.

Ejercicio 23.5.8. Demuestre o refute: dada $f : A \to B$ función, si f tiene inversa a izquierda, esta es única.

Ejercicio 23.5.9. Demuestre o refute: dada $f : A \to B$ función, si f tiene inversa a derecha, esta es única.

Parte VI

Cardinales

Lección

veinticuatro

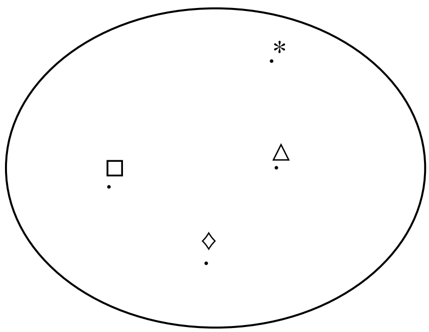
Equipotencia y dominación entre conjuntos

Intuitivamente, la noción de *cardinal de un conjunto* corresponde al *tamaño* del mismo; es decir, al número de elementos que tiene. Pero, ¿cómo determinamos el número de elementos de un conjunto? En otras palabras, ¿cómo es el proceso de contar? En esta lección analizaremos cómo contamos los elementos de un conjunto y, a partir de este análisis, formalizaremos dos mecanismos que nos permitirán comparar cualesquiera par de conjuntos respecto a su tamaño.

24.1. Equipotencia

Pensemos por un momento cómo es el proceso que realizamos para responder a la pregunta: ¿cuántos elementos tiene un cierto conjunto? Para mayor simplicidad pensemos que el conjunto en cuestión es finito. Recordemos que el sistema numérico en el que nos apoyamos para realizar el proceso del conteo de elementos de conjuntos finitos es el conjunto de los números naturales $\mathbb{N}$. En estas notas no estudiaremos en detalle este sistema numérico (el cuál es uno de los temas de la asignatura Sistemas Numéricos de la carrera de Matemáticas de la Universidad Nacional de Colombia), nos apoyaremos en la intuición que tenemos de ellos.

Concretamente, supongamos que nos preguntan cuántos objetos hay en el siguiente conjunto:



Para contar los elementos de este conjunto empezamos por cualquier elemento del conjunto, digamos $\square$. A este le asociamos el número 1.

A continuación escogemos otro elemento del conjunto, diferente de $\square$, digamos $\diamond$, a este le asociamos el natural que le sigue al 1 en el orden usual de $\mathbb{N}$, es decir le asociamos el número 2. De nuevo, escogemos otro elemento diferente a los que fueron tomados, digamos $\triangle$, y le asociamos el siguiente natural (3 en este caso). La intuición que tenemos del concepto de conjunto finito nos dice que este proceso acabará en algún momento. En nuestro ejemplo, el único elemento que nos falta por hacer esta asociación es $*$, a quien siguiendo este orden de ideas le asociamos el número 4. De esta manera y usando el lenguaje estudiado en las lecciones previas, hemos definido la siguiente función:

$$\begin{array}{ccc} \square & \mapsto & 1 \\ \diamond & \mapsto & 2 \\ \triangle & \mapsto & 3 \\ * & \mapsto & 4. \end{array}$$

No es difícil darnos cuenta de que esta función que hemos definido entre nuestro conjunto $\{\square, \diamond, \triangle, *\}$ y el conjunto $\{1, 2, 3, 4\}$ es una *biyección*. Por lo tanto, podemos concluir que nuestro conjunto $\{\square, \diamond, \triangle, *\}$ tiene 4 elementos.

En conclusión, el proceso de *contar* el número de elementos de un cierto conjunto finito no vacío corresponde a establecer una función biyectiva de este conjunto en el conjunto $[1, n]_{\mathbb{N}} = \{1, 2, \cdots, n\}$ para algún $n \in \mathbb{N}$. Esta nueva forma de ver el conteo nos permitirá definir con más precisión dos mecanismos que nos permitirán comparar conjuntos respecto a su tamaño.

Definición 24.1.1. Sean A y B conjuntos. Diremos que A es *equipotente* a B, lo que denotamos por $A \sim B$, si y solo si existe una biyección $f : A \to B$.

Consecuentemente, podemos afirmar que nuestro conjunto $\{\square, \diamond, \triangle, *\}$ es *equipotente* al conjunto $\{1, 2, 3, 4\}$. En efecto, basados en la anterior discusión, diremos que dos conjuntos A y B *tienen la misma cantidad de elementos* si y solo si son *equipotentes*. Este concepto lo podemos extender incluso si estamos trabajando con conjuntos infinitos (no nos preocupemos por ahora qué es formalmente un conjunto infinito, más adelante en estas notas precisaremos este concepto).

Basados en propiedades que fueron demostradas sobre funciones biyectivas, tenemos como corolario el siguiente hecho:

Proposición 24.1.2. *Sean A, B y C conjuntos. Entonces,*

1. $A \sim A$.

2. *Si* $A \sim B$, *entonces* $B \sim A$.

3. *Si* $A \sim B$ *y* $B \sim C$, *entonces* $A \sim C$.

Dejamos la demostración de esta proposición como ejercicio para el lector.

Dados dos conjuntos A y B tales que $A \sim B$, la Proposición 24.1.2 (2) nos dice que también vale que $B \sim A$. Es decir, que si A es equipotente a B, entonces B es equipotente a A. Por lo tanto, podemos afirmar simplemente que estos dos conjuntos *son equipotentes* sin lugar a confusiones.

Observación 24.1.3. Alguien podría pensar que la Proposición 24.1.2 nos dice que el *vínculo* $\sim$ entre conjuntos se comporta como una *relación de equivalencia*. Pero, ¿sobre cuáles conjuntos estaría definido $\sim$? Es decir, ¿cuáles serían los conjuntos de salida y de llegada? Observemos que, en la Proposición 24.1.2, estamos considerando A, B y C conjuntos arbitrarios, así que la colección de conjuntos de referencia donde deberíamos definir $\sim$ es la colección de *todos los conjuntos*[1]. Pero en axiomáticas como la de Zermelo-Fraenkel (volvemos a aclarar que no es objetivo de estas notas profundizar en ninguna axiomática de la *teoría de conjuntos*) podemos demostrar fácilmente que dicha colección de conjuntos no es un conjunto (ver [6]). Desde ese punto de vista, para que un vínculo entre objetos matemáticos tenga el derecho de llamarse *relación*, este debe estar definido entre elementos de un mismo conjunto de referencia, lo cual *no* es el caso.

[1] En teoría de conjuntos la colección de todos los conjuntos es un ejemplo de lo que se conoce como *clase*.

Ejemplo 24.1.4. La función $f : \mathbb{Z} \longrightarrow \mathbb{N}$ definida por

$$n \longmapsto f(n) := \begin{cases} 2n & \text{si } n \geq 0, \\ 2(-n) - 1 & \text{si } n < 0, \end{cases}$$

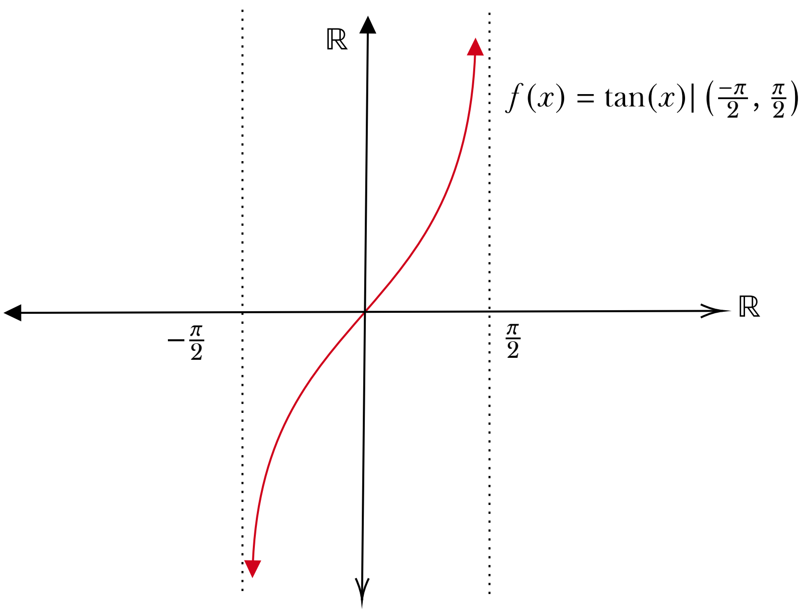
es una biyección (ejercicio para el lector). Por lo tanto, tenemos que $\mathbb{Z} \sim \mathbb{N}$.

Ejemplo 24.1.5. Sean $a, b, c, d \in \mathbb{R}$ tales que $a < b$ y $c < d$. La función

$$\begin{aligned} f : (a, b) &\rightarrow (c, d) \\ x &\mapsto \left(\frac{d-c}{b-a}\right)(x - a) + c, \end{aligned}$$

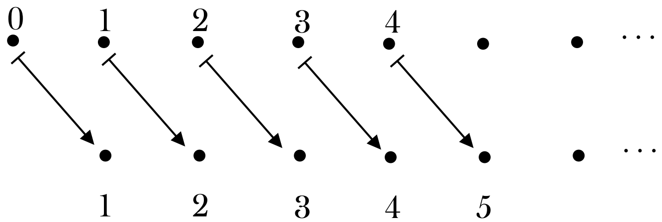
es una biyección (ejercicio para el lector). Esto nos dice que cualesquiera intervalos reales abiertos (a, b) y (c, d) ($a < b$ y $c < d$) son equipotentes.

Ejemplo 24.1.6. La función $tan\,|_{(\frac{-\pi}{2},\frac{\pi}{2})} : \left(\frac{-\pi}{2}, \frac{\pi}{2}\right) \rightarrow \mathbb{R}$ es biyectiva. Es un hecho conocido desde la secundaria que el gráfico de esta función se puede dibujar en el plano cartesiano de la siguiente manera:



Por lo tanto, $\left(\frac{-\pi}{2}, \frac{\pi}{2}\right) \sim \mathbb{R}$. De esta manera, dados $a, b \in \mathbb{R}$ tales que $a < b$, en virtud de lo anterior y del hecho de que $(a, b) \sim \left(\frac{-\pi}{2}, \frac{\pi}{2}\right)$ (Ejemplo 24.1.5), por la Proposición 24.1.2 (3) tenemos que $(a, b) \sim \mathbb{R}$.

Ejemplo 24.1.7. Notemos que la función $f : \mathbb{N} \to \mathbb{N} \setminus \{0\}$ definida por $n \mapsto n + 1$ es una biyección. Veamos que f es sobreyectiva: dado $n \in \mathbb{N} \setminus \{0\}$, vimos que existe $k \in \mathbb{N}$ tal que $f(k) = k + 1 = n$ (Ejemplo 9.1.2), por lo tanto, f es sobreyectiva. Para demostrar la inyectividad, tomemos $m, n \in \mathbb{N}$ tales que $f(m) = f(n)$, es decir $m + 1 = n + 1$. Puesto que $\mathbb{N} \subseteq \mathbb{Z}$, viendo m y n como números enteros tenemos que $m = m + 0 = m + (1 + (-1)) = (m + 1) + (-1) = (n + 1) + (-1) = n + (1 + (-1)) = n + 0 = n$ (dejamos como ejercicio para el lector justificar cada una de las anteriores igualdades). Por lo tanto, como f es inyectiva y sobreyectiva entonces es biyectiva. De esta manera, $\mathbb{N} \sim \mathbb{N} \setminus \{0\}$.



24.2. Dominación

Al inicio de esta lección vimos cómo establecer una biyección del conjunto $\{\Box, \Diamond, \triangle, *\}$ en el conjunto $[1, 4]_{\mathbb{N}} = \{1, 2, 3, 4\}$, por lo que intuitivamente concluimos que $\{\Box, \Diamond, \triangle, *\}$ tiene 4 elementos. Si consideramos el conjunto $\{\boxtimes, \boxdot, \circledcirc\}$, haciendo un ejercicio similar, podemos construir una biyección entre este conjunto y $[1, 3]_{\mathbb{N}} = \{1, 2, 3\}$ (ejercicio para el lector). Esto implica que $\{\boxtimes, \boxdot, \circledcirc\}$ tiene 3 elementos. Si suponemos por un momento que no conocemos el orden usual en $\mathbb{N}$, ¿cómo podemos determinar cuál conjunto tiene más elementos? Para responder esta pregunta realizaremos un proceso de comparación similar al que hicimos al inicio de esta lección, es decir, tomaremos cada uno de los elementos del conjunto $\{\boxtimes, \boxdot, \circledcirc\}$ y le asignaremos un único elemento del conjunto $\{\square, \diamond, \triangle, *\}$.

Empecemos con el elemento $\boxtimes$, al cual le asociamos algún elemento del conjunto $\{\square, \diamond, \triangle, *\}$, digamos $\square$. A otro elemento del conjunto $\{\boxtimes, \boxdot, \circledcirc\}$ distinto de $\boxtimes$, digamos $\boxdot$, le asociamos otro elemento diferente de $\square$, digamos $\diamond$. Por último, al elemento de $\{\boxtimes, \boxdot, \circledcirc\}$ que aún no le hemos asociado nada ($\circledcirc$) le asignamos un elemento diferente de $\square$ y de $\diamond$, digamos $\triangle$. De esta manera, hemos definido la siguiente función con dominio $\{\boxtimes, \boxdot, \circledcirc\}$ y codominio $\{\square, \diamond, \triangle, *\}$:

$$\begin{array}{ccc} \boxtimes & \mapsto & \square \\ \boxdot & \mapsto & \diamond \\ \circledcirc & \mapsto & \triangle \end{array}$$

Notemos que esta función es *inyectiva* pero *no sobreyectiva*, al menos un elemento del conjunto $\{\square, \diamond, \triangle, *\}$, $*$, no es imagen de nadie según esta asignación. Este proceso de comparación nos lleva a intuir que por más que intentemos establecer asignaciones, de los elementos de $\{\boxtimes, \boxdot, \circledcirc\}$ en los elementos de $\{\square, \diamond, \triangle, *\}$, nunca vamos a obtener una función sobreyectiva. Por lo tanto, intuitivamente concluímos que el conjunto $\{\boxtimes, \boxdot, \circledcirc\}$ tiene menos elementos que el conjunto $\{\square, \diamond, \triangle, *\}$. Basados en esta intuición, definimos a continuación el concepto de *dominación entre conjuntos*.

Definición 24.2.1. Sean A y B conjuntos.

1. Decimos que B *domina* a A o que A *es dominado* por B, hecho que denotaremos por $A \preccurlyeq B$, si y solo si existe una función inyectiva $f : A \to B$.
2. Decimos que B *domina estrictamente* a A o que A es *dominado estrictamente* por B, hecho que denotaremos por $A \prec B$, si y solo si $A \preccurlyeq B$ **pero** $A \nsim B$ (es decir, existen funciones inyectivas pero no existen funciones biyectivas de A en B).

Ejemplo 24.2.2. Tomando $A := \{\boxtimes, \boxdot, \circledcirc\}$ y $B := \{\square, \diamond, \triangle, *\}$ (los ejemplos del inicio de esta sección), tenemos que $A \preccurlyeq B$. Más aún, $A \prec B$ (ejercicio para el lector).

A continuación, veremos algunas propiedades que tiene la noción de *dominación entre conjuntos*.

Proposición 24.2.3. *Sean A, B y C conjuntos. Entonces,*

1. $A \preccurlyeq A$.
2. *Si* $A \preccurlyeq B$ *y* $B \preccurlyeq C$, *entonces* $A \preccurlyeq C$.
3. *Si* $A \subseteq B$, *entonces* $A \preccurlyeq B$.

Dejamos como ejercicio para el lector la demostración de los hechos anteriores.

Con base a la Observación 24.1.3, sabemos que $\preccurlyeq$ no es una relación y, consecuentemente, no podemos decir que es una relación reflexiva, ni tampoco que es relación transitiva. Sin embargo, una pregunta natural es: ¿vale que dados A y B conjuntos, si $A \preccurlyeq B$ y $B \preccurlyeq A$, entonces $A = B$? No es difícil ver que esta propiedad no es válida pero sí se satisface una propiedad similar que recibe el nombre de *Teorema de Cantor-Schroeder-Bernstein*, debido a los matemáticos Georg Cantor, Ernst Schroeder y Felix Bernstein; aunque usualmente es conocido solamente como el *Teorema de Cantor-Bernstein* debido a que Schroeder había dado una prueba inicialmente y esta tenía errores que fueron corregidos por Bernstein en su tesis doctoral. En estas notas no haremos su demostración, a pesar de que tenemos las herramientas para verla, porque es muy laboriosa y de todas maneras se estudiará con cuidado en el curso Introducción a la Teoría de Conjuntos. Los lectores curiosos pueden leer la demostración de este hecho en [6] (Teorema 1.6).

Hecho 24.2.4 (Teorema de Cantor-Schroeder-Bernstein). *Sean A y B conjuntos. Si $A \preccurlyeq B$ y $B \preccurlyeq A$, entonces $A \sim B$.*

Este resultado será muy útil cuando tengamos que determinar si dos conjuntos son equipotentes, porque no será necesario dar explícitamente una biyección entre los conjuntos que estamos estudiando, sino que bastará presentar un par de funciones inyectivas que *a priori* que pueden ser más fáciles de construir. Es decir, para probar que dos conjuntos A y B son equipotentes basta con mostrar que existen una función inyectiva $f : A \to B$ y otra función inyectiva $g : B \to A$.

Ejemplo 24.2.5. No es simple encontrar una biyección entre los conjuntos $[0, 1)$ y $(0, 1)$ con el fin de determinar si estos conjuntos son equipotentes. Sin embargo, es fácil encontrar inyecciones que nos permitan afirmar que $(0, 1) \preccurlyeq [0, 1)$ y que $[0, 1) \preccurlyeq (0, 1)$. Como $(0, 1) \subseteq [0, 1)$, la función inclusión es inyectiva, y por lo tanto, $(0, 1) \preccurlyeq [0, 1)$. En el otro sentido, definimos la función $f : [0, 1) \to (0, 1)$ por la expresión $f(x) = \frac{2x+1}{4}$ para todo $x \in [0, 1)$. Esta función f es inyectiva (aunque no es sobreyectiva, pero realmente no nos interesa que no lo sea), por lo tanto, $[0, 1) \preccurlyeq (0, 1)$. Por el Teorema de Cantor-Schroeder-Bernstein, $[0, 1) \sim (0, 1)$.

24.3. Ejercicios

Ejercicio 24.3.1. Demuestre la Proposición 24.1.2.

Ejercicio 24.3.2. Dado A un conjunto, demuestre que $A \times \{*\} \sim A$.

Ejercicio 24.3.3. Demuestre o refute: dados A, B y C conjuntos, si $A \sim B$, entonces $A \cup C \sim B \cup C$. Caso negativo, determine una condición suficiente para A, B y C en la cual la conclusión es verdadera, justificando su respuesta.

Ejercicio 24.3.4. Dada $f : A \to B$ función inyectiva, demuestre que $A \sim f[A]$.

Ejercicio 24.3.5. Dados A y B conjuntos, demuestre que $A \times B \sim B \times A$.

Ejercicio 24.3.6. Dados A, B y C conjuntos, demuestre que $(A \times B) \times C \sim A \times (B \times C)$.

Ejercicio 24.3.7. Dados A, B, C y D conjuntos, demuestre que si $A \sim C$ y $B \sim D$, entonces $A \times B \sim C \times D$.

Ejercicio 24.3.8. Demuestre o refute: dados A, B, C y D conjuntos, si $A \sim C$ y $A \times B \sim C \times D$, entonces $B \sim D$.

Ejercicio 24.3.9. Demuestre la Proposición 24.2.3.

Ejercicio 24.3.10. Dados A, B conjuntos tales que $A \subseteq B$, demuestre que $A \preccurlyeq B$.

Ejercicio 24.3.11. Considere los conjuntos $A := \{\circ, \square, \triangle\}$ y $B := \{*, \odot\}$.

1. Demuestre o refute: $A \preccurlyeq B$.
2. Demuestre o refute: $B \preccurlyeq A$.
3. ¿Podemos afirmar que $A \sim B$? Justifique su respuesta.

Ejercicio 24.3.12. Demuestre o refute: dado A un conjunto, $\varnothing \preccurlyeq A$.

Ejercicio 24.3.13. Dados A y B conjuntos, demuestre que si $A \preccurlyeq B$ entonces $\mathscr{P}(A) \preccurlyeq \mathscr{P}(B)$.

Ejercicio 24.3.14. Dados $a, b \in \mathbb{R}$ tales que $a < b$, demuestre que $[a, b) \sim \mathbb{R}$ (sugerencia: utilice el Teorema de Cantor-Schroeder-Bernstein).

Ejercicio 24.3.15. Dados A y B conjuntos, demuestre que si $A \preccurlyeq B$ y si existe $g : A \to B$ sobreyectiva, entonces $A \sim B$ (sugerencia: utilice AE o una de sus consecuencias vistas en estas Notas).

Lección

veinticinco

Conjuntos finitos

En la lección anterior formalizamos la noción de *contar* elementos de cualquier conjunto y vimos cómo podemos comparar conjuntos respecto a su tamaño por medio de la construcción de funciones biyectivas o inyectivas. Ahora estudiaremos aquellos conjuntos en los cuales el proceso de contar en algún momento acaba, es decir, tiene fin. Estos conjuntos son llamados *conjuntos finitos*. Adicionalmente, asignaremos un número *cardinal* a cada conjunto finito el cual nos facilitará la tarea de comparar estos conjuntos respecto a su tamaño.

25.1. Intervalos naturales y definición de conjunto finito

Como se discutió al inicio de la Lección 24, el conjunto $\{\square, \diamond, \triangle, *\}$ es equipotente al conjunto $\{1, 2, 3, 4\}$ y de esto se concluyó que este conjunto tiene 4 elementos. Vamos a apoyarnos en esta intuición, para definir nuestro concepto de conjunto finito.

Definición 25.1.1. Sea $n \in \mathbb{N} \setminus \{0\}$. El conjunto

$$[1, n]_{\mathbb{N}} := \{k \in \mathbb{N} : 1 \leq k \leq n\},$$

es llamado *intervalo natural entre* 1 *y* n y corresponde al conjunto conformado por todos los números naturales desde 1 hasta n.

Ejemplo 25.1.2.

1. $[1, 1]_{\mathbb{N}} := \{k \in \mathbb{N} : 1 \leq k \leq 1\} = \{1\}$.
2. $[1, 2]_{\mathbb{N}} := \{k \in \mathbb{N} : 1 \leq k \leq 2\} = \{1, 2\}$.
3. $[1, 4]_{\mathbb{N}} := \{k \in \mathbb{N} : 1 \leq k \leq 4\} = \{1, 2, 3, 4\}$.
4. $[1, 9]_{\mathbb{N}} := \{k \in \mathbb{N} : 1 \leq k \leq 9\} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Intuitivamente vemos que, una vez fijado $n \in \mathbb{N} \setminus \{0\}$, el intervalo natural $[1, n]_{\mathbb{N}}$ tiene n elementos. Recordemos que en la Lección 24 se describió que el proceso de contar los elementos de un conjunto

A corresponde a establecer una biyección que asigna a cada elemento de A un único número natural empezando desde el número 1. En general, si este proceso de contar los elementos de un cierto conjunto acaba, es decir, si existe $n \in \mathbb{N} \setminus \{0\}$ tal que cada uno de los elementos de A está relacionado con un único natural del intervalo natural $[1, n]_{\mathbb{N}}$ diremos que tal conjunto es *finito*. Esto incluye el caso especial del conjunto vacío $\emptyset$, puesto que al no tener elementos ni siquiera empezamos este proceso. Siguiendo esta idea, definamos formalmente el concepto de *conjunto finito*.

Definición 25.1.3. Sea A un conjunto. Decimos que A es *finito* si y solo si A es el conjunto vacío o $A \sim [1, n]_{\mathbb{N}}$ para algún $n \in \mathbb{N} \setminus \{0\}$.

Ejemplo 25.1.4. Sea $n \in \mathbb{N} \setminus \{0\}$ cualquiera. Como el intervalo natural $[1, n]_{\mathbb{N}}$ es equipotente a sí mismo, entonces dicho intervalo es un conjunto finito.

Ejemplo 25.1.5. El conjunto $\{\square, \diamond, \triangle, *\}$ del inicio de la Lección 24 es finito porque es equipotente al intervalo natural $[1, 4]_{\mathbb{N}}$.

25.2. Algunas propiedades de los conjuntos finitos

Veamos algunos hechos básicos sobre conjuntos finitos.

Proposición 25.2.1. *Dado $n \in \mathbb{N} \setminus \{0\}$,* **ningún** *subconjunto propio X de $[1, n]_{\mathbb{N}}$ es equipotente a $[1, n]_{\mathbb{N}}$.*

Demostración. Haremos esta demostración utilizando el *Principio de inducción matemática forma II* (ver Proposición 9.2.1). Consideremos la propiedad auxiliar

$$P(n) : \text{“ningún subconjunto propio } X \text{ de } [1, n]_{\mathbb{N}} \\ \text{es equipotente a } [1, n]_{\mathbb{N}}\text{”}.$$

Veamos que $P(n)$ es verdadera para todo natural $n \geq 1$.

1. Considerando $n = 1$, el resultado es fácil de demostrar, puesto que $[1, 1]_{\mathbb{N}} := \{1\}$ y el único subconjunto propio de $[1, 1]_{\mathbb{N}}$ es $X := \emptyset$. No es difícil ver que no existen funciones con dominio $[1, 1]_{\mathbb{N}}$ y codominio $X := \emptyset$, mucho menos que sean biyectivas. Esto prueba que $P(1)$ es verdadera.

2. Supongamos que para cierto $n \in \mathbb{N} \setminus \{0\}$ fijo (es decir $n \geq 1$) la proposición $P(n)$ es verdadera (*hipótesis de inducción*). Veamos que esto implica que $P(n + 1)$ es verdadero. Razonando por *reducción al absurdo*, supongamos que el enunciado es falso para $n + 1$. Esto significa que existe $X \subsetneq [1, n + 1]_{\mathbb{N}}$ equipotente a $[1, n + 1]_{\mathbb{N}}$. Como $[1, n + 1]_{\mathbb{N}} \sim X$, sea $f : [1, n + 1]_{\mathbb{N}} \to X$ función biyectiva. Nótese además que bajo nuestro supuesto se tiene que existe $m \in [1, n + 1]_{\mathbb{N}}$ tal que $m \notin X$ porque $X \subsetneq [1, n + 1]_{\mathbb{N}}$. Esto nos lleva a considerar las siguientes dos posibilidades que analizaremos a continuación.

   a) Supongamos que $n+1 \notin X$. Esto implica que $X \subseteq [1, n]_{\mathbb{N}}$ y consecuentemente que $f(n + 1) \neq n + 1$ (¿por qué?). Sea $a := f(n + 1) \in X \subseteq [1, n]_{\mathbb{N}}$. Claramente, $a \notin X \setminus \{f(n+1)\}$. Finalmente, consideremos la función restricción $f\mid_{[1,n]_{\mathbb{N}}}: [1, n]_{\mathbb{N}} \to X \setminus \{f(n+1)\}$ la cual es también biyectiva (¿por qué?). En conclusión, $X \setminus \{f(n+1)\} \subsetneq [1, n]_{\mathbb{N}}$ y es equipotente a $[1, n]_{\mathbb{N}}$.

   b) Supongamos que $n+1 \in X$. Como f es sobreyectiva, existe $k \in [1, n+1]_{\mathbb{N}}$ tal que $f(k) = n+1 \in X$. Consideremos la función $g : [1, n]_{\mathbb{N}} \to X \setminus \{n + 1\}$ dada por

   $$g(i) := \begin{cases} f(i), & \text{si } i \neq k; \\ f(n+1), & \text{si } i = k, \end{cases}$$

   donde $i \in [1, n]_{\mathbb{N}}$. Note que si $k = n + 1$, $g = f\mid_{[1,n]_{\mathbb{N}}}$. En cualquier caso, esta función g es biyectiva (¿por qué?). Como existe $m \in [1, n + 1]_{\mathbb{N}}$ tal que $m \notin X$, entonces $m \neq n + 1 \in X$. Luego, $m \in [1, n]_{\mathbb{N}}$ y $m \notin X \setminus \{n + 1\}$. Esto prueba que $X \setminus \{n + 1\} \subsetneq [1, n]_{\mathbb{N}}$.

Sea que $n + 1 \in X$ o no, hemos construido en cualquiera de estos dos casos una biyeción entre $[1, n]_{\mathbb{N}}$ y un subconjunto propio de él. Esto contradice la *hipótesis de inducción*.

Por el *Principio de inducción matemática forma II* (Proposición 9.2.1), tenemos que para todo $n \in \mathbb{N} \setminus \{0\}$ no existe un subconjunto propio $X \subsetneq [1, n]_{\mathbb{N}}$ equipotente a $[1, n]_{\mathbb{N}}$. ☑

Corolario 25.2.2. *Dado un conjunto finito no vacío A, no existe $B \subsetneq A$ equipotente a A.*

Demostración. Es dejada como ejercicio para el lector (utilice la Proposición 25.2.1). ☑

Como consecuencia inmediata de la Proposición 25.2.1 tenemos que dado un conjunto finito no vacío, este es equipotente a un intervalo $[1, n]_{\mathbb{N}}$ para un único $n \in \mathbb{N} \setminus \{0\}$.

Corolario 25.2.3. *Dado A conjunto finito no vacío, existe un único $n \in \mathbb{N} \setminus \{0\}$ tal que $A \sim [1, n]_{\mathbb{N}}$.*

Demostración. Sea $A \neq \emptyset$ finito. Por Definición 25.1.3, existe $n \in \mathbb{N} \setminus \{0\}$ tal que $A \sim [1, n]_{\mathbb{N}}$. Supongamos que existe $k \in \mathbb{N} \setminus \{0\}$, con $k \neq n$, tal que $A \sim [1, k]_{\mathbb{N}}$. Sin pérdida de generalidad podemos considerar que $k < n$. De esta manera, tendríamos que $X := [1, k]_{\mathbb{N}} \subsetneq [1, n]_{\mathbb{N}}$ (¿por qué?) y $[1, n]_{\mathbb{N}} \sim [1, k]_{\mathbb{N}}$ (dejamos la prueba como ejercicio para el lector, utilice la Proposición 24.1.2), lo que contradice la Proposición 25.2.1. Por lo tanto, tal $n \in \mathbb{N} \setminus \{0\}$ es único. ☑

Observación 25.2.4. Notemos que ningún intervalo natural $[1, n]_{\mathbb{N}}$ ($n \in \mathbb{N} \setminus \{0\}$) es equipotente al conjunto vacío $\emptyset$ (ejercicio para el lector).

Ahora sí podemos formalizar el concepto de *cardinal* de un conjunto finito, de manera que no haya ambigüedades, teniendo en cuenta que queremos que este concepto corresponda al *número de elementos que tiene un conjunto*.

Definición 25.2.5. Sea A un conjunto finito. Definimos el *cardinal* de A, denotado por $|A|$, de la siguiente manera:

1. Si $A := \emptyset$, definimos $|A| := 0$.

2. Si $A \neq \emptyset$, definimos $|A| := n$ donde n es el único $n \in \mathbb{N} \setminus \{0\}$ tal que $A \sim [1, n]_{\mathbb{N}}$ (el cual existe en virtud del Corolario 25.2.3).

Observación 25.2.6. Algunos autores denotan el cardinal de un conjunto como $\#(A)$ pero esto corresponde a una notación muy antigua que actualmente está en desuso.

Como consecuencia casi inmediata del Corolario 25.2.2 tenemos que el conjunto de los números naturales no es finito.

Corolario 25.2.7. $\mathbb{N}$ *no es finito.*

Demostración. Razonando por *reducción al absurdo*, supongamos que $\mathbb{N}$ es finito. Como $X := \mathbb{N} \setminus \{0\} \subsetneq \mathbb{N}$ y $\mathbb{N} \sim X$ (Ejemplo 24.1.7), esto contradice el Corolario 25.2.2. Por lo tanto, $\mathbb{N}$ no es finito. ☑

Por otro lado, veamos que todo subconjunto de un conjunto finito debe ser finito.

Proposición 25.2.8. *Si X es un conjunto finito y $Y \subseteq X$, entonces Y es también finito. Más aún, $|Y| \leq |X|$.*

Demostración. Si $X := \varnothing$, es sencillo de demostrar que si $Y \subseteq X$, entonces $Y = \varnothing$. De esta manera Y es finito y $|Y| = 0 \leq 0 = |X|$.

Supongamos que $X \neq \varnothing$. Como X es finito, existen $n \in \mathbb{N} \setminus \{0\}$ y $f : [1, n]_{\mathbb{N}} \to X$ biyectiva. Si $Y = \varnothing$, no hay nada que probar. Supongamos, por lo tanto, que también $Y \neq \varnothing$. Definamos los números k_i recursivamente, de la siguiente manera:

1. $k_1 := \text{mín}\{k \in [1, n]_{\mathbb{N}} : f(k) \in Y\} = \text{mín} f^{-1}[Y]$. Este mínimo existe porque $(\mathbb{N}, <)$ es bien ordenado, vea la Proposición 18.4.1, y porque $\mathbb{N} \supseteq \{k \in [1, n]_{\mathbb{N}} : f(k) \in Y\} \neq \varnothing$ pues $X \supseteq Y \neq \varnothing$ y f es sobreyectiva.
2. $k_{i+1} := \text{mín}\{k \in [1, n]_{\mathbb{N}} : f(k) \in Y \text{ y } k > k_i\}$, si tal mínimo existe. Note que $k_{i+1} = \text{mín} f^{-1}[Y] \setminus \{k_1, \cdots, k_i\}$.

Al intentar definir k_{i+1} es factible que ya estén agotadas todas las posibles preimágenes vía f de los elementos en Y, por lo que en algún momento el conjunto $\{k \in [1, n]_{\mathbb{N}} : f(k) \in Y \text{ y } k > k_i\}$ ya sería vacío y así no tendría mínimo (¿por qué?). Es decir, este proceso de definir k_i acaba en algún momento por la manera en que hemos definido esta sucesión. Por lo tanto, existe $m \in \mathbb{N}$ tal que la función $g : [1, m]_{\mathbb{N}} \to Y$ definida por $g(i) := f(k_i)$ es una función biyectiva. Por otro lado, por el *Principio de inducción matemática forma II* (Proposición 9.2.1) truncada podemos demostrar que para todo $i \in [1, m]_{\mathbb{N}}$ se tiene que $i \leq k_i$ (ejercicio para el lector), en particular $m \leq k_m \in [1, n]_{\mathbb{N}}$, luego $|Y| = m \leq n = |X|$. ☑

Como una consecuencia de la proposición anterior, tenemos el siguiente corolario.

Corolario 25.2.9. *(AE) Dada una función f cuyo dominio contiene a un conjunto finito X, entonces $f[X]$ es finito y $|f[X]| \leq |X|$.*

Demostración. Sea f una función tal que $X \subseteq dom(f)$ y X es finito. Note que la función $f|_X : X \to f[X]$ es sobreyectiva. Si $X = \varnothing$ entonces el resultado es evidente (¿por qué?). Si $X \neq \varnothing$, existe $n \in \mathbb{N}$ tal que $X \sim [1, n]_{\mathbb{N}}$. Luego, existe $g : [1, n]_{\mathbb{N}} \to X$ función biyectiva. Consideremos la función $h = (f|_X) \circ g : [1, n]_{\mathbb{N}} \to f[X]$. Una adaptación de la demostración de la Proposición 25.2.8 nos da el resultado que queremos. Ejercicio para el lector. ☑

Como una consecuencia casi inmediata tenemos que la unión de dos conjuntos finitos es también finito. Más aún:

Corolario 25.2.10. *Sean X y Y conjuntos finitos, entonces $X \cup Y$ es finito. Más aún, $|X \cup Y| \leq |X| + |Y|$; si X y Y son disyuntos, entonces $|X \cup Y| = |X| + |Y|$.*

Demostración. Sean X y Y conjuntos finitos. En el caso de que alguno de esos conjuntos sea el conjunto vacío, sin pérdida de generalidad supongamos que $Y := \varnothing$, tenemos que $|X \cup Y| = |X \cup \varnothing| = |X| = |X| + 0 = |X| + |Y|$ (notemos que en este caso X y Y son disyuntos).

Supongamos ahora que $X \neq \varnothing$ y $Y \neq \varnothing$, luego existen $m, n \in \mathbb{N} \setminus \{0\}$ tales que $|X| := m$ y $|Y| := n$. Sean $f : [1, m]_{\mathbb{N}} \to X$ y $g : [1, n]_{\mathbb{N}} \to Y$ biyecciones. Definamos la función $h : [1, m+n]_{\mathbb{N}} \to X \cup Y$ de la siguiente manera:

$$h(i) := \begin{cases} f(i), & \text{si } 1 \leq i \leq m \\ g(i-m), & \text{si } m+1 \leq i \leq m+n. \end{cases}$$

Notemos que h es sobreyectiva (ejercicio para el lector), aunque es factible que no sea inyectiva (en caso que X y Y no sean disyuntos). Observemos también que $h[[1, m+n]_{\mathbb{N}}] = X \cup Y$ y como $[1, m+n]_{\mathbb{N}}$ es finito (es equipotente a sí mismo), por el Corolario 25.2.9 tenemos que $h[[1, m+n]_{\mathbb{N}}] = X \cup Y$ es finito y $|X \cup Y| = |h[[1, m+n]_{\mathbb{N}}]| \leq |[1, m+n]_{\mathbb{N}}| = m+n = |X| + |Y|$. En el caso de que X y Y sean disyuntos, notemos que h sería inyectiva (ejercicio para el lector), por lo que en ese caso $|X \cup Y| = m+n = |X| + |Y|$. ☑

25.3. Ejercicios

Ejercicio 25.3.1. Demuestre que ningún intervalo natural $[1, n]_{\mathbb{N}}$ ($n \in \mathbb{N} \setminus \{0\}$) es equipotente al conjunto vacío $\varnothing$ (Observación 25.2.4).

Ejercicio 25.3.2. Demuestre que si $A \neq \varnothing$ es finito y $n, k \in \mathbb{N} \setminus \{0\}$ son tales que $A \sim [1, n]_{\mathbb{N}}$ y $A \sim [1, k]_{\mathbb{N}}$, entonces $[1, n]_{\mathbb{N}} \sim [1, k]_{\mathbb{N}}$.

Ejercicio 25.3.3. Demuestre que dado un conjunto finito no vacío A, no existe $B \subsetneq A$ equipotente a A (Corolario 25.2.2).

Ejercicio 25.3.4. Complete la demostración del Corolario 25.2.9 que nos dice que dada una función f cuyo dominio contiene a un conjunto finito X, entonces $f[X]$ es finito y $|f[X]| \leq |X|$.

Ejercicio 25.3.5. Demuestre que si X es un conjunto finito y $A \subseteq X$, entonces $|X| = |A| + |X \setminus A|$. Además, demuestre que si $A \subsetneq X$, entonces $|A| < |X|$.

Ejercicio 25.3.6. Demuestre que si X y Y son conjuntos finitos, entonces $|X \cup Y| = |X| + |Y| - |X \cap Y|$.

Ejercicio 25.3.7. Demuestre que si X es finito, entonces $\mathscr{P}(X)$ es finito. Más aún, si $|X| = n$ entonces $|\mathscr{P}(X)| = 2^n$ (sugerencia: utilice el *Principio de inducción matemática*).

Lección

veintiséis

Conjuntos infinitos

En el Corolario 25.2.7 demostramos que el conjunto de los números naturales $\mathbb{N}$ no es finito. Esto implica que ningún número natural puede asignarse como cardinal del conjunto $\mathbb{N}$. En esta lección compararemos los tamaños de los conjuntos que no son finitos y les asignaremos números cardinales. En efecto, veremos que, sorprendentemente, por aplicación del Teorema de Cantor, existen conjuntos infinitos de diferentes tamaños.

26.1. Conjuntos infinitos y conjuntos contables

Definición 26.1.1. Un conjunto A se dice *infinito* si y solo si no es finito.

Ejemplo 26.1.2. $\mathbb{N}$ es infinito (Corolario 25.2.7).

Ejemplo 26.1.3. $\mathbb{Z}$ (el conjunto de los números enteros) también es infinito, puesto que si fuera finito, como $\mathbb{Z} \sim \mathbb{N}$ (Ejemplo 24.1.4) entonces $\mathbb{N}$ también sería finito (¿por qué?).

Definición 26.1.4. Un conjunto A se dice *contable* si y solo si $A \sim \mathbb{N}$.

Observación 26.1.5. El hecho de que un conjunto sea equipotente a $\mathbb{N}$ recibe diferentes nombres en la literatura. El término que utilizamos en estas notas (ser *contable*) es la más utilizada en la literatura de la teoría de conjuntos y es la utilizada en [6], que es el texto guía del curso Introducción a la Teoría de Conjuntos de la carrera de Matemáticas de la Universidad Nacional de Colombia, sede Bogotá, motivo por el cual utilizamos este término en estas notas. Bloch, en su texto [1], llama a estos conjuntos *contablemente infinitos* (el cual no es el nombre estándar en la literatura) y hay textos que los llaman conjuntos *enumerables* (por ejemplo [8]). Siempre que se consulte un texto de matemáticas se debe revisar cuidadosamente las definiciones que hace el autor porque, como vemos en este caso, el mismo concepto recibe diferentes nombres en diferentes textos.

Definición 26.1.6. El *cardinal* del conjunto $\mathbb{N}$ es denotado por el símbolo $\aleph_0$, que se lee *alef cero*. Es decir,

$$|\mathbb{N}| := \aleph_0.$$

$\aleph$ es la primera letra del alfabeto hebreo.

Una pregunta natural después de esta definición es: ¿por qué colocamos el subíndice cero a la letra $\aleph$? ¿Acaso existen cardinales como $\aleph_1$, $\aleph_2$, etcétera? Como veremos, hay conjuntos infinitos de diferentes tamaños. Esto implicará que existen diferentes cardinales infinitos, de los cuales $\aleph_0$ es el primer cardinal infinito, es decir, $\aleph_0$ es el menor de los cardinales infinitos. Este hecho será probado. Vea la Observación 26.1.9.

Proposición 26.1.7. *Sean A y B conjuntos. Si $B \subseteq A$, B es infinito y A es contable, entonces B es contable.*

Demostración. Sean A y B conjuntos tales que $B \subseteq A$, B es infinito y A es contable. Como $A \sim \mathbb{N}$, por Definición 26.1.4, existe $f : \mathbb{N} \to A$ biyección. Recursivamente definimos la siguiente sucesión:

1. Definimos $k_0 := \text{mín}\{k \in \mathbb{N} : f(k) \in B\}$. Como B es infinito, no puede ser vacío, luego este mínimo existe por el *Principio del buen orden* de $\mathbb{N}$ (vea Proposición 18.4.1). Definamos además $g(0) := f(k_0)$.
2. Supongamos definido k_n para $n \in \mathbb{N}$ fijo. Definamos

$$k_{n+1} := \text{mín}\{k \in \mathbb{N} : f(k) \in B \text{ y } f(k) \neq g(i) \text{ para todo } i \leq n\}.$$

   Este mínimo existe por aplicación del *Principio del buen orden* en $\mathbb{N}$ porque, como B es infinito, es no vacío y así, el conjunto dado por $\{k \in \mathbb{N} : f(k) \in B \text{ y } f(k) \neq g(i) \text{ para todo } i \leq n\}$ es un subconjunto de $\mathbb{N}$ no vacío (vea Proposición 18.4.1). Definamos $g(n+1) := f(k_{n+1})$.

Notemos que para todo $n \in \mathbb{N}$ tenemos que $g(n) \in B$ y tal $g(n)$ es único porque está definido en términos del mínimo de un conjunto no vacío, que también es único. Luego, g es una función con dominio $\mathbb{N}$ y codominio B. Por esta misma definición recursiva de g, podemos ver que g es inyectiva (la justificación de este detalle es dejado como ejercicio para el lector). Veamos que g es también sobreyectiva: razonando por *reducción al absurdo*, supongamos que g no es sobreyectiva.

Por lo tanto, existe $b \in B$ tal que $g(n) \neq b$ para todo $n \in \mathbb{N}$. Como $b \in B \subseteq A$ y $f : \mathbb{N} \to A$ es biyectiva, en particular es sobreyectiva, entonces existe $k \in \mathbb{N}$ tal que $b = f(k)$. Como $b \notin rango(g)$, no puede ocurrir que $k \leq k_n$ para algún $n \in \mathbb{N}$ por la misma definición de cada uno de los elementos de la sucesión $(k_n)_{n\in\mathbb{N}}$. Consecuentemente, vemos que $k_n < k$ para todo $n \in \mathbb{N}$. Esto nos dice que el rango de la sucesión $(k_n)_{n\in\mathbb{N}}$ es finito, pero por la condición recursiva 2 vemos que realmente todos los elementos de esa suceción son diferentes, es decir, ese rango es infinito. Absurdo. Por lo tanto, $g : \mathbb{N} \to B$ es una biyección, es decir, $B \sim \mathbb{N}$. ☑

Corolario 26.1.8. *Sean A y B conjuntos tales que $B \subseteq A$. Si A es contable, entonces B es finito o es contable.*

Observación 26.1.9. Una consecuencia inmediata del anterior Corolario 26.1.8 es que $\aleph_0$ es el *primer cardinal infinito*. En efecto, si tuviéramos un cardinal λ tal que $n < \lambda$ para todo $n \in \mathbb{N}$ y $\lambda < \aleph_0$, existiría un conjunto A de cardinal λ, una función inyectiva $f : A \to \mathbb{N}$ y no existirá ninguna función sobreyectiva $g : A \to \mathbb{N}$, en particular f no sería sobreyectiva. Consecuentemente $A \sim f[A]$ y $f[A] \subsetneq \mathbb{N}$. Entonces por el Corolario 26.1.8, $f[A]$ sería finito o contable. Esto es absurdo.

Proposición 26.1.10. *Dada $f : \mathbb{N} \to A$, $f[\mathbb{N}]$ es finito o contable.*

Demostración. Sea $f : \mathbb{N} \to A$. Definimos la sucesión, de los términos k_n, recursivamente, así:

1. Definamos $k_0 := 0$.
2. Sea $n \in \mathbb{N}$ cualquiera. Supongamos que se ha definido k_i para todo $i \in \mathbb{N}$ donde $i \leq n$ y además cumplen que $f(k_i) \neq f(k_j)$ cuando $i \neq j$, para cualesquiera $i, j \in \mathbb{N}$ con $i, j \leq n$. Consideremos el conjunto

$$D_n := \{k \in \mathbb{N} : f(k_i) \neq f(k) \text{ para todo } i \in \mathbb{N} \text{ con } i \leq n\}.$$

Para cada $n \in \mathbb{N}$, tenemos dos posibles casos, que son, $D_n = \varnothing$ o $D_n \neq \varnothing$. Veamos cada uno de estos casos.

a) Si $D_n = \varnothing$, esto quiere decir que $f[\mathbb{N}]$ es finito puesto que $g : [1, n+1]_{\mathbb{N}} \to f[\mathbb{N}]$ definida por $g(i) := f(k_{i-1})$

es una función biyectiva con rango $f[\mathbb{N}]$ (dejamos como ejercicio para el lector comprobar esta afirmación). Por lo tanto, $f[\mathbb{N}]$ sería en este caso *finito*.

b) Si $D_n \neq \varnothing$, por el *Principio del buen orden* en $\mathbb{N}$ (Proposición 18.4.1) tenemos que existe el mínimo del conjunto D_n. De este modo, definimos la condición recursiva así: $k_{n+1} := \min D_n$.

Si para algún $n \in \mathbb{N}$, $D_n = \varnothing$, definitivamente $f[\mathbb{N}]$ sería finito tal y como se vió en *a*). Si por el contrario, para todo $n \in \mathbb{N}$ se tiene que $D_n \neq \varnothing$, es decir, nunca ocurre el caso *a*) anterior, entonces podemos definir una función $g : \mathbb{N} \to f[\mathbb{N}]$ dada por $n \mapsto g(n) := b_n = f(k_n)$. Por la condición recursiva de la anterior definición de la sucesión de términos k_n, vemos que $g : \mathbb{N} \to f[\mathbb{N}]$ es inyectiva (ejercicio para el lector). Además, por un argumento similar al presentado en la prueba de la Proposición 26.1.7 podemos demostrar que g es sobreyectiva (ejercicio para el lector). Por lo tanto, $g : \mathbb{N} \to f[\mathbb{N}]$ es biyectiva. Consecuentemente, en este caso, $f[\mathbb{N}]$ es *contable*. ☑

Estas proposiciones nos permiten demostrar fácilmente que la unión de dos conjuntos contables es también contable.

Proposición 26.1.11. *Dados A y B conjuntos contables, entonces $A \cup B$ es también contable.*

Demostración. Sean A y B conjuntos contables. Luego, existen funciones biyectivas $f : \mathbb{N} \to A$ y $g : \mathbb{N} \to B$. Definamos la función $h : \mathbb{N} \to A \cup B$ de la siguiente manera:

$$h(i) := \begin{cases} f(i/2), & \text{si } i \in \mathbb{N} \text{ es par;} \\ g(((i-1)/2), & \text{si } i \in \mathbb{N} \text{ es impar.} \end{cases}$$

Notemos que h es sobreyectiva (ejercicio para el lector) aunque no necesariamente inyectiva. La inyectividad fallaría en el caso en que A y B no sean disyuntos, pero realmente esto no interesa en nuestro argumento. Luego, $h[\mathbb{N}] = A \cup B$. Como $A \subseteq A \cup B$ y A es infinito, por ser contable, de la Proposición 25.2.8 tenemos que $A \cup B$ tiene que ser infinito (ejercicio para el lector). Por la Proposición 26.1.10 tenemos que $h[\mathbb{N}] = A \cup B$ es finito o contable, pero como $A \cup B$ es infinito, entonces $A \cup B$ tiene que ser contable. ☑

Para finalizar, veamos que el producto cartesiano de dos conjuntos contables es también contable.

Proposición 26.1.12. $\mathbb{N} \times \mathbb{N}$ *es contable.*

Demostración. Sea $f : \mathbb{N}\times\mathbb{N} \rightarrow \mathbb{N}$ definida por $f(k, n) := 2^k \cdot (2n+1) - 1$. Veamos que f es biyectiva:

1. Sean $(k, n), (l, m) \in \mathbb{N} \times \mathbb{N}$ tales que $f(k, n) = f(l, m)$. Por lo tanto, $2^k \cdot (2n + 1) - 1 = 2^l \cdot (2m + 1) - 1$, es decir, $2^k \cdot (2n + 1) = 2^l \cdot (2m + 1)$. Por el *Teorema fundamental de la aritmética*, Proposición 7.2.2, podemos decir que $k = l$ y que $2n + 1 = 2m + 1$. De esto, podemos decir que $2n = 2m$ y, por lo tanto, $n = m$. Así, $(k, n) = (l, m)$. Esto implica que f es inyectiva. Consecuentemente, tenemos que $\mathbb{N} \times \mathbb{N} \preceq \mathbb{N}$.

2. Sea $g : \mathbb{N} \mapsto \mathbb{N} \times \mathbb{N}$ definida por $f(m) := (0, m)$ para todo $m \in \mathbb{N}$. No es difícil ver que g es inyectiva (ejercicio para el lector). Por lo tanto, $\mathbb{N} \preceq \mathbb{N} \times \mathbb{N}$.

Puesto que $\mathbb{N} \times \mathbb{N} \preceq \mathbb{N}$ y $\mathbb{N} \preceq \mathbb{N} \times \mathbb{N}$, por el Teorema de Cantor-Schroeder-Berstein (Hecho 24.2.4) tenemos que $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$. ☑

Como un corolario de este hecho, tenemos que el producto cartesiano de dos conjuntos contables es contable.

Corolario 26.1.13. *Sean A y B conjuntos contables, entonces $A \times B$ es contable.*

Demostración. Se deja como ejercicio para el lector. ☑

Ejemplo 26.1.14. Como ya vimos anteriomente, $\mathbb{Z}$ es un conjunto contable. No es difícil ver que $\mathbb{Z} \setminus \{0\}$ es también contable (ejercicio para el lector). De esta manera, por el Corolario 26.1.13 tenemos también que $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ es un conjunto contable.

Comparemos ahora el tamaño del conjunto de los números racionales $\mathbb{Q}$ con el tamaño de $\mathbb{N} \sim \mathbb{Z}$. Sorprendentemente, $\mathbb{Q}$ tiene la misma cantidad de elementos que $\mathbb{N}$. Veamos su demostración.

Proposición 26.1.15. $\mathbb{Q}$ *es contable.*

Demostración. Consideremos la función $f : \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \to \mathbb{Q}$ definida por $f(p, q) := \frac{p}{q}$ para cualesquiera $p \in \mathbb{Z}$ y $q \in \mathbb{Z} \setminus \{0\}$. Es claro que f es sobreyectiva, por lo que $f[\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})] = \mathbb{Q}$. Del Ejemplo 26.1.14, sabemos que $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \sim \mathbb{N}$, entonces la Proposición 26.1.10 nos permite afirmar que $\mathbb{Q} = f[\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})]$ es finito o contable. Pero $\mathbb{Q}$ es infinito (¿por qué?). Por lo tanto, $\mathbb{Q}$ es contable. ☑

26.2. Conjuntos no contables

Hemos visto que los sistemas numéricos $\mathbb{N}$, $\mathbb{Z}$ y $\mathbb{Q}$ son todos contables. Una pregunta natural que nos podemos hacer es: ¿existen conjuntos infinitos que no sean contables? La respuesta a esta pregunta es afirmativa y la dio Georg Cantor en un célebre teorema que lleva su nombre.

Teorema 26.2.1 (Teorema de Cantor). *Dado cualquier conjunto A, $A \prec \mathcal{P}(A)$.*

Demostración. Sea A cualquier conjunto. La función $F : A \to \mathcal{P}(A)$ definida por $x \mapsto \{x\}$, para todo $x \in A$, es una función inyectiva (ejercicio para el lector). Por lo tanto, $A \preccurlyeq \mathcal{P}(A)$.

Veamos ahora que no hay ninguna función sobreyectiva de A en $\mathcal{P}(A)$. Razonando por el absurdo, supongamos que existe una función sobreyectiva $G : A \to \mathcal{P}(A)$. Entonces, para el conjunto $B := \{x \in A : x \notin G(x)\} \in \mathcal{P}(A)$, existiría $x \in A$ tal que $B = G(x)$. En particular, como $x \in A$, hay dos posiblidades:

1. Si $x \in B$, por la definición de B tendríamos que $x \notin G(x) = B$, contradicción.

2. Si $x \notin B = G(x)$, como $x \in A$, por la definición de B, tendríamos entonces que $x \in G(x)$, absurdo.

En resumen, cualquier posibilidad nos lleva a una contradicción. Por lo tanto, tal función G no puede existir.

De esta manera, como no hay funciones $G : A \to \mathcal{P}(A)$ sobreyectivas, en particular, tampoco existen funciones $G : A \to \mathcal{P}(A)$ biyectivas. Luego, $A \nsim \mathcal{P}(A)$ y, en consecuencia, $A \prec \mathcal{P}(A)$. ☑

Como un corolario inmediato del *Teorema de Cantor* tenemos la existencia de por lo menos un conjunto infinito no contable.

Corolario 26.2.2. $\mathcal{P}(\mathbb{N})$ *es infinito no contable.*

Demostración. Consideremos la función $F : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ definida por $n \mapsto \{n\}$, para todo $n \in \mathbb{N}$. Sabemos que F es inyectiva de la demostración del *Teorema de Cantor* 26.2.1, por lo tanto, $\mathcal{P}(\mathbb{N})$ es infinito. De lo contrario, esto implicaría que $\mathbb{N}$ sería finito, lo cual es absurdo.

Por aplicación del *Teorema de Cantor* (Teorema 26.2.1), tenemos que $\mathbb{N} \prec \mathcal{P}(\mathbb{N})$, en particular $\mathbb{N} \nsim \mathcal{P}(\mathbb{N})$. Se concluye entonces que $\mathcal{P}(\mathbb{N})$ no es contable. ☑

Observación 26.2.3. Por el Ejercicio 26.3.3, dado A cualquier conjunto, vale que $\mathcal{P}(A) \sim \{0, 1\}^A$. Recordemos que $\{0, 1\}^A$ denota el conjunto conformado por todas las funciones $f : A \to \{0, 1\}$, vea Ejercicios 22.5. En el caso en el que A es finito, suponga que $|A| = n$ para algún $n \in \mathbb{N}$, no es difícil ver que el cardinal de $\{0, 1\}^A$ es justamente $|\{0, 1\}|^{|A|} = 2^{|A|} = 2^n$. Es decir, $|\mathcal{P}(A)| = 2^{|A|}$. Motivados por este hecho, para cualquier conjunto A, definimos[1]

$$|\mathcal{P}(A)| := 2^{|A|}. \tag{26.1}$$

En particular, cuando $A = \mathbb{N}$, tendremos que

$$|\mathcal{P}(\mathbb{N})| = 2^{|\mathbb{N}|} = 2^{\aleph_0}.$$

Ahora vamos a estudiar cuál es el tamaño del conjunto de los números reales $\mathbb{R}$. Para comenzar veamos que $\mathbb{R} \nsim \mathbb{N}$. El razonamiento que utilizaremos para probar esto es conocido como *argumento diagonal de Cantor*. Esta idea ha inspirado otras demostraciones y por esto también es conocido como *método de la diagonal.*

Proposición 26.2.4. $\mathbb{R}$ *no es contable.*

[1]En el curso de Introducción a la Teoría de Conjuntos se estudia con toda rigurosidad el tema de aritmética cardinal, en el que se define la potenciación de números cardinales.

Demostración. Tenemos que $\mathbb{R}$ es infinito (¿por qué?). Razonando por reducción al absurdo, supongamos que $\mathbb{R}$ es contable. Por el Ejemplo 24.1.6, sabemos que $\mathbb{R} \sim (0, 1)$. Esto significa que $(0, 1)$ es también contable. Consideremos $f : \mathbb{N} \to (0, 1)$ una biyección.

Como todo número real $x \in (0, 1)$ tiene una representación única, con infinitos decimales, de la forma $x = 0.c_0c_1c_2 \cdots$ en la que no aparece el dígito 9 de manera periódica al final,[2] entonces para todo $n \in \mathbb{N}$ tenemos que para $f(n) \in (0, 1)$ existe una única representación decimal infinita de la forma $f(n) = 0.a_0^n a_1^n a_2^n \cdots$ sin el dígito 9 repetido periodicamente a final.

Consideremos el número $b := 0.b_0b_1b_2 \cdots$, que está en el intervalo $(0, 1)$, tal que para cualquier $k \in \mathbb{N}$

$$b_k := \begin{cases} 1, & \text{si } a_k^k \neq 1 \\ 2, & \text{si } a_k^k = 1. \end{cases}$$

Notemos que para todo $n \in \mathbb{N}$, $b_n \neq a_n^n$, en otras palabras, b difiere en la n-ésima cifra decimal del real $f(n)$ para todo $n \in \mathbb{N}$. Por lo tanto, $b \neq f(n)$ para todo $n \in \mathbb{N}$; es decir, b no tiene preimagen bajo la función f. Esto contradice el hecho de que f es una biyección pues, por lo anterior, f no es sobreyectiva. Entonces, $\mathbb{R}$ no es contable. ☑

Claramente, como $\mathbb{R}$ no es contable, su cardinal no es $\aleph_0$. Pero entonces, ¿cuál es el cardinal de $\mathbb{R}$? Para enfrentar esta pregunta recordemos que, de los Ejemplos 24.1.6 y 24.2.5, $\mathbb{R} \sim (0, 1) \sim [0, 1)$. Así que bastará con hallar el cardinal del conjunto $[0, 1)$.

El siguiente teorema tiene como consecuencia inmediata que $\mathbb{R} \sim \mathcal{P}(\mathbb{N})$, lo cual implica que

$$|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| = 2^{|\mathbb{N}|} = 2^{\aleph_0}.$$

Teorema 26.2.5. $[0, 1) \sim \mathcal{P}(\mathbb{N})$.

Demostración. Por el Teorema 24.2.4 de Cantor-Schroeder-Bernstein es suficiente con encontrar dos funciones inyectivas $f : [0, 1) \to \mathcal{P}(\mathbb{N})$ y $g : \mathcal{P}(\mathbb{N}) \to [0, 1)$.

[2] Recuerde que, por ejemplo, $0.58247\overline{9} = 0.58248\overline{0}$, vea el apéndice.

Como todo número x en $[0, 1)$ tiene una representación decimal única $x = 0.c_0c_1c_2\cdots$ donde cada c_j, $j \in \mathbb{N}$, es un dígito y no aparece el 9 repetido de forma periódica al final, entonces definimos $f : [0, 1) \to \mathscr{P}(\mathbb{N})$ como

$$f(x) = f(0.c_0c_1c_2c_3\cdots) = \{c_0, 10c_1, 10^2c_2, 10^3c_3, \cdots\},$$

para cada $x \in [0, 1)$. Por ejemplo,

$$\begin{aligned} f(0.868303\overline{0}) &= \{8, 60, 800, 3000, 0, 300000\} \subset \mathbb{N}, \\ f(0.\overline{3}) &= \{3, 30, 300, 3000, 30000, \cdots\} \subset \mathbb{N}, \\ f(0.03) &= \{0, 30\} \subset \mathbb{N}, \end{aligned}$$

etcétera. Esta función f es inyectiva (ejercicio para el lector).

Definimos la función $g : \mathscr{P}(\mathbb{N}) \to [0, 1)$ tal que para todo $X \subseteq \mathbb{N}$, $g(X) = 0.c_0c_1c_2c_3\cdots$ es el número para el cual $c_j = 1$, si $j \in X$, y $c_j = 0$, si $j \notin X$. Por ejemplo, $g(P) = 0.101010\overline{10}$, donde P es el conjunto de todos los naturales pares; $g(\mathbb{N}) = 0.111\overline{1}$, $g(\varnothing) = 0$, $g(\{0\}) = 0.1\overline{0}$, etcétera. Esta función g es inyectiva (ejercicio para el lector).

Como f y g son funciones inyectivas, tenemos que $[0, 1) \preccurlyeq \mathscr{P}(\mathbb{N})$ y $\mathscr{P}(\mathbb{N}) \preccurlyeq [0, 1)$. Por el Teorema de Cantor-Schroeder-Bernstein concluímos que $[0, 1) \sim \mathscr{P}(\mathbb{N})$. ☑

Ejemplo 26.2.6. Determinemos el cardinal del intervalo real $[0, 1]$. Como $(0, 1) \subseteq [0, 1]$, entonces $(0, 1) \preccurlyeq [0, 1]$. Como $\mathbb{R} \sim (0, 1)$, no es difícil ver que $\mathbb{R} \preccurlyeq [0, 1]$ (ejercicio para el lector). Puesto que $[0, 1] \subseteq \mathbb{R}$, entonces $[0, 1] \preccurlyeq \mathbb{R}$. Como $\mathbb{R} \preccurlyeq [0, 1]$ y $[0, 1] \preccurlyeq \mathbb{R}$, por el Teorema 24.2.4 de Cantor-Schroeder-Bernstein, tenemos que $[0, 1] \sim \mathbb{R}$. Por lo tanto, $|[0, 1]| = 2^{\aleph_0}$.

Por el Teorema de Cantor, sabemos que $2^{\aleph_0}$ es un cardinal que es mayor estricto que $\aleph_0$. Es posible demostrar que existe un primer cardinal no contable infinito[3], que es denotado por $\aleph_1$. Como consecuencia del Teorema de Cantor y de la definición de $\aleph_1$ tenemos

[3]Esta prueba utiliza los conocidos números de Hartogs y es ampliamente estudiada en el curso Introducción a la Teoría de Conjuntos, ver [6].

que $2^{\aleph_0} \geq \aleph_1$. Cantor se preguntó si $2^{\aleph_0}$ es precisamente el primer cardinal infinito no contable (pregunta que David Hilbert recogió en su famosa lista de preguntas dada en el Congreso Internacional de Matemáticas de 1900). La afirmación $2^{\aleph_0} = \aleph_1$ es la que se conoce como *hipótesis del continuo*. Esta pregunta no fue fácil de responder, de hecho Kurt Gödel construyó un universo de la teoría de conjuntos de Zermelo-Fraenkel donde esta afirmación es cierta (usando lo que se conoce como el universo de los definibles) y en los años 60 Paul Cohen (quien ganó la Medalla Fields por este trabajo) construyó un universo de la teoría de conjuntos de Zermelo-Fraenkel donde esta afirmación es falsa (usando una técnica llamada *forzamiento*, la cual es estudiada en un segundo curso de Teoría de Conjuntos). Estos dos argumentos prueban que la hipótesis del continuo es *independiente* de la Teoría de Conjuntos de Zermelo-Fraenkel, es decir, es imposible probar la hipótesis del continuo, pero también es imposible probar que es falsa, a partir de la axiomática de la teoría de conjuntos de Zermelo-Fraenkel.

Aplicando el Teorema de Cantor tantas veces como queramos, tenemos que

$$\mathbb{N} \prec \mathscr{P}(\mathbb{N}) \prec \mathscr{P}(\mathscr{P}(\mathbb{N})) \prec \mathscr{P}(\mathscr{P}(\mathscr{P}(\mathbb{N}))) \prec \cdots,$$

y aplicando la definición dada en (26.1), expuesta en la Observación 26.2.3, tenemos que

$$\aleph_0 < 2^{\aleph_0} < 2^{2^{\aleph_0}} < 2^{2^{2^{\aleph_0}}} < \cdots,$$

demostrando de esta manera que hay muchísimos cardinales no contables cada vez mayores.

26.3. Ejercicios

Ejercicio 26.3.1. Demuestre que si A y B son contables, entonces $A \times B$ es contable.

Ejercicio 26.3.2. Sea $F = \{X \in \mathscr{P}(\mathbb{N}) : X \text{ es finito}\}$. Pruebe que F es contable.

Ejercicio 26.3.3. Sea A cualquier conjunto. Demuestre que $\mathcal{P}(A)$ es equipotente a $\{0,1\}^A = \{f : f \text{ es función de } A \text{ en } \{0,1\}\}$. *Sugerencia*: a cada $B \in \mathcal{P}(A)$ asígnele la función característica χ_B.

Ejercicio 26.3.4. Sean A, B y C conjuntos arbitrarios. Pruebe que:

1. $(B \times C)^A \sim B^A \times C^A$.
2. $C^{A\times B} \sim (C^B)^A$.

Ejercicio 26.3.5. Pruebe que $\mathcal{P}(\mathbb{N})^{\mathbb{N}} \sim \mathcal{P}(\mathbb{N})$.

Ejercicio 26.3.6. Pruebe que las funciones f y g dadas en el Teorema 26.2.5 son inyectivas.

Ejercicio 26.3.7. Determine el cardinal de los siguientes conjuntos, justificando su respuesta:

1. $\mathbb{Z} \setminus \{0\}$.
2. $\{0, 1, 2\} \times \mathbb{N}$.
3. $\mathbb{Q} \setminus \mathbb{N}$.
4. El intervalo real $(0, +\infty)$.
5. $\mathcal{P}(\mathbb{Q})$.
6. El intervalo real $(-\infty, \pi]$.
7. El intervalo real $[-1, 1)$.
8. $\mathcal{P}(\mathbb{R})$.
9. $\mathbb{R} \setminus \mathbb{Q}$.

Ejercicio 26.3.8. Considere la función $f : \mathbb{R} \to \mathcal{P}(\mathbb{Q})$ definida por $x \mapsto f(x) := \{q \in \mathbb{Q} : q < x\}$. Pruebe que f es inyectiva (*sugerencia*: use el Teorema A.4.3 del apéndice). Adicionalmente, use este resultado para probar, de manera distinta a la expuesta en esta lección, que $\mathbb{R} \sim \mathcal{P}(\mathbb{N})$.

Parte VII

Apéndice

Apéndice

A

Números reales

El concepto de *número* es uno de los más profundos de las matemáticas. Su origen se remonta a los tiempos en los que la ciencia y la religión eran indistinguibles. En efecto, durante el siglo VI a.C., los estudios de la Escuela Pitagórica estaban envueltos de un cierto misticismo porque creían que existía una cierta armonía interna en el mundo que era gobernada por los números. Los números para ellos eran lo que hoy escribimos como 2, 3, 4, 5, etcétera. El mismo 1 era entendido como la unidad fundamental a partir de la cual los números eran formados. La creencia de la necesidad de tener intimidad con estos objetos abstractos acabó cuando un descubrimiento en el seno de la misma comunidad pitagórica violó uno de sus principios más fundamentales; este era que dos segmentos de recta son siempre conmensurables. El descubrimiento se dio en una figura geométrica que tiene propiedades aparentemente muy simples, el cuadrado. Específicamente, el lado y la diagonal de un cuadrado son inconmensurables. Esta situación fue estudiada por el matemático y astrónomo Eudoxo de Cnidos (408 a.C-355 a.C.), miembro de la escuela platónica, quien creó la *Teoría de las proporciones*, registrada en los *Elementos de Euclides*, justamente con el objetivo de profundizar en las grandezas inconmensurables a través de la geometría. Solamente, hasta finales del siglo XIX, por los trabajos de Richard Dedekind (1831-1916), Georg Cantor (1845-1918) y Giuseppe Peano (1858-1932) fue que el concepto de número quedó totalmente formalizado. Esta fundamentación del concepto fue motivada por las demandas teóricas que surgieron a partir del desarrollo del cálculo de Isaac Newton (1643-1727) y Gottfried Leibniz (1646-1716), en el siglo XVII.

A.1. Axiomas de cuerpo

Nuestra presentación en este apéndice de los números reales no es constructiva. De este modo, la naturaleza intrínseca de estos objetos es irrelevante y lo importante son las relaciones entre ellos. Suponemos entonces la existencia de un conjunto $\mathbb{R}$ de objetos, llamados *números reales*, dotado de dos *operaciones binarias*, llamadas *adición* $(+)$ y *multiplicación* $(\cdot)$, que satisfacen los siguientes 10 axiomas que serán especificados abajo. Todas las propiedades de los números reales pueden ser deducidas de estos axiomas. Cuando los reales son definidos por un proceso constructivo, las propiedades que listamos como axiomas deben ser probadas como teoremas.

Cuando decimos que la adición y la multiplicación son operaciones binarias nos referimos a que estas son funciones del siguiente tipo:

$$\begin{aligned} + : \mathbb{R} \times \mathbb{R} &\longrightarrow S \\ (x, y) &\longmapsto x + y, \end{aligned} \qquad \text{y} \qquad \begin{aligned} \cdot : \mathbb{R} \times \mathbb{R} &\longrightarrow P \\ (x, y) &\longmapsto x \cdot y, \end{aligned}$$

donde S y P son los conjuntos de llegada de la función adición (+) y de la función multiplicación (·), respectivamente[1]. A continuación, enunciamos el primer grupo de axiomas, que son conocidos como *axiomas de cuerpo*.

A1. ***Clausuratividad***: la adición y la multiplicación hacen corresponder a cada par de elementos x y y en $\mathbb{R}$ su *suma* $x + y$ y su *producto* $x \cdot y$ que también están en $\mathbb{R}$. Es decir, $S = \mathbb{R}$ y $P = \mathbb{R}$.

A2. ***Conmutatividad***: $x + y = y + x$ y $x \cdot y = y \cdot x$, para cualesquiera x y y en $\mathbb{R}$.

A3. ***Asociatividad***: $(x + y) + z = x + (y + z)$ y $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, para cualesquiera $x, y, z \in \mathbb{R}$.

A4. ***Modulatividad***: existen elementos $0, 1 \in \mathbb{R}$ tales que $x + 0 = x$ y $x \cdot 1 = x$ para todo $x \in \mathbb{R}$.

A5. ***Opuesto Aditivo***: para todo $x \in \mathbb{R}$ existe un elemento $y \in \mathbb{R}$ tal que $x + y = 0$.

A6. ***Inverso Multiplicativo***: para todo $x \in \mathbb{R} \setminus \{0\}$ existe un elemento $y \in \mathbb{R}$ tal que $x \cdot y = 1$.

Los números 0 y 1 que aparecen en los axiomas **A5** y **A6** son los mismos que aparecen en el axioma **A4**. De estos axiomas de cuerpo podemos deducir todas las propiedades usuales del álgebra elemental. Las más importantes de esas propiedades se encuentran en el siguiente teorema.

[1] Dado un conjunto A, una *operación binaria* sobre A es una función de $A \times A$ en A. En efecto, la adición y la multiplicación serán operaciones binarias sobre $\mathbb{R}$, pero aquí, en principio, no estamos exigiendo que el conjunto de llegada de estas operaciones sea $\mathbb{R}$ con el único propósito de resaltar en el Axioma A1 la clausuratividad de estas operaciones.

Teorema A.1.1. *Sean a, b, c y d números reales arbitrarios.*

1. *Si $a + b = a + c$, entonces $b = c$.*
2. *El número 0 del axioma* **A4** *es único.*
3. *Existe un único $x \in \mathbb{R}$ tal que $a + x = b$. Este x es denotado por $b - a$.*
4. *$b - a = b + (-a)$. En particular, $0 - a = -a$ que es llamado el inverso aditivo de a.*
5. *$-(-a) = a$.*
6. *$a(b - c) = ab - ac$.*
7. *$a \cdot 0 = 0 \cdot a = 0$.*
8. *Si $a \cdot b = a \cdot c$ y $a \neq 0$, entonces $b = c$.*
9. *El número 1 del axioma* **A4** *es único.*
10. *Si $a \neq 0$, existe un único $x \in \mathbb{R}$ tal que $a \cdot x = b$. Este x es denotado por $\frac{b}{a}$ o b/a.*
11. *Si $a \neq 0$, $\frac{b}{a} = b \cdot \frac{1}{a}$. En particular, $\frac{1}{a}$ es denotado por a^{-1} y es llamado el inverso multiplicativo de a.*
12. *Si $a \neq 0$, $(a^{-1})^{-1} = a$.*
13. *Si $a \cdot b = 0$, entonces $a = 0$ o $b = 0$.*
14. *$(-a)b = -(ab)$ y $(-a)(-b) = ab$.*
15. *$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ si $b \neq 0$ y $d \neq 0$.*
16. *$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ si $b \neq 0$ y $d \neq 0$.*
17. *$\frac{a}{b} / \frac{c}{d} = \frac{ad}{bc}$ si $b \neq 0$, $c \neq 0$ y $d \neq 0$.*

A.2. Axiomas de orden

El segundo grupo de axiomas nos permitirá establecer una relación de orden en el conjunto $\mathbb{R}$. Es por esta razón que estos axiomas son llamados *axiomas de orden*. Con este propósito suponemos que existe un subconjunto $\mathbb{R}^+ \subset \mathbb{R}$ cuyos elementos serán llamados reales positivos. Estos números positivos satisfacen los siguientes axiomas:

A7. ***Cerradura en*** $\mathbb{R}^+$**:** si $x, y \in \mathbb{R}^+$, entonces $x+y \in \mathbb{R}^+$ y $x \cdot y \in \mathbb{R}^+$.

A8. ***Tricotomía*****:** para todo real $x \neq 0$, $x \in \mathbb{R}^+$ o $-x \in \mathbb{R}^+$, pero no ambas.

A9. ***Neutralidad*****:** $0 \notin \mathbb{R}^+$.

A continuación, se definen las relaciones definidas sobre $\mathbb{R}$, representadas por los símbolos: $<$, $\leq$, $>$ y $\geq$.

Definición A.2.1. Sean $x, y \in \mathbb{R}$ cualesquiera. Decimos que:

i. x es *menor que* y (en símbolos: $x < y$) si y solo si $y - x \in \mathbb{R}^+$.

ii. x es *mayor que* y (en símbolos: $x > y$) si y solo si $y < x$.

iii. x es *menor o igual que* y (en símbolos: $x \leq y$) si y solo si $x < y$ o $x = y$.

iv. x es *mayor o igual que* y (en símbolos: $x \geq y$) si y solo si $y \leq x$.

Adicionalmente, diremos que:

v. x es *positivo* si y solo si $x > 0$.

vi. x es *negativo* si y solo si $x < 0$.

vii. x es *no positivo* si y solo si $x \leq 0$.

viii. x es *no negativo* si y solo si $x \geq 0$.

Sean x, y y z reales. Es muy usual, cuando tenemos dos desigualdades del tipo $x < y$ y $y < z$, escribir simplemente: $x < y < z$. Del mismo modo, por ejemplo, $x \leq y < z$ significa que $x \leq y$ y

$y < z$. De manera similar interpretamos las cadenas de desigualdades: $x < y \leq z$ y $x \leq y \leq z$.

De estos axiomas de orden podemos deducir todas las reglas que nos permitirán trabajar con desigualdades. Las más importantes de esas propiedades se encuentran listadas en el siguiente teorema.

Teorema A.2.2. *Sean a, b, c y d números reales arbitrarios.*

1. *Vale una y solo una de las siguientes tres afirmaciones: $a < b$ o $b < a$ o $a = b$.*
2. *Si $a < b$ y $b < c$, entonces $a < c$.*
3. *Si $a < b$, entonces $-a > -b$. En particular, si a es negativo, $-a$ es positivo.*
4. *Si $a < b$ y $c > 0$, entonces $ac < bc$.*
5. *Si $a \neq 0$, entonces $a^2 > 0$.*
6. $1 > 0$.
7. *Si $a < b$ y $c < 0$, entonces $ac > bc$.*
8. *Si $a < c$ y $b < d$, entonces $a + b < c + d$.*
9. *Si $ab > 0$, entonces ambos son positivos o ambos son negativos.*
10. *La suma de dos números negativos es negativa.*
11. *Si $a > 0$, entonces $a^{-1} > 0$. Si $a < 0$, entonces $a^{-1} < 0$.*
12. *Si $0 < a < b$, entonces $0 < b^{-1} < a^{-1}$.*
13. *Si $a \leq b$ y $b \leq c$, entonces $a \leq c$.*
14. *Si $a \leq b$ y $b \leq a$, entonces $a = b$.*
15. *Si $a \leq b \leq c$ y $a = c$, entonces $b = c$.*
16. *Si $a^2 + b^2 \geq 0$ y a y b no son ambos cero, entonces $a^2 + b^2 > 0$.*
17. *Si $0 \leq a < \epsilon$ para todo $\epsilon > 0$, entonces $a = 0$.*

Note que evidentemente $a \leq a$ para cualquier $a \in \mathbb{R}$. Esta propiedad junto con las propiedades consignadas en los numerales 13 y 14 muestran que $\leq$ es en efecto una relación de orden definida sobre $\mathbb{R}$ y este orden $\leq$ es conocido como el *orden usual* en $\mathbb{R}$. Es más, por el numeral 1 del anterior teorema vemos fácilmente que $(\mathbb{R}, \leq)$ es un conjunto totalmente ordenado.

A.3. Sistemas numéricos

Uno de los sistemas numéricos contenidos en $\mathbb{R}$ es el de los *números naturales*. El conjunto de los números naturales será denotado por la letra $\mathbb{N}$. Los números naturales son los utilizamos para contar y además están asociados con la idea de cantidad. Para mostrar la existencia de los números naturales comenzamos con los números 0 y 1 que aparecen citados en el Axioma A4. Como $0 < 1$, por el Teorema A.2.2(6.), es claro que $0 \neq 1$. Es más, $0+1 = 1$ por el Axioma A4. Los objetos: $1+1$, $(1+1)+1$, $((1+1)+1)+1$, $(((1+1)+1)+1)+1$, $\cdots$, son todos números reales por el Axioma A1. El número $1 + 1$ será denotado por 2, $2 + 1$ será denotado por 3, $3 + 1$ será denotado por 4, $4 + 1$ será denotado por 5, y así sucesivamente. Los números reales $0, 1, 2, 3, 4, 5, \cdots$, obtenidos al sumar 1 repetidamente son los llamados números naturales. Para referirnos a cada uno de los números naturales usamos la numeración en base 10 o decimal que es en la que usamos 10 símbolos que están en el siguiente conjunto

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

Este conjunto es llamado conjunto de los dígitos.

A pesar de que esta descripción de los elementos de $\mathbb{N}$ pueda parecernos muy clara e intuitiva lo cierto es que no es nada rigurosa porque las expresiones "así sucesivamente", "sumar 1 repetidamente" o inclusive el símbolo "$\cdots$", no son absolutamente claros. No hay duda de que es necesaria una definición mucho más precisa y detallada de los números naturales, y aunque hay varias formas de hacerlo, nos saltaremos esa definición aquí y diremos simplemente que:

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, \cdots\},$$

es el conjunto de los números naturales.

Consideremos ahora los inversos aditivos de cada uno de los números naturales. Del Teorema A.1.1(4) sabemos que el inverso aditivo de cualquier número real a es denotado por $-a$. Por lo tanto, -1, -2, -3, -4, -5, $\cdots$, son también números reales. Sería redundante considerar -0 en la lista anterior porque $-0 = 0$ (¿por qué?). El conjunto conformado por todos los números naturales juntos a sus opuestos aditivos es el conjunto de los números *enteros*, el cual será denotado por $\mathbb{Z}$, en referencia a la primera letra de la palabra alemana *zahl*, que quiere decir número. Más precisamente:

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

es el conjunto de los números enteros. El conjunto conformado por todos los números naturales distintos al 0 es llamado el conjunto de los números *enteros positivos* el cual será denotado por $\mathbb{Z}^+$. El conjunto conformado por todos los opuestos aditivos de los elementos de $\mathbb{Z}^+$ es llamado el conjunto de los números enteros negativos y será denotado por $\mathbb{Z}^-$. Más exactamente:

$$\mathbb{Z}^+ = \{1, 2, 3, 4, 5, \cdots\},$$

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

En conclusión,

$$\mathbb{Z} = \mathbb{Z}^- \cup \{0\} \cup \mathbb{Z}^+.$$

Si se estuviera presentando un estudio riguroso del sistema de los números reales, en este punto tendríamos que demostrar ciertas propiedades de los números enteros como las que están consideradas en la Sección 6.2 como axiomas. Esto no se detallará aquí.

Debido al Teorema A.1.1(10) podemos considerar las fracciones $\frac{m}{n}$ en el caso particular en el que $m, n \in \mathbb{Z}$, con $n \neq 0$. El conjunto conformado por todos estos números que se expresan como cociente o razón de dos números enteros es llamado el conjunto de los números *racionales*, que será denotado por la letra $\mathbb{Q}$, en referencia a la primera letra de la palabra italiana *quoziente*, vea la Definición 7.2.4. Es decir,

$$\mathbb{Q} = \left\{\frac{m}{n} \ : \ m \in \mathbb{Z} \text{ y } n \in \mathbb{Z} - \{0\}\right\}.$$

El lector puede comprobar que $\mathbb{Q}$ satisface todos los axiomas de cuerpo y todos los axiomas de orden consignados arriba. Para referirnos a esto diremos simplemente que $\mathbb{Q}$ es un cuerpo ordenado. Por lo tanto, todos los teoremas que se deducen de estos axiomas también son válidos cuando tomamos como universo de referencia al conjunto $\mathbb{Q}$ a cambio de $\mathbb{R}$. Pero, entonces ¿qué tienen de diferente los cuerpos ordenados $\mathbb{Q}$ y $\mathbb{R}$? Volvamos al descubrimiento "desafortunado" de los pitagóricos. Supongamos que la diagonal y el lado de un cuadrado son conmensurables[2]. Digamos que la diagonal mide mu y el lado nu, donde u es la medida de un tercer segmento que es submúltiplo común de la diagonal y del lado del cuadrado. Por el Teorema de Pitágoras se deduce que:

$$m^2u^2 = (mu)^2 = (nu)^2 + (nu)^2 = 2n^2u^2.$$

Esto implica que $m^2 = 2n^2$, lo cual es absurdo porque m^2 se descompone en una cantidad par de factores primos y, en cambio, $2n^2$ en una cantidad impar de factores primos. Esto es contradictorio con la unicidad de la descomposición de un número natural en factores primos como muestra el Teorema fundamental de la aritmética 7.2.2. Así es claro que la diagonal y el lado de un cuadrado no son conmensurables pero además, como la relación $m^2 = 2n^2$, lo cual equivale a que $\left(\frac{m}{n}\right)^2 = 2$, no se puede dar, entonces, no existe un número racional cuyo cuadrado sea 2, vea la Proposición 7.2.7. Esto nos muestra que existen números que no son racionales. En efecto, el último de los axiomas de los números reales, el *axioma del extremo superior,* nos permitirá mostrar la existencia de otros números reales que no son racionales. Esos otros números reales que no son racionales son los llamados números *irracionales*. El conjunto de los números irracionales será denotado por $\mathbb{I}$. De hecho, $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$, con $\mathbb{Q} \cap \mathbb{I} = \varnothing$.

[2]Dos segmentos de recta cualesquiera, $\overline{AB}$ y $\overline{CD}$, se dicen *conmensurables* si y solo si existe un tercer segmento $\overline{EF}$ contenido un número entero de veces en $\overline{AB}$ y un número entero de veces en $\overline{CD}$. También se dice que $\overline{EF}$ es un *submúltiplo común* de $\overline{AB}$ y $\overline{CD}$.

A.4. Axioma del extremo superior

El último axioma que establece el sistema de los números reales, llamado *Axioma del extremo superior*, o también llamado *Axioma de completez*, es el que marca la diferencia existente entre los cuerpos ordenados $\mathbb{Q}$ y $\mathbb{R}$.

A10. ***Del extremo superior***: todo conjunto no vacío V de números reales acotado superiormente tiene extremo superior; esto significa que existe un número real α tal que $\alpha = \sup V$.

Vale la pena mencionar que si el lector no sabe el contenido de la Lección 17, será muy difícil para él comprender el enunciado del anterior axioma. Sin embargo, si el lector conoce esa lección, no sobra resaltar que el extremo superior del conjunto V no pertenece necesariamente a V. En efecto, $\sup V$ está en V si y solo si V tiene máximo, es decir, $\max V = \sup V$.

El siguiente teorema contiene algunas propiedades importantes que son consecuencia del axioma de completez.

Teorema A.4.1.

1. *Todo conjunto no vacío $W \subset \mathbb{R}$ acotado inferiormente posee extremo inferior.*

2. *El conjunto $\mathbb{Z}^+$ no está acotado superiormente.*

3. *Para cada $x \in \mathbb{R}$ existe $n \in \mathbb{Z}^+$ tal que $n > x$.*

4. *Si $x > 0$ y $y \in \mathbb{R}$ cualquiera, entonces existe $n \in \mathbb{Z}^+$ tal que $nx > y$.*

5. *Si tres números reales a, x y y satisfacen las desigualdades*

$$a \leq x \leq a + \frac{y}{n},$$

para todo entero $n \geq 1$, entonces $x = a$.

La proposición enunciada en el numeral 4 del anterior teorema es llamada *Propiedad arquimediana* del sistema de los números reales. Se llama así porque Arquímedes consideró esta como una propiedad geométrica fundamental de la recta real, en efecto, la incluyó como uno de los axiomas de la geometría[3].

Demostración.

1. Sea W cualquier conjunto no vacío de números reales acotado inferiormente. Consideremos el conjunto

$$V = \{x \in \mathbb{R} \ : \ \text{existe } y \in W \text{ tal que } x = -y\},$$

conformado por todos los números que son opuestos aditivos de los elementos de W. Luego, V es no vacío y acotado superiormente porque W, por hipótesis, es no vacío y acotado inferiormente. Por el Axioma A10 sabemos que existe un número $\alpha \in \mathbb{R}$ tal que $\alpha = \sup V$. Note que $-\alpha = \text{ínf}\, W$ (¿por qué?). Esto significa que existe un número real $\beta = -\alpha$ tal que $\beta = \text{ínf}\, W$.

2. Supongamos que $\mathbb{Z}^+$ es acotado superiormente. Como $\mathbb{Z}^+$ no es vacío, el Axioma A10 nos asegura que $\mathbb{Z}^+$ tiene extremo superior. Digamos que $\sigma = \sup \mathbb{Z}^+$. Note que $\sigma - 1 < \sigma$ no puede ser cota superior de $\mathbb{Z}^+$. Por lo tanto, existe $n \in \mathbb{Z}^+$ tal que $n > \sigma - 1$, o mejor: $n + 1 > \sigma$. Como $n + 1 \in \mathbb{Z}^+$, esto niega que σ sea una cota superior de $\mathbb{Z}^+$. Absurdo.

3. Si no fuera así, x sería una cota superior de $\mathbb{Z}^+$. Esto es contradictorio con el numeral anterior.

4. Basta aplicar el numeral anterior pero cambiando x por $\frac{y}{x}$.

5. Es dejado como ejercicio para el lector.

☑

Una forma equivalente de enunciar la Proposición 7.2.7 ($\sqrt{2}$ no es racional) es diciendo que la ecuación $x^2 = 2$ no tiene solución en $\mathbb{Q}$. Veremos a continuación que usando el Axioma A10 se puede demostrar que la ecuación $x^2 = a$ tiene solución en $\mathbb{R}$ cuando $a \geq 0$.

Teorema A.4.2. *Para cada real no negativo a existe un único real no negativo x tal que $x^2 = a$.*

---

[3]Desde el siglo XIX se han construido geometrías no arquimedianas que son aquellas en las que la propiedad arquimediana no es válida.

Demostración. Sea $a \geq 0$ cualquiera. Si $a = 0$, $x = 0$ es la única solución para $x^2 = 0$. Entonces, supongamos que $a > 0$. Consideremos

$$V = \{x \in \mathbb{R} : x > 0 \text{ y } x^2 \leq a\}.$$

Note que V es no vacío y acotado superiormente (¿por qué?). Así, por aplicación del axioma A10, existe $\beta \in \mathbb{R}$ tal que $\beta = \sup V$. Claramente $\beta > 0$ (¿por qué?). Por el numeral 1 del Teorema A.2.2 vale una y solo una de las siguientes tres afirmaciones: $\beta^2 < a$ o $\beta^2 > a$ o $\beta^2 = a$.

Supongamos que $\beta^2 < a$. Luego, $a - \beta^2 > 0$, y como $\beta > 0$, entonces $(a - \beta^2)/3\beta > 0$. Por lo tanto, existe $\gamma > 0$ tal que $\gamma < \beta$ y $\gamma < (a - \beta^2)/3\beta$. Esto implica que

$$(\beta + \gamma)^2 = \beta^2 + 2\beta\gamma + \gamma^2 < \beta^2 + 2\beta\gamma + \beta\gamma < \beta^2 + (a - \beta^2) = a,$$

porque $3\beta\gamma < a - \beta^2$. Esto muestra que $\beta + \gamma \in V$, lo cual es contradictorio con que β es la menor de las cotas superiores de V porque $\beta < \beta + \gamma$. En conclusión, no se puede dar que $\beta^2 < a$.

Supongamos que $\beta^2 > a$. Mostraremos que $\gamma = \frac{1}{2}\left(\beta + \frac{a}{\beta}\right) > 0$ siendo menor que β es también cota superior de V. Notemos primero que

$$\gamma = \frac{2\beta^2 - \beta^2 + a}{2\beta} = \beta - \frac{\beta^2 - a}{2\beta} < \beta,$$

porque $\frac{\beta^2 - a}{2\beta} > 0$. Es decir, $0 < \gamma < \beta$.

Ahora,

$$\gamma^2 = \beta^2 - (\beta^2 - a) + \frac{(\beta^2 - a)^2}{4\beta^2} = a + \frac{(\beta^2 - a)^2}{4\beta^2} > a.$$

Entonces, $\gamma^2 > x^2$ para todo $x \in V$, o mejor, $\gamma > x$ para todo $x \in V$. En conclusión, γ es cota superior de V pero γ es menor que β que es la menor de las cotas superiores de V. Esto es absurdo. Así que es imposible que valga $\beta^2 > a$.

La única opción posible es $\beta^2 = a$. ☑

En general, si $n \in \mathbb{Z}^+$ impar, para todo $a \in \mathbb{R}$ existe un único $x \in \mathbb{R}$ tal que $x^n = a$. Y si $n \in \mathbb{Z}^+$ es par, para todo $a \in \mathbb{R}$, no negativo, existe un único $x \in \mathbb{R}$, no negativo, tal que $x^n = a$. En estos casos, tal x se llama raíz n-ésima de a y se denota por: $x = a^{1/n}$ o $x = \sqrt[n]{a}$. En el caso en que n es par, $x^n \geq 0$ para todo $x \in \mathbb{R}$, por lo que la ecuación $x^n = a$ no tiene sentido cuando a es negativo. Estos resultados pueden ser probados usando el Axioma A10, sin embargo las pruebas no las expondremos aquí porque se estudian en el curso Cálculo Diferencial en Una Variable.

Adicionalmente, no sobra decir que, si $\frac{m}{n} \in \mathbb{Q}$ y $x \neq 0$, se define $x^{\frac{m}{n}} := (x^m)^{1/n}$, es decir, $x^{\frac{m}{n}}$ es la raíz n-ésima de x^m, siempre que esta exista.

Teorema A.4.3 (Densidad de $\mathbb{Q}$ en $\mathbb{R}$). *Suponga que $x, y \in \mathbb{R}$ tales que $x < y$. Entonces existe un $q \in \mathbb{Q}$ tal que $x < q < y$.*

Demostración. Sea $k \in \mathbb{Z}^+$ mayor que $\frac{1}{y-x}$. Esto es posible porque $\mathbb{Z}$ no es acotado superiormente en $\mathbb{R}$. Entonces, $\frac{1}{k} < y - x$. Sean $m, n \in \mathbb{Z}$ tales que $m < x < n$ y consideremos el conjunto

$$A = \left\{ j \in \mathbb{N} \,:\, m + \frac{j}{k} > x \right\}.$$

Note que $m + \frac{k(n-m)}{k} = n > x$, lo que significa que $k(n-m) \in A$. Es decir, $A \neq \varnothing$. Por el Principio del buen orden, vea la Proposición 18.4.1, existe $l = \min A$. Como $0 \notin A$, porque $m + \frac{0}{k} = m < x$, entonces $l > 0$. Luego, $l - 1 \in \mathbb{N}$ pero $l - 1 \notin A$ porque l es el menor de los elementos de A. Por lo tanto, $m + \frac{l-1}{k} \leq x$.

Tomemos $q = m + \frac{l}{k} \in \mathbb{Q}$. Como $l \in A$ entonces $q > x$. Además,

$$q = m + \frac{l}{k} = m + \frac{l-1}{k} + \frac{1}{k} \leq x + \frac{1}{k} < x + (y - x) = y.$$

En conclusión, $x < q < y$ como queríamos.

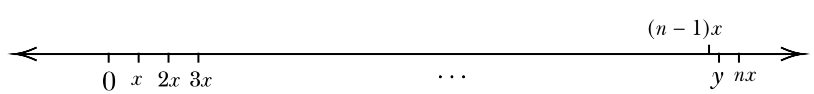
☑

A.4.1. Representación de $\mathbb{R}$

Como el lector debe estar familiarizado, usamos la recta para representar el conjunto de los números reales. Adoptando un conjunto de axiomas adecuados para la geometría euclideana se puede mostrar que a cada número real le corresponde uno y solo un punto de la recta y, recíprocamente, a cada punto de la recta le corresponde uno y solo un número real. Este hecho permite que tratemos indistintamente las expresiones *punto de la recta* y *número real*. Así que cuando ubiquemos el número real x en la recta también podemos decir que x es un punto de la recta. Por todo esto nos referimos a $\mathbb{R}$ como *la recta real*.

Para representar los números reales en la recta elegimos un punto para representar el 0 y otro a la derecha del 0 para representar al 1. Esta elección determina la escala en la recta y con esto podemos determinar fácilmente cualquier número entero o racional en la recta. Todos los números que están a la derecha del 0 son los números positivos y todos los que están a la izquierda son los negativos. Además, el punto x está a la izquierda del punto y si y solo si $x < y$.

Esta representación geométrica de $\mathbb{R}$ es una ayuda inmensa porque nos permite entender mejor ciertas propiedades. Aunque en estas notas nos hemos concentrado principalmente en mostrar cómo se pueden escribir las demostraciones de teoremas, no podemos descartar para nada las intuiciones sobre los objetos que estudiamos. Por ejemplo, en el caso de $\mathbb{R}$, la intuición geométrica sobre la recta algunas veces es mucho más contundente que una demostración analítica soportada exclusivamente en los axiomas de los números reales. A continuación, presentamos una gráfica que nos ayuda a entender mejor la propiedad arquimediana, vea el Teorema A.4.1(4). Sean $x > 0$ y y cualquier real. Existe $n \in \mathbb{Z}^+$ tal que $nx > y$. Intuitivamente, si avanzamos desde 0 con pasos de tamaño x, sin importar que tan pequeño sea x, existe una cantidad finita $n \in \mathbb{Z}^+$ de pasos, este n podría ser gigante, que al realizarlos nos permiten superar a y.



Informalmente, si pudieramos resaltar de algún modo en la recta únicamente los puntos correspondientes a los números racionales, estos serían una cantidad contable de puntos[4] y obtendríamos una recta incompleta. Esto sería, intuitivamente, una recta con un número incontable de "huecos" porque $\mathbb{R} \setminus \mathbb{Q}$ no es contable, vea el Ejercicio 26.3.7. Estos "huecos" corresponderían a los números irracionales. Así que podemos decir que los irracionales completan la recta. En efecto, diremos que $\mathbb{R}$ es *completo* mientras que $\mathbb{Q}$ no lo es. Este ejercicio intuitivo explica porqué el Axioma del extremo superior es también llamado *Axioma de completez*.

A.5. Ejercicios

Ejercicio A.5.1. Sean x, y números reales positivos. Pruebe que si $p, q \in \mathbb{Q}$, entonces

1. $x^p x^q = x^{p+q}$.
2. $(x^p)^q = x^{pq}$.
3. $(x y)^p = x^p y^p$.

¿Estas igualdades valen para cualesquiera $x, y \in \mathbb{R}$?

[4] $|\mathbb{Q}| = \aleph_0$, es decir, $\mathbb{Q}$ es contable, vea la Proposición 26.1.15.

Apéndice

B

Sistemas deductivos clásicos

Desde la reforma del 2008, en la Universidad Nacional de Colombia se venía enseñando en el curso Fundamentos de Matemáticas los sistemas deductivos proposicionales y de predicados clásicos. Realmente muy pocos libros de fundamentos de matemáticas desarrollan estos temas; de hecho, de los textos guía utilizados en nuestro curso –[1, 5, 8]– el único que hace "algo" de estos temas es [1], pero realmente no lo hace con mucho detalle. Como parte del proceso de autoevaluación, desde hace un par de años empezamos la discusión en el interior del Departamento de Matemáticas sobre la conveniencia de reemplazar estos temas por algunos que potencialmente puedan ser más útiles para un estudiante que acaba de iniciar su pregrado en Matemáticas o carreras afines, como por ejemplo el principio de inducción matemática y las definiciones recursivas. Sin embargo, hay colegas que piensan que desarrollar estos sistemas deductivos puede ayudar al estudiante a afianzar la mecánica al realizar demostraciones en matemáticas. En contraste, otros piensan que es suficiente con que dichas estrategias de demostración estén basadas en argumentos semánticos (valores de verdad). Como esto hace parte todavía de la discusión, decidimos dejar los sistemas deductivos clásicos dentro de estas notas, pero a manera de apéndice.

B.1. Sistema deductivo proposicional clásico

En las primeras lecciones basamos nuestros argumentos en hallar todos los posibles valores de verdad de diferentes tipos de proposiciones. Esto es, estudiamos las proposiciones desde el punto de vista semántico. Sin embargo, no es así como se realizan demostraciones de teoremas en matemáticas, en las cuales comenzamos desde afirmaciones que suponemos *a priori* verdaderas –que denominamos *hipótesis*–, pasando por proposiciones que están debidamente justificadas; es decir, son consecuencias de las anteriores e implican la siguiente, hasta llegar a la conclusión o *tesis*. Consideremos el siguiente conjunto de proposiciones:

Si estudias otras culturas, aprenderás que existen diversas costumbres.
Si aprendes que existen diversas costumbres, evaluarás tus propias costumbres.
Por lo tanto, si estudias otras culturas, evaluarás tus propias costumbres.

Esta colección o conjunto de proposiciones es un ejemplo de un *argumento*. Entenderemos por *argumento* un conjunto finito de proposiciones $\alpha_1, \cdots, \alpha_n, \beta$ donde las primeras proposiciones $\alpha_1, \cdots, \alpha_n$ son llamadas *premisas* y la última β es llamada *conclusión*. Denotaremos esto por: $\alpha_1, \cdots, \alpha_n / \beta$.

Un conjunto finito de proposiciones arbitrario, donde no hay relación entre las afirmaciones que lo componen, no corresponde a los argumentos que deseamos estudiar. Justamente por esto, será necesario distinguir entre argumentos válidos de inválidos. Intuitivamente, un argumento es *válido* cuando su conclusión es consecuencia directa de sus premisas y un argumento es *inválido* simplemente si no es válido. Cuando decimos que una proposición β es consecuencia directa de otras $\alpha_1, \cdots \alpha_n$ queremos decir que suponiendo $\alpha_1, \cdots, \alpha_n$ (premisas) verdaderas podemos concluir que β (conclusión) es verdadera. Pero, ¿cómo obtenemos conclusiones verdaderas a partir de proposiciones que suponemos verdaderas? Una manera de hacerlo es realizando un análisis de valores de verdad de las premisas y la conclusión como se hizo en la Sección 3.2 de la Lección 3 (viendo que las premisas implican semánticamente la conclusión). Este análisis podría ser muy tedioso y ocultaría la esencia de los razonamientos que empezaremos a estudiar en esta lección.

Cuando queremos estudiar si una implicación semántica complicada se tiene, lo que podemos hacer es descomponer dicha afirmación en una sucesión de implicaciones semánticas más simples de manipular que sean conocidas. En este momento, la pregunta sería cuáles de esas implicaciones semánticas más simples debemos considerar de manera que con ellas se pueda capturar todos los posibles argumentos válidos.

Dichas implicaciones semánticas que escogeremos para tal fin las llamaremos *reglas de inferencia*.

B.1.1. Las reglas de inferencia del sistema deductivo proposicional clásico

Un *sistema deductivo* se compone de una serie de proposiciones que siempre vamos a poder introducir en cualquier argumento –que llamaremos *axiomas*– y unas reglas de inferencia. La idea es que si tenemos una semántica desarrollada en el contexto en el que estemos trabajando, los axiomas sean siempre tautologías y que las reglas de inferencia sean compatibles con los valores de verdad de las premisas de las que partimos y de la conclusión del argumento.

En esta parte estudiaremos un sistema deductivo que es conocido como *cálculo proposicional clásico*. No daremos un sistema deductivo a la Hilbert (muchos axiomas y pocas reglas de inferencia –generalmente Modus Ponens–), sino por simplicidad daremos una presentación equivalente que es denominada *deducción natural* (una regla general para introducir axiomas y muchas reglas de inferencia).

Basaremos las reglas de inferencia del *cálculo proposicional clásico* en las implicaciones semánticas estudiadas los Ejemplos 3.2.4, 3.2.5 y en el Ejercicio 3.5.2.

1. Modus Ponens (MP): de la afirmación $\alpha \to \beta$ y de α podemos concluir β. Esto lo denotamos por

$$\alpha \to \beta, \alpha \vdash \beta.$$

2. Modos Tollendo Ponens (MTP): de las afirmaciones $\alpha \vee \beta$ y $\neg\alpha$ podemos concluir β, lo que denotamos por

$$\alpha \vee \beta, \neg\alpha \vdash \beta,$$

y de las afirmaciones $\alpha \vee \beta$ y $\neg\beta$ podemos concluir α, lo que denotamos por

$$\alpha \vee \beta, \neg\beta \vdash \alpha.$$

3. Modus Tollendo Tollens (MTT): de las proposiciones $\alpha \to \beta$ y $\neg\beta$ podemos concluir $\neg\alpha$. Esto lo denotamos por

$$\alpha \to \beta, \neg\beta \vdash \neg\alpha.$$

4. Silogismo hipotético (SH): de las afirmaciones $\alpha \to \beta$ y $\beta \to \gamma$ podemos concluir $\alpha \to \gamma$. Esta regla la denotamos por

$$\alpha \to \beta, \beta \to \gamma \vdash \alpha \to \gamma.$$

5. Doble negación (DN): de α podemos concluir $\neg\neg\alpha$, lo que denotamos por

$$\alpha \vdash \neg\neg\alpha,$$

y de $\neg\neg\alpha$ podemos concluir α, lo que denotamos por

$$\neg\neg\alpha \vdash \alpha.$$

6. Introducción de la conjunción (I$\wedge$): de las proposiciones α y β podemos concluir $\alpha \wedge \beta$, lo que denotamos por

$$\alpha, \beta \vdash \alpha \wedge \beta.$$

7. Eliminación de la conjunción (E$\wedge$): de la proposición $\alpha \wedge \beta$ podemos concluir tanto α, lo que denotamos por

$$\alpha \wedge \beta \vdash \alpha,$$

como β, lo que denotamos por

$$\alpha \wedge \beta \vdash \beta.$$

8. Introducción de la disyunción (I$\vee$): de α podemos concluir $\alpha \vee \beta$, lo que denotamos por

$$\alpha \vdash \alpha \vee \beta.$$

9. Dilema constructivo (DC): de las proposiciones $\alpha \to \beta$ y $\gamma \to \delta$ podemos concluir $(\alpha \vee \gamma) \to (\beta \vee \delta)$, lo que denotamos por

$$\alpha \to \beta, \gamma \to \delta \vdash (\alpha \vee \gamma) \to (\beta \vee \delta).$$

Una deducción de β con premisas $\alpha_1, \cdots, \alpha_n$ es una sucesión finita de proposiciones $\gamma_1, \cdots, \gamma_k$ donde cada γ_i, con $i = 1, \cdots, k-1$, es:

1. axioma,
2. alguna de las proposiciones α_j (que llamamos premisas),
3. o se obtuvo usando alguna de las reglas de inferencia anteriores aplicadas con las proposiciones γ_l que aparecen previamente en dicha lista.
4. $\gamma_k = \beta$.

En tal caso, diremos que β es *teorema* de $\alpha_1, \cdots, \alpha_n$, lo que denotaremos por $\alpha_1, \cdots, \alpha_n \vdash \beta$.

Ejemplo B.1.1. Queremos ver que $p \to \neg q, q \vdash \neg p$. Nuestras premisas son las afirmaciones $p \to \neg q$ y q (es de lo que tenemos que partir) y tenemos que deducir $\neg p$. Lo primero que tenemos que analizar es cómo podemos obtener lo que se nos solicita (en este caso $\neg p$) a partir de la información que tenemos ($p \to \neg q$ y q). Mirando las reglas de inferencia descritas atrás, como p es el antecedente de una implicación que tenemos como premisa ($p \to \neg q$) y tenemos que obtener $\neg p$, la regla que deberíamos utilizar es Modus Tollendo Tollens. Pero para poder utilizar esta regla, deberíamos tener la negación del consecuente de dicha implicación $p \to \neg q$, es decir, deberíamos tener $\neg\neg q$. Pero directamente no tenemos esta proposición, realmente tenemos como premisa la afirmación q, pero a la luz de las reglas de inferencia dadas anteriormente podemos obtener $\neg\neg q$ a partir de q usando la regla de la doble negación. El anterior análisis no corresponde realmente a la deducción formal solicitada, pero nos da una idea de la manera para construirla. A continuación, daremos la deducción formal del anterior argumento.

1.	$p \to \neg q$	Premisa.
2.	q	Premisa.
3.	$\neg\neg q$	DN 2. (esto dice que aplicamos la regla DN a la proposición 2 en la lista).
4.	$\neg p$	MTT 1, 3. (esto dice que aplicamos la regla MTT a las proposiciones 1 y 3 de la lista).

Ejemplo B.1.2. Queremos realizar una deducción formal del argumento $p \vee \neg q, q \vee (p \vee r), \neg p \vdash r$. Es decir, partiendo de las proposiciones $p \vee \neg q$, $q \vee (p \vee r)$, $\neg p$ (premisas de nuestro argumento) tenemos que concluir r. Como queremos concluir r, analizamos que la podríamos obtener a partir de la proposición $q \vee (p \vee r)$ que tenemos como premisa, pero para lograrlo primero deberíamos tener sólo $p \vee r$, lo que se obtendría utilizando Modos Tollendo Ponens, en el caso de que podamos incluir en el argumento $\neg q$. Pero para obtener $\neg q$ necesitamos tener $\neg p$ para poder aplicar Modus Tollendo Ponens en la proposición $p \vee \neg q$. Pero nosotros tenemos $\neg p$ como premisa, por lo tanto, podemos concluir $p \vee r$. Para obtener r, debemos tener en nuestro argumento $\neg p$ para poder aplicar Modos Tollendo Ponens a $p \vee r$, pero recordemos que tenemos a $\neg p$ como premisa. Como en el ejemplo anterior, este análisis no es la deducción formal, pero es una descripción de la manera como debemos escribir dicha deducción.

1.	$p \vee \neg q$	Premisa.
2.	$q \vee (p \vee r)$	Premisa.
3.	$\neg p$	Premisa.
4.	$\neg q$	MTP 1, 3. (esto dice que aplicamos la regla MTP a las proposiciones 1 y 3 de la lista).
5.	$p \vee r$	MTP 2, 4. (esto dice que aplicamos la regla MTP a las proposiciones 2 y 4 de la lista).
6.	r	MTP 3, 5. (esto dice que aplicamos la regla MTP a las proposiciones 3 y 5 de la lista).

B.1.2. Regla de reemplazo

En una deducción, vamos a permitir reemplazar una proposición por alguna que sea semánticamente equivalente. Esta regla se conoce como *regla de reemplazo*.

Es decir, si α y β son proposiciones que son semánticamente equivalentes (recordemos, esto quiere decir que tienen la misma tabla de verdad), entonces de α podemos deducir β (en símbolos, $\alpha \vdash \beta$) y de β podemos deducir α (es decir, $\beta \vdash \alpha$).

Ejemplo B.1.3. Veamos una deducción de $\neg(p \to q) \vdash p$. Directamente no podríamos obtener p, ya que no podemos usar directamente ninguna de las reglas vistas anteriormente. Así que usamos una proposición semánticamente equivalente a nuestra premisa adecuada. Recordemos que una implicación $p \to q$ es falsa si p es verdadera y q es falsa, luego no es complicado demostrar que $\neg(p \to q) \equiv p \wedge \neg q$ (ejercicio). De esta afirmación equivalente a nuestra premisa, podemos obtener directamente p por medio de la eliminación de la conjunción. Por lo tanto, la deducción queda de la siguiente manera:

1.	$\neg(p \to q)$	Premisa.
2.	$p \wedge \neg q$	Reemplazo 1. $\neg(p \to q) \equiv p \wedge \neg q$
3.	p	E$\wedge$ 2.

B.1.3. Validez de argumentos proposicionales

Recordemos que un *argumento* es una sucesión finita de proposiciones $\alpha_1, \cdots, \alpha_n/\beta$. Decimos que el argumento $\alpha_1, \cdots, \alpha_n/\beta$ es *válido* si y sólo si $\alpha_1, \cdots, \alpha_n \models \beta$. Caso contrario, diremos que el argumento es *inválido*.

Ejemplo B.1.4. Veamos que el argumento $p \to q, p \wedge r/q$ es válido, es decir, $p \to q, p \wedge r \models q$. Supongamos que q es falso. Veamos que no es posible que ambas premisas de este argumento sean verdaderas simultáneamente bajo este supuesto. Nótese que el valor de verdad de $p \wedge r$ no depende del valor de verdad de q.

1. Supongamos ahora que $p \wedge r$ es verdadera y veamos que en este caso la premisa $p \to q$ debe ser falsa. Puesto que $p \wedge r$ es verdadera en este caso, tanto p como r son verdaderas. Así p es verdadera y q es falsa en este caso, entonces $p \to q$ es falsa.

2. Supongamos que $p \to q$ es verdadera y veamos que bajo este supuesto $p \wedge r$ no puede ser verdadera. Como q es falsa y $p \to q$ es verdadera, la única opción de valor de verdad para p es que sea falso. Por lo tanto, $p \wedge r$ es falsa.

Hemos visto que, suponiendo que q es falsa, alguna de las premisas es falsa. Por lo tanto, el argumento es válido.

Ejemplo B.1.5 (Modus Ponens erróneo). El argumento $\alpha \to \beta, \beta/\alpha$ *no* es válido, ya que $\alpha \to \beta, \beta \not\models \alpha$ (Ejemplo 3.2.6).

Hay que tener cuidado con este argumento erróneo, es un error muy común de los estudiantes que apenas están empezando a mirar estos temas a usar el erróneo argumento $\alpha \to \beta, \beta/\alpha$ como si fuera válido.

Observación B.1.6. Si un argumento $\alpha_1, \cdots, \alpha_n/\beta$ es válido, tendremos la seguridad de que podremos dar una deducción para $\alpha_1, \cdots, \alpha_n \vdash \beta$. Este resultado se conoce como *Teorema de completitud*. Pero en el caso de que $\alpha_1, \cdots, \alpha_n/\beta$ no sea válido, con certeza no podremos encontrar una deducción con premisas $\alpha_1, \cdots, \alpha_n$ y conclusión β. Esto nos lo garantiza el *Teorema de validez*. La demostración del *Teorema de completitud* y del *Teorema de validez* se escapa del objetivo y del nivel de estas notas, así que no las daremos aquí. Los lectores curiosos pueden encontrarlas en libros de lógica matemática como [2, 3].

Observación B.1.7. Verificar que un argumento $\alpha_1, \cdots, \alpha_n/\beta$ sea válido (argumento semántico) no es lo mismo que dar una deducción formal en el sistema deductivo (argumento sintáctico, usando las reglas de inferencia). A pesar de que los Teoremas de completitud y validez del cálculo proposicional clásico implican que argumentos sintácticos son equivalentes a argumentos semánticos, cuando se pida verificar la validez de un argumento se pide hacer un argumento semántico (es decir, usando valores de verdad) y cuando se pida la deducción del argumento se pide hacer un argumento sintáctico (es decir, usando las reglas de inferencia vistas atrás).

B.1.4. Regla indirecta reducción al absurdo

Algunas veces no podemos deducir una proposición β directamente de unas proposiciones $\alpha_1, \cdots, \alpha_n$. Una forma de argumentación utilizada en la antigua Grecia consistía en suponer que tanto $\alpha_1, \cdots, \alpha_n$

son verdaderas pero que β es falsa (es decir, $\neg\beta$ es verdadera) y si llegaban a una contradicción es porque la afirmación β era verdadera.

Notemos que en la Proposición 3.3.1 vimos que si $\perp$ es una contradicción y $\alpha_1, \cdots, \alpha_n, \neg\beta \models \perp$, entonces tenemos que $\alpha_1, \cdots, \alpha_n \models \beta$.

Argumentando vía validez de argumentos, podemos introducir la siguiente regla de inferencia indirecta, que denominaremos *reducción al absurdo* (RA):

Si $\alpha_1, \cdots, \alpha_n, \neg\beta \vdash \perp$, entonces tenemos que $\alpha_1, \cdots, \alpha_n \vdash \beta$.

Esta regla de inferencia la denominamos *indirecta* puesto que la idea inicial es deducir β a partir de $\alpha_1, \cdots, \alpha_n$, y utilizando esta regla de inferencia no deducimos directamente a β sino que suponiendo $\neg\beta$ como premisa adicional, lo que realmente deducimos es una contradicción.

Ejemplo B.1.8. Analicemos el argumento $p \to q, p \to r / p \to (q \vee r)$. De las reglas de inferencia dadas anteriormente, la única manera de obtener un condicional es utilizando la regla silogismo hipotético (SH), pero en este caso aquí no la podemos usar directamente. Así que intentemos un argumento indirecto utilizando la regla de inferencia indirecta reducción al absurdo (que abreviaremos RA).

1.	$p \to q$	Premisa.
2.	$p \to r$	Premisa.
3.	$\neg(p \to (q \vee r))$	Premisa adicional (RA).
4.	$p \wedge \neg(q \vee r))$	Reemplazo 3 $\neg(p \to (q \vee r)) \equiv p \wedge \neg(q \vee r))$.
5.	p	E$\wedge$ 4.
6.	q	MP 1, 5.
7.	$\neg(q \vee r)$	E$\wedge$ 4.
8.	$\neg q \wedge \neg r$	Reemplazo Leyes de De Morgan.
9.	$\neg q$	E$\wedge$ 8.
10.	$q \wedge \neg q$	I$\wedge$ 6, 9.
11.	$p \to (q \vee r)$	RA 3, 10.

Analicemos esta deducción. En la líneas 1 y 2 hemos colocado las premisas originales del argumento que estamos estudiando y en la línea 3 hemos colocado como premisa adicional la negación de lo que nos piden deducir.

En la línea 10 de esta deducción hemos obtenido una contradicción: $q \wedge \neg q$. Por lo tanto, apelando a la regla RA aplicada a las proposiciones 3 (negación de lo que queremos deducir) y 10 (la contradicción obtenida) en la siguiente línea podemos colocar la proposición que buscamos deducir: $p \to (q \vee r)$.

Observemos que en esta deducción no obtenemos directamente lo que nos piden, sino que entre las líneas 3 a la 10 hacemos una deducción auxiliar. Para indicar esto, entre esas líneas colocamos una línea vertical a la izquierda de esta deducción auxiliar. Note que la línea 11 ya no tiene esa línea vertical a su izquierda, puesto que ya no hace parte de la deducción auxiliar.

B.1.5. Regla indirecta Teorema de la deducción

La única regla de inferencia que nos permite deducir un condicional es el silogismo hipotético (SH), pero únicamente se puede utilizar si tenemos en nuestra deducción proposiciones de la forma $\alpha \to \beta$ y $\beta \to \gamma$, lo que nos permitiría deducir $\alpha \to \gamma$, pero no siempre lo que nos piden obtener tiene este patrón. En el fondo, podemos entender $\models$ como un condicional, si lo vemos desde el punto de vista de su interpretación. En la Proposición 3.4.1 vimos la siguiente implicación semántica:

Sean $\alpha_1, \cdots, \alpha_n, \alpha, \beta$ proposiciones. Si $\alpha_1, \cdots, \alpha_n, \alpha \models \beta$, entonces tenemos que $\alpha_1, \cdots, \alpha_n \models \alpha \to \beta$.

Si reemplazamos $\models$ por $\vdash$, obtenemos la siguiente regla de inferencia, que denominaremos *Teorema de la deducción* (abreviado como TD):

Si $\alpha_1, \cdots, \alpha_n, \alpha \vdash \beta$, entonces tenemos que $\alpha_1, \cdots, \alpha_n \vdash \alpha \to \beta$.

Ejemplo B.1.9. Veamos una deducción indirecta del argumento $p \to q, p \to r / p \to (q \wedge r)$, usando la regla de inferencia TD.

1.	$p \to q$	Premisa.
2.	$p \to r$	Premisa.
3.	$\mid p$	Premisa adicional TD.
4.	$\mid q$	MP 1, 3.
5.	$\mid r$	MP 2, 3.
6.	$\mid q \wedge r$	I$\wedge$ 4, 5.
7.	$p \to (q \wedge r)$	TD 3, 6.

Nótese que no hemos realizado una deducción directa del condicional $p \to (q \wedge r)$, sino que en la línea 3 colocamos p (el antecedente de lo que queremos deducir) como premisa adicional hasta que obtenemos en la línea 6 el consecuente de lo pedido: $q \wedge r$. Así, en la línea 7 colocamos $p \to (q \wedge r)$ apelando a la regla TD aplicada a p (línea 3 de la deducción) y a $q \wedge r$ (línea 6 de la deducción). Además, observemos que desde la línea 3 hasta la línea 6 corresponde a la deducción auxiliar que utilizamos para poder aplicar TD, razón por la cual al lado izquierdo de las proposiciones entre estas líneas colocamos una línea vertical continua para indicar que esto hace parte de dicha deducción auxiliar.

B.2. Reglas de inferencia del cálculo de predicados clásico

Como habíamos visto antes, el cálculo proposicional clásico dejaba de lado el análisis de la estructura interna de las afirmaciones y solo se centra en la forma como las afirmaciones se conectaban externamente con otras, lo que deja por fuera el análisis de propiedades de los objetos considerados y de cuantificar en los argumentos. Entonces, nos vemos en la necesidad de introducir reglas de inferencia que nos permitan trabajar tanto con propiedades (predicados) como con cuantificadores, vea la Lección 4. El objetivo de esta sección es introducir dichas reglas de inferencia asociadas a cuantificadores y trabajar argumentos desde este punto de vista.

En esta parte, las constantes van a representar elementos fijos de un conjunto de referencia donde estemos trabajando, que denotaremos por letras minúsculas, usualmente $a, b, c,$ etc.

Desde este punto de vista, vamos a considerar las siguientes reglas de inferencia:

1. Las mismas reglas del cálculo proposicional clásico.
2. Introducimos nuevas reglas de inferencia relacionadas con los cuantificadores.
    i. (Especificación del universal, $E\forall$) Dada cualquier constante c,
    $$\forall x\varphi(x) \vdash \varphi(c).$$
    Esta regla nos dice que si en un argumento tenemos que una propiedad φ vale para todo elemento de un conjunto de referencia, en particular esa propiedad φ vale para cualquier elemento de ese conjunto que hayamos fijado.
    ii. (Especificación del existencial, $E\exists$)
    $$\exists x\varphi(x) \vdash \varphi(c),$$
    siempre y cuando c sea una constante que no haya aparecido en el argumento. Esta regla nos dice que si en un argumento hemos llegado a una expresión de la forma $\exists x\varphi(x)$, podemos exhibir un elemento representado por una constante que cumpla la propiedad φ. Aquí es muy importante resaltar que debemos usar una constante c que no haya aparecido antes en el argumento; ilustremos el motivo de esta exigencia con un ejemplo: en el conjunto de los estudiante de Fundamentos de Matemáticas es cierto que la afirmación $\forall x E(x)$ es cierta, donde $E(x)$ es el predicado $E(x)$: "x es estudiante". Supongamos que la constante p representa a *Perencejo*, quien es estudiante de Física y no de Matemáticas que está viendo el curso de Fundamentos. Por otro lado, si la afirmación $\exists x M(x)$ es cierta, donde $M(x)$ es el predicado $M(x)$: "x es estudiante de Matemáticas", no la podemos especificar con la misma letra p que ya aparecía en el contexto y además no cumple

el predicado $M(x)$. El problema potencial que surge al especificar existenciales con constantes que ya aparecían en el contexto, es precisamente que no hay garantía de que el objeto que representa esa constante cumpla realmente la propiedad pedida, como vimos en el ejemplo anterior.

Cuando en un argumento tengamos un universal y un existencial, se sugiere especificar primero la afirmación existencial y luego especificar la afirmación universal (en el caso de la especificación del universal no hay limitaciones, puesto que en ese caso la propiedad vale para cualquier elemento del universo, en particular para aquel que cumple la propiedad existencial). Es un error muy común en los estudiantes especificar primero la propiedad universal y luego la propiedad existencial con la misma constante con la que se especificó la propiedad universal. Hay que tener mucho cuidado, por el posible problema que se puede presentar, que analizamos atrás.

iii. (Generalización del universal, $G\forall$)

$$\varphi(c),\ c \text{ constante arbitraria} \vdash \forall x\varphi(x).$$

Esta regla de inferencia nos dice que si en un argumento tenemos que el predicado $\varphi(c)$ vale donde c es una constante que no es fija (es decir, representa cualquier elemento de nuestro conjunto de referencia), entonces podemos concluir $\forall x\varphi(x)$. En este caso, c no debe representar a un elemento particular del conjunto de referencia, sino que representa cualquier elemento del conjunto de referencia. Un error muy común de los estudiantes es generalizar el universal a partir de un existencial. Consideremos nuestro ejemplo dado atrás, donde el conjunto de referencia es la colección de estudiantes del curso de Fundamentos de Matemáticas. Si s es una constante que representa a Sutano, quien es estudiante de Matemáticas, tenemos que $\exists xM(x)$ es cierto y de hecho lo podemos especificar con la constante s, obteniendo $M(s)$. Pero de esta afirmación no podemos generalizar el universal y así obtener $\forall xM(x)$, pues de hecho habíamos considerado que había un estudiante del curso, Perencejo, quien no era estudiante de Matemáticas; el error aquí consiste en que s no representa a cualquier elemento del conjunto de referencia sino que representa a un estudiante fijo (Sutano).

iv. (Generalización del existencial, $G\exists$)

$$\varphi(c), \text{ alguna constante } c \vdash \exists x \varphi(x)$$

Esta regla nos dice que si para algún elemento fijo se tiene una afirmación, podemos concluir que existe un elemento que cumple dicha afirmación.

Ejemplo B.2.1. Dar una deducción del siguiente argumento

$$\forall x(P(x) \to Q(x)), \exists x(\neg Q(x) \wedge R(x)) / \exists x(\neg P(x)).$$

1.	$\forall x(P(x) \to Q(x))$	Premisa.
2.	$\exists x(\neg Q(x) \wedge R(x))$	Premisa.
3.	$\neg Q(c) \wedge R(c)$	$E\exists$ 2, c constante fija. (Primero especificamos las expresiones existenciales. Aquí podemos especificar con cualquier constante c, ya que aún no hay ninguna constante en el contexto).
4.	$P(c) \to Q(c)$	$E\forall$ 1. (Especificamos el universal en 1, pues esa afirmación universal vale para cualquier elemento; en particular para aquel que satisface el existencial dado en 2).
5.	$\neg Q(c)$	E$\wedge$ 3.
6.	$\neg P(c)$	MTT 5, 4.
7.	$\exists x(\neg P(x))$	$G\exists$ 6. (Como hay una constante que satisface $\neg P(x)$, así vale que $\exists x(\neg P(x))$).

Ejemplo B.2.2. Dar una deducción de

$$\forall x(P(x) \in Q(x)), \forall x(Q(x) \to R(x)) / \forall x(P(x) \to R(x)).$$

1.	$\forall x(P(x) \in Q(x))$	Premisa.
2.	$\forall x(Q(x) \to R(x))$	Premisa.
3.	$P(c) \to Q(c)$	$E\forall$ c arbitraria. (Nótese que aquí c no representa una constante fija como en el paso 3 del ejemplo anterior, sino que representa un elemento arbitrario).
4.	$Q(c) \to R(c)$	$E\forall$ donde c fue dada en 3.
5.	$P(c) \to R(c)$	SH 3, 4.
6.	$\forall x(P(x) \to R(x))$	$G\forall$ 5. (Podemos generalizar el universal en 6, dado que la constante tomada en 3 y 4 representa un elemento arbitrario y no fijo como cuando especificamos un existencial).

Ejemplo B.2.3. Dar una deducción del siguiente argumento: todo número entero es par o impar. Existe un número entero que no es impar que es primo. Entonces existe un número entero que es par y primo.

Lo primero que tenemos que hacer es identificar los predicados más sencillos que aparecen en este argumento

$$
\begin{aligned}
E(x) &: \text{“}x \text{ es un número entero”.}\\
I(x) &: \text{“}x \text{ es impar”.}\\
P(x) &: \text{“}x \text{ es par”.}\\
R(x) &: \text{“}x \text{ es primo”.}
\end{aligned}
$$

De esta manera, las premisas de nuestro argumento quedan simbolizados en lenguaje lógico de la siguiente manera:

$\forall x(E(x) \to (P(x) \vee I(x)))$, que afirma que todo número entero es par o impar; $\exists x(E(x) \wedge \neg I(x) \wedge R(x))$, que nos dice que existe un número entero que no es impar que es primo.

La conclusión de este argumento queda simbolizado de la siguiente manera: $\exists x(E(x) \wedge P(x) \wedge R(x))$, esto afirma que existe un número entero que es par y primo. Veamos una deducción de este argumento:

1.	$\forall x(E(x) \rightarrow (P(x) \vee I(x)))$	Premisa.
2.	$\exists x(E(x) \wedge \neg I(x) \wedge R(x))$	Premisa.
3.	$E(c) \wedge \neg I(c) \wedge R(c)$	$E\exists$ 2, donde c representa una constante particular fija. (Nótese que especificamos primero afirmaciones existenciales antes que las afirmaciones universales, aquí c representa un entero que no es impar y es primo).
4.	$E(c) \rightarrow (P(c) \vee I(c))$	$E\forall$ 3.
5.	$E(c)$	$E\wedge$ 3.
6.	$P(c) \vee I(c)$	MP 5, 4.
7.	$\neg I(c)$	E$\wedge$ 3.
8.	$P(c)$	MTP 6, 7.
9.	$R(c)$	E$\wedge$ 3.
10.	$E(c) \wedge P(c) \wedge R(c)$	I$\wedge$ 5, 8, 9.
11.	$\exists x(E(x) \wedge P(x) \wedge R(x))$	$G\exists$ 10.

B.3. Ejercicios

Ejercicio B.3.1. Dé una deducción de los siguientes argumentos válidos, usando reglas de inferencia:

1. $(p \vee q) \rightarrow (r \vee s), (r \vee s) \rightarrow (t \wedge u), p/u$.
2. $(n \vee o) \rightarrow p, (p \vee q) \rightarrow r, q \vee n/r$.
3. O bien el gerente no notó el cambio o lo aprobó. Él notó el cambio, por lo tanto, debe haberlo aprobado.
4. Si una función f de valor y variable real es diferenciable en un punto $a \in \mathbb{R}$ entonces es continua en a. Si f es continua en a, entonces $f(a)$ está definida y $\lim_{x \to a} f(x) = f(a)$. Pero f no está definida en a. Por lo tanto, f no es diferenciable en a.
5. $p \rightarrow q, r \rightarrow s, (\neg q \vee \neg s) \wedge (\neg p \vee \neg q) /\neg p \vee \neg r$.

6. $p \to (q \wedge \neg r), (q \vee r) \to s, p \ /s.$

Ejercicio B.3.2. Señale en las siguientes estructuras sintácticas cuándo se trata de premisas (p) y cuándo de conclusiones (c).

a) Teniendo en cuenta____, y puesto que____, habría entonces que____.
b) Si_____, y_____, entonces_____.
c) _____, ya que _____.
d) Porque_____ y _____, _____
e) _____ y _____ porque_____ y _____.
f) _____ pues _____.
g) De _____ y _____, se deduce _____.
h) _____ se sigue de _____.
i) Suponiendo _____ tenemos que _____, luego _____.
j) Solo bajo la condición de _____ se puede admitir _____.
k) Acepto _____ pero si _____, pues _____ y _____.
l) Debido a _____, y considerando _____, tendríamos que _____.

Ejercicio B.3.3. Use las reglas de inferencia del cálculo de predicados clásico para dar una deducción de los siguientes argumentos:

1. Todos los celulares con cámara y plan de datos consumen mucha energía. Todo iPhone es un celular. Todo iPhone tiene cámara. Hay iPhones que no consumen mucha energía. Entonces hay celulares sin plan de datos.

2. Todo alumno que haga el taller correctamente entiende las nociones básicas. Juan es estudiante, pero no entiende las nociones básicas. Por lo tanto, Juan es un estudiante que no hace el taller correctamente.

3. Todo número es alef o es beth. Un número es alef si y solo si es guímel y no es dálet. Hay un número que es dálet. Por lo tanto, hay un número que es beth.

4. Ningún número impar es divisible por dos. Cinco es un número entero que no es par. Todo número entero es par o impar. Por lo tanto, cinco no es divisible por dos.

Referencias

[1] E. Bloch, *Proofs and fundamentals*, 2^a ed., Springer, New York, USA, 2011.

[2] X. Caicedo, *Elementos de lógica y calculabilidad*, 2^a ed., Una Empresa docente (Universidad de los Andes), Bogotá, Colombia, 1990.

[3] L. den Dries, *Mathematical Logic (Lecture Notes)*, disponible en https://faculty.math.illinois.edu/~vddries/main2.pdf.

[4] H. D. Ebbinghaus, J. Flum, and W. Thomas, *Mathematical Logic*, 2^a ed., Springer, NYC, USA, 1994.

[5] R. Hammack, *Book of Proof*, 2^a ed., Richard Hammack (publisher), Richmond, USA, 2013.

[6] K. Hrbacek y T. Jech, *Introduction to Set Theory*, 3^a ed., Taylor and Francis Group, Boca Raton, USA, 1999.

[7] K. Rosen, *Elementary Number Theory*, 5^a ed., Addison-Wesley, Reading, USA, 2005.

[8] D. J. Velleman, *How To Prove It*, 2^a ed., Cambridge University Press, Cambridge, UK, 2006.

[9] F. Zalamea, *Fundamentos de Matemáticas*, Facultad de Ciencias, Universidad Nacional de Colombia, Bogotá, Colombia, 2007.

Índice