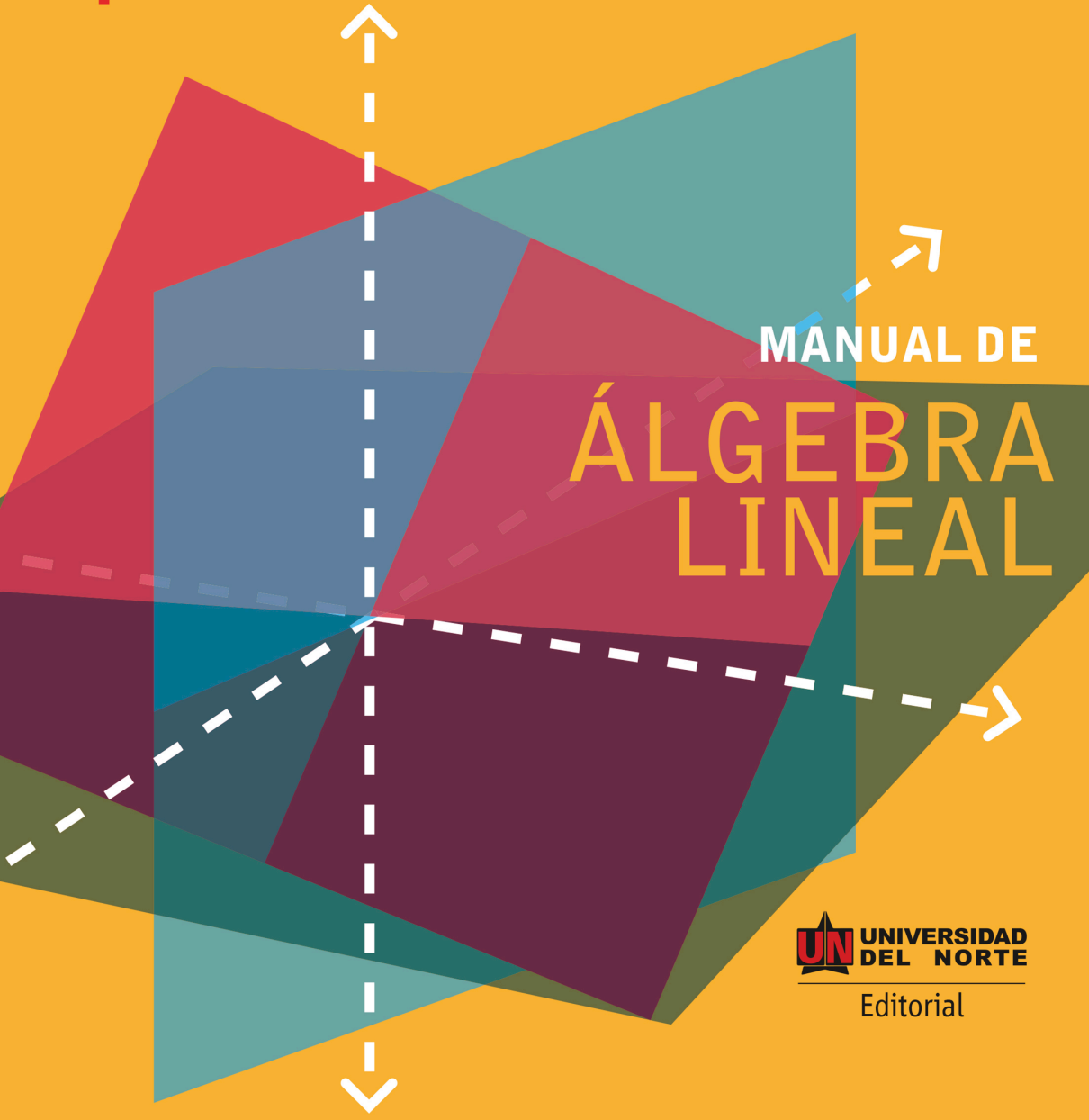
Sebastián Castañeda Hernández
Agustín Barrios Sarmiento
Ismael Gutiérrez García



MANUAL DE ÁLGEBRA LINEAL

UN UNIVERSIDAD DEL NORTE
Editorial

Manual de Álgebra lineal

Manual de Álgebra lineal

Sebastián Castañeda Hernández
Agustín Barrios Sarmiento
Ismael Gutiérrez García

Área metropolitana
de Barranquilla (Colombia), 2017

UNIVERSIDAD DEL NORTE
Editorial

Castañeda Hernández, Sebastián.
Manual de Álgebra líneal / Sebastián Castañeda Hernández, Agustín Barrios Sarmiento, Ismael Gutiérrez García. – Barranquilla, Colombia : Editorial Universidad del Norte, 2017.

viii, 218 p. : il. ; 24 cm.
Incluye referencias bibliográficas
ISBN 978-958-741-847-7 (impreso)
ISBN 978-958-741-848-4 (pdf)

1. Álgebras lineales. I. Barrios Sarmiento, Agustín. II. Gutiérrez García, Ismael. I.tít.

(512.5 C346 ed. 23) (CO-BrUNB)

UNIVERSIDAD DEL NORTE
Vigilada Mineducación
www.uninorte.edu.co
Km 5, vía a Puerto Colombia, A.A. 1569
Área metropolitana de Barranquilla (Colombia)

Sebastián Castañeda Hernández, Agustín Barrios Sarmiento,
Ismael Gutiérrez García

Coordinación editorial
Zoila Sotomayor O.

Diagramación
Sebastián Castañeda Hernández

Diseño de portada
Joaquín Camargo Valle

Corrección de textos
Nury Ruiz Bárcenas

Impreso y hecho en Colombia
La Imprenta Editores (Bogotá)
Printed and made in Colombia

LOS AUTORES

SEBASTIÁN CASTAÑEDA HERNÁNDEZ
Licenciado en Matemáticas de la Universidad del Atlántico (Colombia). Magíster en Ciencias matemáticas de la Universidad del Valle en convenio con la Universidad del Norte (Colombia). Docente de tiempo completo del departamento de Matemáticas y Estadística de la Universidad del Norte desde 1988. Ha publicado con la Editorial Universidad del Norte varios textos de álgebra lineal, así como de fundamentos de matemáticas y teoría de números.

AGUSTÍN BARRIOS SARMIENTO
PhD de la Facultad de Matemáticas de la Universidad de Valencia (España). Profesor asociado de la Universidad del Norte (Colombia), adscrito al Departamento de Matemáticas y Estadística. Su principal línea de investigación es la Optimización que le permite construir modelos que recrean situaciones reales, entre las que se encuentran: procesos de fabricación por lotes, construcción de infraestructuras, mantenimiento de sistemas complejos y desarrollo e introducción en el mercado de nuevos productos, entre otros.

ISMAEL GUTIÉRREZ GARCÍA
PhD en Ciencias Naturales de la Universidad Johannes Gutenberg de Mainz (Alemania). Magíster en Matemáticas de la Universidad del Valle (Colombia) y licenciado en Matemáticas y Física de la Universidad del Atlántico (Colombia). Profesor-investigador de la Universidad del Norte (Colombia). Posee una amplia experiencia como docente universitario y además ha liderado proyectos de investigación en el área de matemáticas discretas y sus aplicaciones, concretamente en teoría clásica de códigos y en códigos de subespacios.

Contenido

Prólogo

El presente texto puede considerarse como una simplificación del libro "Introducción al Álgebra Lineal" [3], de dos de los autores de este manual. Aquí se presenta un material mínimo para desarrollar en un semestre con tres horas semanales presenciales. La idea básica es que el texto sea utilizado como material de lectura obligatoria para los estudiantes, incluyendo lecturas en algunas sesiones presenciales en las cuales como control se entreguen tareas individuales o en parejas, a criterio del profesor. En ese sentido el manual incluye tareas de entrega obligatoria por parte del estudiante.

El contenido cubierto por el manual, como se puede apreciar, es el básico en un primer curso de álgebra lineal dirigido a estudiantes de primer semestre de Ingeniería, Economía, Administración de empresas, o programas donde la asignatura sea electiva. Para estudiantes de Ciencias (Física o Matemáticas, especialmente) el profesor podrá recomendar la profundización de los temas en el texto citado [3] o en otros textos adecuados. El capítulo uno introduce la definición de operación binaria y, en particular, la de ley de composición interna, a partir de ejemplos familiares que permitan una fácil comprensión a través de la lectura individual para el estudiante. Se introducen también las definiciones de las estructuras algebraicas básicas sobre las cuales se construye la estructura principal: la de espacio vectorial.

El capítulo dos aborda el estudio de los sistemas lineales y de las matrices sobre el campo real. Se introduce inicialmente la estructura de espacio vectorial de $\mathbb{R}^n$ así como el producto escalar y el producto matricial como herramientas teóricas importantes en el estudio de ecuaciones y sistemas lineales. En este mismo capítulo, en su apéndice, se muestra el caso de las ecuaciones lineales diofantinas y se sugiere el uso de software libre específico para cálculos en álgebra lineal. Se incluye también un primer acercamiento al concepto de determinante, para el caso de sistemas 2×2. Tal concepto será extendido en

el capítulo tres a matrices $n \times n$. Por razones de brevedad en la exposición, el desarrollo del material relativo a determinantes se limita en buena parte a presentar los resultados más importantes, citando el texto base de este manual.

El capítulo cuatro se dedica a los sistemas homogéneos y a los subespacios de $\mathbb{R}^n$, aprovechando el contexto para introducir con rigurosidad los conceptos de base y dimensión de subespacios de $\mathbb{R}^n$. Se cierra el capítulo con los conceptos de norma y vectores unitarios, introduciendo las definiciones de ángulo entre vectores, paralelismo y dirección desde un punto de vista algebraico. Estos conceptos serán interpretados geométricamente en el capítulo cinco, dedicado a los vectores en $\mathbb{R}^2$ y $\mathbb{R}^3$ y a las aplicaciones geométricas de los resultados antes obtenidos.

Se incluyen, además del correspondiente al capítulo dos, tres apéndices al final. En el apéndice A, se hace una breve presentación del símbolo sumatorio y sus principales propiedades y en el B se presenta el alfabeto griego. En el apéndice C se presenta una breve introducción a la Teoría de códigos, de suma importancia en la teoría de la información. Básicamente, el objetivo de la teoría de códigos es codificar información que se transmite a través de canales "ruidosos"; es decir, susceptibles de distorsionar la información ya sea por razones internas o externas (por acción de terceros). Es entonces necesario que el mensaje sea codificado adecuadamente de manera que se pueda verificar su autenticidad y detectar posibles errores o distorsiones y corregirlos, de ser posible. En tal sentido, los códigos lineales (subespacios de $\mathbb{K}^n$, siendo $\mathbb{K}$ un campo finito) juegan un papel importante.

Finalmente, agradecemos cualquier comentario, sugerencia o corrección que consideren necesarios para mejorar la presente edición. Los autores.

scasta@uninorte.edu.co
abarrios@uninorte.edu.co
isgutier@uninorte.edu.co

Capítulo 1

Preliminares

1.1 Introducción

El Álgebra, hablando en términos rudimentarios pero modernos, es la disciplina matemática dedicada al estudio de las denominadas *estructuras algebraicas*. Una estructura así está formada básicamente por un conjunto no vacío y una o más *operaciones* definidas sobre ese conjunto. El *Álgebra Lineal*, también en términos generales, tiene como objeto de estudio principal cierto tipo de estructura conocida como *espacio lineal* o *espacio vectorial*. En esta primera sección presentamos las definiciones de operación (especialmente las denominadas binarias) y de las estructuras algebraicas básicas: semigrupos, monoides, grupos, anillos y campos. En el capítulo dos, en particular, se hace una primera presentación de la estructura de espacio vectorial en un ejemplo específico. Tal definición se hará desde la perspectiva matemática o algebraica y en un capítulo posterior se relacionará con la noción física o geométrica de vector con la cual seguramente los lectores, aún los principiantes, tendrán alguna familiaridad. Iniciamos justamente con el concepto de *estructura algebraica*.

1.2 El concepto de estructura algebraica

Existe cierta familiaridad con la noción de operación, específicamente con la de operación binaria. Así, por ejemplo, la *adición*, la *multiplicación* y sus operaciones "inversas" (sustracción y división) en conjuntos numéricos constituyen ejemplos de operaciones binarias. Para ir abriendo paso a una

generalización[1] de tales operaciones "familiares", consideremos inicialmente la adición de números enteros.

En la adición de enteros, partimos tomando dos números enteros, por ejemplo 3 y 4, y al hacer la operación obtenemos el entero $7 = 3 + 4$, denominado la suma de 3 y 4. Más generalmente, si tomamos dos enteros, notados x e y, la adición produce un entero $z = x + y$. Técnicamente hablando, hemos tomado un par (x, y) de enteros y le hemos asignado un entero $x + y$, la suma de las componentes del par (x, y). En el lenguaje de la teoría de conjuntos lo que se tiene es una función

$$\begin{array}{rccc} + : & \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & (x, y) & \longmapsto & x + y \end{array}$$

cuyo dominio es el producto cartesiano del conjunto de los enteros, $\mathbb{Z}$, consigo mismo y las imágenes –o resultados de la acción de la función– pertenecen al mismo conjunto $\mathbb{Z}$. Un análisis similar puede hacerse para la multiplicación de enteros, la cual es una función

$$\begin{array}{rccc} \cdot : & \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & (x, y) & \longmapsto & xy. \end{array}$$

Estos son dos ejemplos particulares de lo que denominaremos una *ley de composición interna* definida sobre un conjunto. El hecho de que los elementos operados (sumados o multiplicados) se consideren formando pares ordenados parecería no ser importante en estos ejemplos ya que el resultado obtenido –la suma o el producto, respectivamente– es el mismo independientemente de si el par considerado es (x, y) o (y, x). Esto es debido, en este caso, a que las dos operaciones consideradas gozan de la denominada *propiedad conmutativa* según la cual "el orden de los sumandos (o factores) no altera la suma (el producto)". Sin embargo, basta con pensar en la *sustracción* de enteros para convencerse de que si queremos generalizar nuestras particulares observaciones a conjuntos (y operaciones) arbitrarios el "orden" de las componentes es importante. Así, la sustracción en el conjunto de los enteros es una función

$$\begin{array}{rccc} - : & \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & (x, y) & \longmapsto & x - y. \end{array}$$

Como tal, es una ley de composición interna pero, por ejemplo, la imagen de la pareja $(2, 3)$, esto es $2 - 3 = -1$, no es la misma que la de $(3, 2)$, la cual

[1]Para un desarrollo detallado de estos conceptos véanse [3], capítulo uno, del cual se ha tomado buena parte de esta exposición.

es $3 - 2 = 1$. Esto, por supuesto, significará que la sustracción no es una operación conmutativa.
Algunas preguntas son pertinentes en este momento. ¿Podemos operar solo elementos del mismo conjunto? o ¿estarán siempre los "resultados" de las operaciones en el mismo conjunto al cual pertenecen los elementos operados? Si pensamos, por ejemplo, en la división de enteros, es claro que solo podemos dividir un entero cualquiera entre un entero diferente de cero y que los resultados no necesariamente son enteros. Así, la división a la que estamos haciendo referencia es entonces una función

$$\begin{array}{rccc} \div : & \mathbb{Z} \times (\mathbb{Z} - \{0\}) & \longrightarrow & \mathbb{Q} \\ & (x, y) & \longmapsto & x \div y \end{array}$$

Aquí el dominio de nuestra función es el producto cartesiano de dos conjuntos distintos y las imágenes (cocientes) pertenecen al conjunto de los números *racionales* $\mathbb{Q}$, del cual los conjuntos cuyo producto cartesiano es el dominio son subconjuntos propios.
Generalizando lo anterior, dados conjuntos no vacíos A, B y C, una función

$$\begin{array}{rccc} * : & A \times B & \longrightarrow & C \\ & (x, y) & \longmapsto & x * y \end{array}$$

es denominada una *operación binaria*. Note que la imagen del par (x, y) bajo la función $*$ se denota por $x * y$. Si $A = B = C$ decimos que $*$ es una *ley de composición interna* en el conjunto A o, simplemente, una operación binaria definida sobre A. Como dijimos antes, una *estructura algebraica* es un conjunto con una o más operaciones binarias definidas sobre tal conjunto. La notación para una estructura algebraica generalmente involucra al conjunto (y, posiblemente, a otros con cuyos elementos se opera o al cual pertenecen los resultados) y a los símbolos de las operaciones. En particular, si A es un conjunto no vacío y $*$ es una ley de composición interna en A se acostumbra notar por $(A, *)$ a la estructura algebraica resultante. Se debe resaltar que dicha notación hace referencia no solo a los elementos del conjunto A sino, principalmente, al comportamiento de los mismos con relación a la operación $*$. Así, por ejemplo, cuando nos referimos a la estructura "aditiva" $(\mathbb{Z}, +)$, estamos hablando de una estructura distinta a la "multiplicativa" $(\mathbb{Z}, \cdot)$. En ambos casos los elementos del conjunto "soporte" de la estructura son los mismos, pero el comportamiento algebraico no es igual. Por ejemplo, mientras que la estructura aditiva goza de la propiedad de *existencia* de inversos para cada elemento de $\mathbb{Z}$, esta propiedad no es válida, en general, en la estructura multiplicativa, en la cual solo 1 y -1 tienen inversos (multiplicativos).

Propiedades, seguramente familiares para el lector, como la conmutatividad, la asociatividad, entre otras, de la adición y la multiplicación en los enteros, pueden ser definidas también para leyes de composición interna. Estas se presentan a continuación.

Definición 1.2.1 *Sean A y B conjuntos no vacíos con $B \subseteq A$. Si $*$ y $\diamond$ son leyes de composición interna definidas en A. Entonces:*

1. *B es* **cerrado** *bajo $*$ si y solo si para todo $x, y \in B$ se cumple que $x * y \in B$.*
   Trivialmente, el conjunto A es, por ser $*$ una ley de composición interna en A, cerrado para $*$.

2. *$*$ es:*

   (a) **Conmutativa** *si y solo si para todo $x, y \in A$ se satisface:*

   $$x * y = y * x \tag{1.1}$$

   (b) **Asociativa** *si y solo si para todo $x, y, z \in A$ se cumple:*

   $$(x * y) * z = x * (y * z) \tag{1.2}$$

   (c) **Modulativa** *si y solo si existe $e \in A$ tal que para todo $x \in A$ se tiene:*

   $$x * e = e * x = x \tag{1.3}$$

   El elemento e, el cual puede probarse que es único, se denomina **elemento neutro** *para $*$ en A. En ese sentido, la propiedad modulativa también se denomina de* existencia de elemento neutro.

   (d) **Invertiva** *si y solo si es modulativa, con neutro e, y para todo elemento $x \in A$ existe un elemento $y \in A$ tal que:*

   $$x * y = y * x = e \tag{1.4}$$

   Para una operación invertiva y asociativa, para cada $x \in A$ el elemento y de la ecuación (1.4) es único (ejercicio). Tal elemento es denominado el **inverso***, bajo $*$, de x. En una estructura $(A, *)$ asociativa y modulativa puede suceder que la condición de existencia de inverso no se cumpla para todos los elementos de A; si se cumple para algún elemento particular x, diremos que x es* **invertible** *(o* **regular** *o* **no singular***) bajo $*$ y, consecuentemente, que y es el inverso de x.*

(e) **Distributiva con relación a** $\diamond$ *si y solo si para todo* $x, y, z \in A$ *se tienen:*

$$(x \diamond y) * z = (x * z) \diamond (y * z) \tag{1.5}$$
$$x * (y \diamond z) = (x * y) \diamond (x * z) \tag{1.6}$$

La propiedad dada por (1.5) se denomina usualmente **distributiva (de $*$ con relación a $\diamond$) por la derecha**, *mientras que la dada por (1.6) lo será por la* **izquierda**.

Algunas de las definiciones dadas pueden extenderse a operaciones binarias que no sean necesariamente leyes de composición interna. Por ejemplo, para una operación binaria $*$: $A \times B \longrightarrow B$, decimos que es *modulativa a izquierda* si y solo si existe $e \in A$ tal que para todo $x \in B$ se tiene $e * x = x$. En este caso e es denominado un *neutro a izquierda*. De manera similar se puede definir elemento neutro a derecha para operaciones del tipo $* : A \times B \longrightarrow A$. Nótese así que para leyes de composición interna el neutro, si existe, lo es tanto a izquierda como a derecha. También es costumbre, para una operación $* : A \times B \longrightarrow B$, decir que un conjunto no vacío $D \subseteq B$ es *cerrado* para $*$ si y solo si, siempre que se tengan $x \in A, y \in D$, se tiene también que $(x * y) \in D$. Se dejan al lector otras posibles extensiones de las definiciones dadas. Diremos también que una estructura $(A, *)$ es asociativa (o conmutativa, modulativa, etc.) si lo es la operación $*$.
Si $*$ es una ley de composición interna en el conjunto A y B es un subconjunto de A, cerrado bajo $*$, entonces la restricción de $*$ a B, usualmente notada $*|_B$,

$$\begin{array}{rccc} *|_B : & B \times B & \longrightarrow & B \\ & (x, y) & \longmapsto & x * y, \end{array}$$

es también una ley de composición interna en B. Algunas de las propiedades ya definidas (conmutativa, asociativa, distributivas) claramente son válidas también para la restricción de $*$ a B, en caso de que se cumplan en A, diremos en tal caso que son *hereditarias*.[2] Las propiedades (1.3) y (1.4), por su parte, se satisfacen –si se cumplen en A– para todo $x \in B$, pero no se garantiza la pertenencia del neutro e, o el inverso de x al conjunto B.

[2]De hecho son válidas sobre cualquier subconjunto no vacío de A, aún no siendo cerrado.

Ejemplo 1.2.1

1. La conocida estructura aditiva de los enteros $(\mathbb{Z}, +)$ es, como recordará el lector, asociativa, conmutativa, modulativa e invertiva. Una estructura tal, como se definirá después, es denominada un *grupo abeliano*. Aquí el elemento neutro (aditivo) es cero, 0, y cada entero x tiene un inverso aditivo $-x$. Por su parte la estructura multiplicativa $(\mathbb{Z}, \cdot)$ es asociativa, conmutativa y modulativa, pero no es invertiva. Solamente, como ya se mencionó, son invertibles el 1 y el -1 y, en cada caso, el inverso es el mismo elemento. Para enteros distintos de cero y de 1 y -1, por ejemplo 2, el inverso multiplicativo existe si se consideran como parte del conjunto de los racionales, es decir de la estructura $(\mathbb{Q}, \cdot)$, pero no es un entero. En el ejemplo considerado, el inverso de 2 es $0.5 = \frac{1}{2}$. Este ejemplo resalta la importancia de que una estructura depende tanto del conjunto como de la o las operaciones consideradas.
   Grupos abelianos, como el caso de $(\mathbb{Z}, +)$, son también $(\mathbb{Q}, +), (\mathbb{R}, +)$, $(\mathbb{Q} - \{0\}, \cdot)$ y $(\mathbb{R} - \{0\}, \cdot)$.

2. Consideremos el conjunto $A = \{a, b, c\}$. Una ley de composición interna sobre A debe asignar a cada par $(x, y) \in A \times A$, es decir, a cada par de elementos de A, un elemento único del mismo conjunto. Se puede elegir arbitariamente tales "resultados" de la operación. En este caso, la operación puede definirse mediante una tabla; por ejemplo, las que se muestran a continuación.

$*$	a	b	c
a	a	b	c
b	c	a	b
c	b	a	c

$\diamond$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

   En la primera fila y la primera columna de cualquiera de las tablas se muestran el símbolo de la operación y los elementos del conjunto A. El resultado de operar un elemento de una columna con uno de una fila es el elemento en la intersección de dichas fila y columna. Así, por ejemplo:

$$\begin{aligned} a * b &= b \\ b \diamond c &= a \\ b * b &= a \\ b \diamond b &= c \end{aligned}$$

Nótese que en $(A, *)$, a es un neutro a izquierda pero no a derecha $(b * a = c)$, mientras que en $(A, \diamond)$ es neutro tanto a derecha como a izquierda; es decir, $\diamond$ es modulativa. Puesto que $a * b = b \neq c$ se sigue que $*$ no es conmutativa. ¿Es asociativa? Puede verificarse que $\diamond$ es asociativa, modulativa, invertiva y conmutativa; es decir, $(A, \diamond)$ es un grupo abeliano. Nótese que el inverso de b, bajo $\diamond$, es c y el de c es b. a, por su parte, es su propio inverso bajo $\diamond$.

3. Para un entero $n \geq 2$ sea $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, el conjunto de los enteros no negativos menores que n. Por ejemplo:

$$\begin{aligned} \mathbb{Z}_2 &= \{0, 1\} \\ \mathbb{Z}_3 &= \{0, 1, 2\} \\ \mathbb{Z}_6 &= \{0, 1, 2, 3, 4, 5\} \end{aligned}$$

Así, $\mathbb{Z}_n$ es, en principio, un subconjunto del conjunto de los enteros. Es claro, sin embargo, que no es *cerrado* bajo la adición "usual" de enteros. Así, por ejemplo $1 + (n-1) = n$, pero $n \notin \mathbb{Z}_n$. Para la multiplicación, si $n > 2$, tampoco el conjunto considerado es cerrado. Sin embargo, es un hecho conocido que el cociente de un entero no negativo entre $n \geq 2$ tiene residuo menor que n. Así, podemos definir unas "nuevas" adición y multiplicación en $\mathbb{Z}_n$, tomando como resultados los residuos de la división entre n de la adición y multiplicación "usuales" de los elementos considerados, garantizando así la *cerradura* del conjunto bajo tales operaciones (adición y multiplicación *módulo* n).
Por ejemplo, si consideramos $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, entonces como "suma" de 3 y 4 tomamos el residuo de dividir 7 (la suma usual) entre 6. Así, en este caso, tenemos $3 + 4 = 1$. Por su parte, $3(4) = 0$ dado que el residuo de dividir 12 (producto usual de 3 por 4) entre 6 es 0. Las tablas de estas adición y multiplicación (*módulo* 6) se muestran abajo.

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Nótese que ambas operaciones son conmutativas y que 0 y 1 siguen siendo los neutros aditivo y multiplicativo, respectivamente, en $\mathbb{Z}_6$ (y, en general,

en $\mathbb{Z}_n$) y que cada elemento tiene un inverso aditivo. Específicamente, el inverso aditivo de un elemento $x \in \mathbb{Z}_n - \{0\}$ es $n - x$, dado que $(n - x) + x = x + (n - x) = 0$. Si siguiendo la notación familiar en los enteros, se denota por $-x$ al *inverso aditivo* de x, tenemos entonces[3]:

$$\begin{aligned} -0 = 0, \quad -1 = 5, \quad -2 = 4 \\ -3 = 3, \quad -4 = 2, \quad -5 = 1 \end{aligned}$$

Tal como en el caso de los enteros, y siguiendo la notación anterior, los únicos elementos invertibles (multiplicativamente) en $\mathbb{Z}_6$ son 1 y $-1 = 5$ y si, nuevamente tomando "prestada" la notación multiplicativa para inversos en los números reales, para un elemento invertible x, notamos por x^{-1} su inverso en $\mathbb{Z}_6$, tenemos:

$$\begin{aligned} 1^{-1} &= 1 \\ 5^{-1} &= 5 \end{aligned}$$

Es decir, al igual que en $\mathbb{Z}$, cada uno es su propio inverso. Puede mostrarse fácilmente que para cualquier valor de $n \geq 2$, en $(\mathbb{Z}_n, \cdot)$ efectivamente 1 y $n - 1$ (el inverso aditivo de 1) son invertibles y cada uno es su propio inverso. Para $n = 6$, como muestra la tabla, son los únicos elementos invertibles, pero podrían, para otros valores de n, existir otros elementos invertibles. Como ejemplo considere en $(\mathbb{Z}_9, \cdot)$ los elementos $1, 2, 4, 5, 7$ y 8. Como se esperaba, por lo dicho antes, 1 y 8 son invertibles y cada uno es su propio inverso. Sin embargo, los otros elementos considerados también son invertibles. En efecto se tiene:

$$\begin{aligned} 2(5) &= 1 \\ 4(7) &= 1 \end{aligned}$$

Por lo que $2^{-1} = 5, 5^{-1} = 2, 4^{-1} = 7, 7^{-1} = 4$. Al lector puede parecerle sorprendente que bajo la multiplicación módulo n (en este caso $n = 9$), enteros no invertibles bajo la multiplicación usual lo sean en la estructura modular.

[3]Aquí el signo menos no se refiere a *negativo* en el sentido de un entero "menor" que 0, sino que se utiliza como un símbolo para denotar el inverso, bajo +, del elemento al cual precede. Es decir, denota al elemento que sumado con el elemento dado da como resultado el neutro aditivo (0).

Dado un conjunto no vacío G, y una ley de composición interna $*$ en G, la estructura $(G, *)$ es denominada un **grupoide**. Si la operación es asociativa se denominará un **semigrupo**. Un semigrupo tal que la operación sea además modulativa se denomina un **monoide**. Un monoide con la propiedad invertiva es un **grupo**. Si, además, la operación es conmutativa la estructura se denomina **grupo conmutativo** o **grupo abeliano**. En general, para grupoides, usaremos notación multiplicativa escribiendo xy en lugar de $x * y$, así como 1_G para referirnos al neutro de $*$, en caso de existir, y también x^{-1} para referirnos al inverso de x en caso de existir. Por supuesto, en estructuras particulares aditivas escribiremos 0_G y $-x$, respectivamente, para el neutro y el inverso de $x \in G$. Así, tenemos

$$y = x^{-1} \iff xy = yx = 1_G \tag{1.7}$$

$$y = -x \iff x + y = y + x = 0_G \tag{1.8}$$

1.3 La estructura de campo

Como se advirtió antes, la estructura principal a considerar en el curso de Álgebra Lineal es la de *espacio lineal* o *espacio vectorial*. Tales estructuras son construidas sobre una estructura aditivo multiplicativa básica conocida como *campo* o *cuerpo*. Comenzamos con un conjunto no vacío, $\mathbb{K}$ con dos leyes de composición interna $+ : \mathbb{K} \times \mathbb{K} \longrightarrow \mathbb{K}$ y $\cdot : \mathbb{K} \times \mathbb{K} \longrightarrow \mathbb{K}$ (adición y multiplicación). La estructura $(\mathbb{K}, +, \cdot)$ es un *campo* o *cuerpo* si y solo si

- $(\mathbb{K}, +)$ es un grupo abeliano (con neutro $0_{\mathbb{K}}$)
- La multiplicación es conmutativa, asociativa, modulativa, con neutro $1_{\mathbb{K}} \neq 0_{\mathbb{K}}$, y distributiva respecto de la adición.
- Cada elemento $x \in \mathbb{K}$, $x \neq 0_{\mathbb{K}}$, es invertible (multiplicativamente).

Se sigue así que si $(\mathbb{K}, +, \cdot)$ es un campo, entonces $(\mathbb{K}, +)$ y $(\mathbb{K} - \{0_{\mathbb{K}}\}, \cdot)$ son grupos abelianos. La denominación de **anillo** se refiere a una estructura aditiva multiplicativa $(R, +, \cdot)$ tal que $(R, +)$ es un grupo abeliano y la multiplicación es asociativa y distributiva con relación a la adición. Las denominaciones de **anillo conmutativo** y **anillo con elemento identidad** se refieren, respectivamente, a un anillo tal que la multiplicación es conmutativa y a un anillo con elemento neutro para la multiplicación.

Tenemos entonces que todo campo es una anillo conmutativo con identidad en el cual todo elemento no nulo es invertible multiplicativamente. También se acostumbra decir que es un **anillo conmutativo con división**. La estructura $(\mathbb{Z}, +, \cdot)$ (enteros con la adición y la multiplicación) es un anillo conmutativo con elemento identidad, pero claramente no es un campo (¿por qué?). De igual manera, para un natural $n \geq 2$, la estructura $(\mathbb{Z}_n, +, \cdot)$ es un anillo conmutativo con identidad y es un campo si y solo si n es un número primo.

En particular, nos interesa la estructura de campo del conjunto de los números reales. Suponemos por parte del lector un conocimiento, así sea intuitivo, de tal conjunto. Tal conjunto, notado por $\mathbb{R}$, es la unión del conjunto de los *números racionales*, notado $\mathbb{Q}$, con el de los *irracionales*. El primero es el conjunto de los números que pueden expresarse como cociente de dos enteros. Una característica notable de los racionales es también que su expresión decimal es periódica, a diferencia de los irracionales en los cuales la expresión decimal es infinita y no periódica. Ejemplos notables de irracionales son las raíces cuadradas de números naturales que no son cuadrados perfectos ($\sqrt{2}$, $\sqrt{3}$, etc.), el número π (constante universal que representa el cociente de la longitud de una circunferencia cualquiera sobre su diámetro), el número de *Euler*, e, base de los logaritmos naturales. Asumimos como verdadero que la estructura $(\mathbb{R}, +, \cdot)$ es un campo, lo cual de acuerdo con la definición dada antes significa:

- $(\mathbb{R}, +)$ es un grupo abeliano. El neutro aditivo por supuesto es 0 y cada real x tiene un inverso aditivo, notado $-x$.
- La multiplicación es conmutativa, asociativa y distributiva con relación a la suma. Igualmente es modulativa, con neutro $1 \neq 0$.
- Cada real $x \neq 0$ tiene un inverso multiplicativo, notado x^{-1}.

Las propiedades de campo, conjuntamente con las de la igualdad, permiten fácilmente resolver ecuaciones de grado uno en una o más incógnitas. En particular, si $\mathbb{K}$ es un campo, y $a, b, c \in \mathbb{K}$ con $a \neq 0$ la ecuación

$$ax + c = b$$

tiene solución única y puede resolverse fácilmente como en el álgebra elemental. Así, tenemos

$$\begin{aligned} ax + c = b &\iff ax = b + (-c) = b - c \\ &\iff x = a^{-1}(b - c) \end{aligned}$$

En estructuras aditivo multiplicativas más generales, por ejemplo, anillos conmutativos, el problema no es tan simple. Considere por ejemplo la ecuación $2x + 7 = 5$.

1. En $(\mathbb{Z}_{11}, +, \cdot)$ que es un campo, se tiene

$$x = 2^{-1}(5 + (-7)) = 6(-2) = 6(9) = 10.$$

2. En $(\mathbb{Z}_8, +, \cdot)$ que no es un campo, se tiene en cambio $2x = 5-7 = -2 = 6$. Notemos, sin embargo, que no podemos "despejar" x, ya que 2 no es invertible en $\mathbb{Z}_8$. Si bien es claro que 3 es una solución de la ecuación, no podemos afirmar que es la única. Revisando la tabla multiplicativa de $\mathbb{Z}_8$ para el 2 tenemos (método de la "fuerza bruta")

$$\begin{aligned} 2(0) &= 0 \\ 2(1) &= 2 \\ 2(2) &= 4 \\ 2(3) &= \boxed{6} \\ 2(4) &= 0 \\ 2(5) &= 2 \\ 2(6) &= 4 \\ 2(7) &= \boxed{6} \end{aligned}$$

   lo que muestra que la ecuación tiene exactamente dos soluciones: 3 y 7. Por otra parte, la ecuación $2x = 7$ en $\mathbb{Z}_8$ no tiene solución[4] (¿por qué?).

En el capítulo siguiente se resuelve el problema de resolver una *ecuación lineal* sobre el campo real. Los resultados teóricos que se presentan pueden extenderse sin problemas a ecuaciones sobre un campo cualquiera. Una ecuación lineal en las n incógnitas (o variables) $x_1, x_2, \ldots, x_n$ sobre un campo $\mathbb{K}$ es una ecuación de la forma

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b \tag{1.9}$$

donde $a_1, a_2, \ldots, a_n, b \in \mathbb{K}$. Así, por ejemplo, $2x+3y = 6$ es una ecuación lineal en las incógnitas x, y sobre el campo real. Como se verá en el capítulo siguiente,

[4]Una ecuación $ax = b$ en $\mathbb{Z}_n$ tiene solución si y solo si el máximo común divisor, digamos d, de a y n divide a b. En tal caso el número de soluciones es exactamente d. Para una demostración véase [4], teorema 2.3.2, página 41.

cada solución de la ecuación es un par de reales que "satisface" la ecuación. Usualmente ordenaremos las variables y cada solución se tomará como un *par ordenado*. En nuestro ejemplo, una solución es el par $(3, 0)$ $(x = 3, y = 0)$ ya que

$$2(3) + 3(0) = 6.$$

No es difícil entender que tal ecuación tiene infinitas soluciones y que una solución se puede obtener asignándole valores arbitrarios a una de las incógnitas y reduciendo el problema a una ecuación en una sola variable. Así, por ejemplo, si t es un número real cualquiera y asignamos tal valor a x, entonces debe tenerse

$$2t + 3y = 6.$$

Resolviendo esta ecuación en y se tiene

$$y = \frac{6 - 2t}{3}.$$

Así, toda solución, como par ordenado de reales, es de la forma

$$\left(t, \frac{6 - 2t}{3}\right)$$

siendo t un real cualquiera. El conjunto solución (conjunto de todas las soluciones) es entonces

$$S = \left\{ \left(t, \frac{6 - 2t}{3}\right) \middle| \, t \in \mathbb{R} \right\}.$$

Si consideramos la ecuación $2x + 3y = 6$ ahora sobre el campo finito $\mathbb{Z}_7$ podemos también proceder como antes y se tendría que para $x = t$ con $t \in \mathbb{Z}_7$ se obtiene

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

De modo que todas las soluciones son de la forma $(t, 2 + 4t)$ y, así, la ecuación tiene siete soluciones: $(0, 2), (1, 6), (2, 3), (3, 0), (4, 4), (5, 1), (6, 5)$.