SOFTWARE PARA LA CONSTRUCCIÓN DE OPERACIONES DISTRIBUTIVAS CON RESPECTO A OTRAS DADAS

José Leonardo Angel Bautista
Profesor Universidad Pedagógica Nacional
Bogotá D.C, Colombia
jangel@uni.pedagogica.edu.co

Oscar Javier Molina Jaime
Profesor Universidad Pedagógica Nacional
Bogotá D.C, Colombia
omolina@uni.pedagogica.edu.co

Carlos Julio Luque Arias
Profesor Universidad Pedagógica Nacional
Bogotá D.C, Colombia
caluque@uni.pedagogica.edu.co

Introducción

Este escrito presenta información algebraica para construir o definir operaciones distributivas en algunas estructuras finitas, para luego definir operaciones en tales estructuras, análogas a la potenciación y logaritmación en el conjunto de los números reales.

Particularmente, al estudiar los métodos algebraicos de construcción, se desarrolla una serie de aplicaciones (sólo para conjuntos finitos) donde sus algoritmos se basan, primero, en la información algebraica de las proposiciones producto de dichos métodos, y segundo, en ciclos anidados cuyo objetivo es el de comparar datos según tal información algebraica; a su vez, las aplicaciones permiten evitar cálculos repetitivos y tediosos, frecuentes en estructuras finitas, y se dirigen a obtener resultados acerca de la construcción de operaciones distributivas en esas estructuras. Todas estas aplicaciones conllevan a diseñar en lenguaje Visual Basic.Net a *APLICOP*, el software[1] es una herramienta para lograr nuestros objetivos, en donde el usuario, tiene la posibilidad de interactuar con las aplicaciones, realizando las actividades que él crea convenientes para avanzar en el estudio de

[1]El software libre *APLICOP*, hace parte del trabajo de grado "SOFTWARE PARA LA CONSTRUCCIÓN DE OPERACIONES ANÁLOGAS A LA POTENCIACIÓN, EN ALGUNAS ESTRUCTURAS FINITAS", elaborado por Leonardo Angel y Oscar Molina,bajo la dirección de Carlos Luque y disponible en el Departamento de Matemáticas de la Universidad Pedagógica Nacional.

la temática propuesta, sin que éstas sean explícitas en la misma.

Los métodos algebraicos a los que se hace referencia, se basan en que en los grupos abelianos se pueden construir operaciones distributivas con respecto a ellos, usando primero, procedimientos recursivos o estudiando el monoide de sus endomorfismos; se extienden estos procedimientos, para definir operaciones distributivas con respecto a la multiplicación, que son análogas a la operación de potenciación entre números reales.

Otro procedimiento que se explora para construir operaciones análogas a la potenciación, es el de definir homomorfismos entre grupos abelianos y operaciones distributivas con respecto a ellos, construidas con el método anterior.

Por último, se estudia la teoría de índices presentada en la teoría de congruencias, para construir la operación de indización, que es análoga a la operación de logaritmación entre números reales.

Este trabajo está dirigido a usuarios interesados en construir y/o definir operaciones distributivas, que a su vez permitan definir operaciones en estructuras finitas, análogas a la potenciación y logaritmación en $\mathbb{R}$. Para ello, este usuario debe contar con conocimientos básicos acerca de teoría de grupos, anillos, teoría de números y de estructuras como los sistemas numéricos.

1. Operaciones Distributivas

Al estudiar las características que se deducen lógicamente de las operaciones que conforman las estructuras donde se presentan, surge la posibilidad de demostrar la distributividad de una de ellas con respecto a la otra, y luego, inferir un método que permita construir nuevas estructuras en la cuales se presenta la propiedad distributiva.

Observemos la definición de distributividad:

Definición. Dada una estructura algebraica $(X, *, \circ)$, se dice que $\circ$ es distributiva a derecha en X respecto a $*$ si para todo $x, y, z \in X$, se cumple que

$$x \circ (y * z) = (x \circ y) * (x \circ z)$$

y se dice que $\circ$ es distributiva a izquierda en X respecto a $*$ si para todo $x, y, z \in X$

se cumple que

$$(y * z) \circ x = (y \circ x) * (z \circ x)$$

Si $\circ$ es tanto distributiva a izquierda como a derecha en X respecto a $*$, entonces se dice que $\circ$ es distributiva en X respecto a $*$.

La definición de distributividad junto con los enunciados de las propiedades conmutativa, asociativa, modulativa e invertiva, dieron pie para diseñar la aplicación *Algebra* del software *APLICOP*, la cual permite verificar si dos operaciones definidas por el usuario, cumplen con estas propiedades y si una de ellas distribuye con respecto a la otra.

Las operaciones distributivas se presentan en distintas estructuras algebraicas, como por ejemplo, en algunas estructuras pertenecientes a los sistemas numéricos, los retículos y las matrices, de las cuales se infieren características relevantes respecto a tal propiedad.

Particularmente, se destacan ciertas características de forma en cuanto a la definición, tanto de la suma como de la multiplicación en los diferentes conjuntos numéricos, las cuales permiten deducir un método para la construcción de una estructura donde existe la relación de distributividad entre dos operaciones. Este método se presenta en la siguiente proposición y de alguna manera justifica el hecho de que la relación de distributividad en una estructura, se *hereda* de otra con la cual se construye dicha estructura:

Proposición 1. *Dada una estructura algebraica* $(X, +, \times)$ *con las siguientes características:*

1. $+$ *es asociativa y conmutativa*
2. $\times$ *es asociativa y conmutativa*
3. $\times$ *es distributiva respecto a* $+$

Si se construye la estructura $(Y, \oplus, \otimes)$ *a partir de la estructura* $(X, +, \times)$*, de tal manera que*

$$Y = \{(a, b) \mid a, b \in X\}$$

y las operaciones de suma $(\oplus)$ *y de multiplicación* $(\otimes)$ *se definen por medio de:*

1. $x \oplus y = (a + c, b + d)$, *y,* $x \otimes y = (a \times c + b \times d, a \times d + b \times c)$ *ó*

2. $x \oplus y = (a \times d + b \times c, b \times d)$, y, $x \otimes y = (a \times c, b \times d)$ *ó*

3. $x \oplus y = (a + c, b + d)$, y, $x \otimes y = (a \times c, a \times d + b \times c)$ *ó*

4. *Si* $(X, +, \times)$ *es un anillo conmutativo, entonces y* $x \oplus y = (a + c, b + d)$, y, $x \otimes y = (a \times c - b \times d, a \times d + b \times c)$

donde $x = (a, b), y = (c, d)$, $x, y \in Y$, *entonces* $\otimes$ *es distributiva respecto a* $\oplus$ *en* Y.

La anterior proposición nos permite generar nuevas estructuras algebraicas a partir de cambiar la estructura algebraica $(X, +, \times)$ por otra con las condiciones ya expuestas, de tal manera que en la nueva estructura $(Y, \oplus, \otimes)$ se continúe teniendo la distributividad de $\otimes$ respecto a $\oplus$ bajo la misma definición que de $\oplus$ y de $\otimes$ se tenía, o bien bajo una de las maneras expuestas en tal proposición.

Ejemplo. Si retomamos las definiciones tanto de $\oplus$ como de $\otimes$ dadas por el numeral 1 de la anterior proposición, en donde a partir de la estructura $(\mathbb{R}, +, \times)$ se pretende construir la nueva estructura $(Y, \oplus, \otimes)$, tenemos que:
$Y = \{x = (a, b) \mid a, b \in \mathbb{R}\}$, y si , $x = (a, b), y = (c, d), x, y \in \mathbb{R}$, entonces:

$$x \oplus y = (a + c, b + d), \quad y,$$

$$x \otimes y = (a \times c + b \times b, a \times d + b \times c)$$

donde $\otimes$ es distributiva respecto a $\oplus$ en Y.
A esta nueva estructura se le conoce como el anillo conmutativo de los números dobles o de Clifford.

Analizando la **proposición 1**, vemos que en 3 de los 4 casos de definiciones que se dieron para $\oplus$ y $\otimes$, aparece la misma definición para $\oplus$, es decir:

$$x \oplus y = (a + c, b + d)$$

donde $x = (a, b), y = (c, d)$, y que las definiciones para $\otimes$ son distintas, pero todas conservan las siguientes características:

1. Las definiciones dependen únicamente de los elementos a, b, c, d, y de las operaciones $+$ y $\times$ definidas en X bajo las condiciones expuestas.

2. En cada definición están presentes los cuatro elementos a, b, c, d.

3. No se forman productos entre elementos correspondientes a un mismo par ordenado.

Al parecer, para encontrar todas las multiplicaciones ($\otimes$) que sean distributivas respecto a $\oplus$, tendríamos que definir todas las posibles multiplicaciones que sigan las características expuestas. Si fijamos la definición dada para la adición

$$x \oplus y = (a + c, b + d)$$

algunas de las multiplicaciones $\otimes$, definidas bajo las condiciones expuestas son:

1. $x \otimes y = (a \times c + b \times d, a \times d)$
2. $x \otimes y = (a \times c + b \times d, b \times c)$
3. $x \otimes y = (b \times d, a \times d + b \times c)$
4. $x \otimes y = (b \times d, a \times c)$
5. $x \otimes y = (b \times d, a \times c + b \times d)$

El lector puede demostrar que en cada caso, $\otimes$ es distributiva respecto a $\oplus$ en Y, teniendo en cuenta las condiciones bajo las cuales se toma la estructura $(X, +, \times)$. Ahora nos centraremos en que una operación es una función y que la distributividad es un caso particular de **homomorfismos**, para presentar métodos de construcción de operaciones distributivas tanto internas como externas, en algunas estructuras finitas. Veamos la definición de homomorfismo:

Definición. Dadas dos estructuras algebraicas $(A, *)$ y $(B, \circ)$. Una función f de A en B es un homomorfismo de A en B si se cumple:

$$f(a * b) = f(a) \circ f(b)$$

para todo par de elementos $a, b \in A$.

Cuando f es un homomorfismo de A en si mismo, se denomina **endomorfismo** de A; al conjunto de todos los endomorfismos de A se denota por $E(A)$.

La definición de homomorfismos y endomorfismos, nos dio pie para realizar las aplicaciones *Endomorfismos* y *Homomorfismos* del software *APLICOP*; la primera, permite encontrar todos los endomorfismos de un conjunto X, a partir de una operación definida por el usuario, la segunda, permite encontrar todos los homomorfismos de la estructura $(X, +)$ en la estructura $(Y, *)$, a partir de las operaciones $+$ y $*$ definidas por el usuario.

1.1. La distributividad un caso particular de homomorfismos

Con base en la definición de operaciones distributivas internas a derecha e izquierda, mostraremos el hecho de que la distributividad es un caso particular de homomorfismos, y a partir de tal, propondremos métodos para construir operaciones distributivas a derecha y a izquierda respecto a una dada. En seguida definiremos operaciones externas, para luego definir y construir operaciones distributivas externas con base en el concepto de homomorfismo.

Sea $(A, *, \circ)$ una estructura algebraica con dos operaciones $*$ y $\circ$, cada operación $\circ$ define una función

$$\begin{array}{rcl} F : A & \longrightarrow & A^A \\ a & \longmapsto & f_a : \begin{array}{rcl} A & \longrightarrow & A \\ b & \longmapsto & f_a(b) = a \circ b \end{array} \end{array}$$

Donde $A^A = \{f : A \to A \mid f \text{es función}\}$.

Si $\circ$ es distributiva a derecha con respecto a $*$, es decir

$$a \circ (b * c) = (a \circ b) * (a \circ c)$$

entonces de la definición de f_a se tiene que

$$f_a(b * c) = f_a(b) * f_a(c)$$

lo que quiere decir que f_a es un endomorfismo de A.

Así, la distributividad a derecha se puede expresar en términos de homomorfismos. Usaremos este hecho para construir operaciones distributivas.

Proposición 2 (Construcción de operaciones distributivas a derecha). *Sea $(X, *)$ una estructura algebraica; cada función*

$$\begin{array}{rcl} F : X & \longrightarrow & E(X) \\ x & \longmapsto & f_x : X \longrightarrow X \end{array}$$

define una operación $\circ$ distributiva a derecha respecto a $*$, a saber

$$x \circ y = f_x(y)$$

Demostración. Para todo elemento $x, y, z \in X$, se tiene que

$$\begin{aligned} x \circ (y * z) &= f_x(y * z) && \text{Por definición de } \circ \text{ en } X \\ &= f_x(y) * f_x(z) && \text{Por ser } f_x \text{ endomorfismo de } X \\ &= (x \circ y) * (x \circ z) && \text{Por definición de } \circ \text{ en } X \end{aligned}$$

Por tanto $x \circ (y * z) = (x \circ y) * (x \circ z)$. □

La anterior proposición nos permitió realizar la aplicación *Distributivas a derecha* del software *APLICOP*, la cual permite encontrar todas las operaciones internas distributivas a derecha respecto a una operación definida por el usuario.

Notación. De ahora en adelante, un conjunto A con n elementos se representará con:

$$A = \{0, 1, 2, 3, 4, \ldots, (n-1)\}$$

Cada una de las n^n funciones de A en A se representarán con un número de n cifras en base n, donde la cifra k-ésima corresponde a la imagen del elemento $k \in A$ por la función. Por ejemplo, la función

$$\begin{aligned} f : A &\longrightarrow A \\ a &\longmapsto f(a) = 0 \end{aligned}$$

se representa con el número $0000\ldots0$ (n veces) y corresponde a la función número 0 la cual se notará por f_0; en general la k-ésima función se notará por f_k.

El siguiente ejemplo es una aplicación de la **proposición 2**.

Ejemplo. Sea $A = \{0, 1\}$ con la operación $*$ definida como sigue:

$*$	0	1
0	0	1
1	1	0

El conjunto $E(A)$ de los endomorfismos de A es:

$$E(A) = \{E_0, E_1\}$$

Donde

$$\begin{aligned} E_0 = f_0 : A &\longrightarrow A \\ a &\longmapsto f(a) = 0 \end{aligned}$$

$$\begin{aligned} E_1 = f_1 : A &\longrightarrow A \\ 0 &\longmapsto f(0) = 0 \\ 1 &\longmapsto f(1) = 1 \end{aligned}$$

Si se define la función F_0 como:

$$\begin{aligned} F_0 : A &\longrightarrow E(A) \\ a &\longmapsto F_0(a) = E_0 \end{aligned}$$

entonces la operación

$$\begin{aligned} \circ : A \times A &\longrightarrow A \\ (a, b) &\longmapsto a \circ b = E_0(b) \end{aligned}$$

es distributiva a derecha respecto a $*$, que corresponde a la operación

$\circ$	0	1
0	0	0
1	0	0

De igual manera:

- La función F_1 definida por

$$\begin{aligned} F_1 : A &\longrightarrow E(A) \\ 0 &\longmapsto F_1(0) = E_0 \\ 1 &\longmapsto F_1(1) = E_1 \end{aligned}$$

define la operación

$\circ$	0	1
0	0	0
1	0	1

distributiva a derecha respecto a $*$.

- La función F_2 definida por

$$\begin{aligned} F_2 : A &\longrightarrow E(A) \\ 0 &\longmapsto F_2(0) = E_1 \\ 1 &\longmapsto F_2(1) = E_0 \end{aligned}$$

define la operación

$\circ$	0	1
0	0	1
1	0	0

distributiva a derecha respecto a $*$.

- La función F_3 definida por

$$\begin{aligned} F_3 : A &\longrightarrow E(A) \\ a &\longmapsto F_3(a) = E_1 \end{aligned}$$

define la operación

$\circ$	0	1
0	0	1
1	0	1

distributiva a derecha respecto a $*$.

Para presentar el método de construcción de operaciones distributivas a izquierda (proposición 4), se tiene en cuenta el hecho de que la distributividad es un caso particular de homomorfismos. Además es necesario tener clara la siguiente notación y la proposición 3:

Notación. Denotamos por $(X^Y, *)$ a la estructura formada sobre el conjunto de X^Y de todas las funciones del conjunto Y en el conjunto X, y la operación

$$\begin{array}{rcl} \circ : X^Y \times X^Y & \longrightarrow & X^Y \\ (f,g) & \longmapsto & f*g : \begin{array}{rcl} Y & \longrightarrow & X \\ x & \longmapsto & (f*g)(x) = f(x)*f(y) \end{array} \end{array}$$

Proposición 3. *Sea $(X, *)$ una estructura algebraica; una función*

$$\begin{array}{rcl} G : X & \longrightarrow & X^X \\ x & \longmapsto & g_x : \begin{array}{rcl} X & \longrightarrow & X \\ y & \longmapsto & g_x(y) \end{array} \end{array}$$

tal que

$$g_{x*z}(y) = g_x(y) * g_z(y)$$

es un homomorfismo entre X y X^X.

Demostración. Para todo $x, y \in X$, se tiene que

$$\begin{array}{rll} G(x*y) = & g_{x*y} & \text{Por definición de } G \\ = & g_x * g_y & \\ = & G(x) * G(y) & \text{Por definición de } G \end{array}$$

Por tanto $G(x*y) = G(x)*G(y)$. □

Proposición 4 (Construcción de operaciones distributivas a izquierda). *La función G definida en la proposición 3, define una operación*

$$\begin{array}{rcl} \triangle : X \times X & \longrightarrow & X \\ (x,y) & \longmapsto & x \triangle y = g_x(y) \end{array}$$

distributiva a izquierda con respecto a $*$.

Demostración. Para todo elemento $x, y, z \in X$, se tiene que

$$\begin{array}{rll} (x*z) \triangle y = & g_{x*z}(y) & \text{Por definición de } \triangle \text{ en } X \\ = & g_x(y) * g_z(y) & \\ = & (x \triangle y) * (z \triangle y) & \text{Por definición de } \triangle \text{ en } X \end{array}$$

Por tanto $(x*z) \triangle y = (x \triangle y) * (z \triangle y)$. □

Este método nos permitió realizar la aplicación *Distributivas a izquierda* del software *APLICOP*, la cual permite encontrar todas las operaciones internas distributivas a izquierda respecto a una operación definida por el usuario.
Veamos un ejemplo en donde se utiliza la **proposición 4**:

Ejemplo. Sea $A = \{0, 1\}$ con la operación $*$ definida como sigue:

$*$	0	1
0	0	1
1	1	0

El conjunto A^A de las funciones de A en A es:

$$A^A = \{g_0, g_1, g_2, g_3\}$$

donde

$$\begin{aligned} g_0 : A &\longrightarrow A \\ a &\longmapsto g_0(a) = 0 \end{aligned}$$

$$\begin{aligned} g_1 : A &\longrightarrow A \\ 0 &\longmapsto g_1(0) = 0 \\ 1 &\longmapsto g_1(1) = 1 \end{aligned}$$

$$\begin{aligned} g_2 : A &\longrightarrow A \\ 0 &\longmapsto g_2(0) = 1 \\ 1 &\longmapsto g_2(1) = 0 \end{aligned}$$

$$\begin{aligned} g_3 : A &\longrightarrow A \\ a &\longmapsto g_3(a) = 1 \end{aligned}$$

Si se define la función G_0 como:

$$\begin{aligned} G_0 : A &\longrightarrow A^A \\ a &\longmapsto G_0(a) = g_0 \end{aligned}$$

entonces la operación

$$\begin{aligned} \circ : A \times A &\longrightarrow A \\ (a, b) &\longmapsto a \circ b = g_0(b) \end{aligned}$$

es distributiva a izquierda respecto $*$, que corresponde a la operación

$\circ$	0	1
0	0	0
1	1	0

De igual manera:

- La función G_1 definida por

$$\begin{aligned} G_1 : A &\longrightarrow A^A \\ 0 &\longmapsto G_1(0) = g_0 \\ 1 &\longmapsto G_1(1) = g_1 \end{aligned}$$

  define la operación

$\circ$	0	1
0	0	0
1	0	1

  distributiva a derecha respecto a $*$.

- La función G_2 definida por

$$\begin{aligned} G_2 : A &\longrightarrow A^A \\ 0 &\longmapsto G_2(0) = g_0 \\ 1 &\longmapsto G_2(1) = g_2 \end{aligned}$$

  define la operación

$\circ$	0	1
0	0	0
1	1	0

  distributiva a derecha respecto a $*$.

- La función G_3 definida por

$$\begin{aligned} G_3 : A &\longrightarrow A^A \\ 0 &\longmapsto G_3(0) = g_0 \\ 1 &\longmapsto G_3(1) = g_3 \end{aligned}$$

  define la operación

$\circ$	0	1
0	0	0
1	1	1

distributiva a derecha respecto a $*$.

A partir de los anteriores métodos para la construcción de operaciones distributivas a derecha e izquierda y de la proposición 5, presentaremos un método para construir operaciones distributivas respecto a una dada (Proposición 6):

Proposición 5. *Sea $(X, *)$ un semigrupo abeliano, entonces $E(X)$ es cerrada para la operación:*

$$\begin{array}{rcl} *' : E(A) \times E(A) & \longrightarrow & E(A) \\ (f, g) & \longmapsto & f *' g : \begin{array}{ccc} A & \longrightarrow & A \\ x & \longmapsto & (f *' g)(x) = f(x) * f(y) \end{array} \end{array}$$

Demostración. Sean f y g dos elementos de $E(X)$, luego

$$\begin{array}{rll} (f *' g)(x * y) = f(x * y) * g(x * y) & & \text{Por definición de } *' \text{ en } E(A) \\ = (f(x) * f(y)) * (g(x) * g(y)) & & \\ = (f *' g)(x) * (f *' g)(y) & & \end{array}$$

lo cual únicamente es cierto si $*$ es asociativa y conmutativa. □

Proposición 6 (Construcción de operaciones distributivas). *Sea $(X, *)$ un semigrupo abeliano. Cada función*

$$\begin{array}{rcl} H : X \times E(A) & \longrightarrow & E(X) \\ x & \longmapsto & h_x : \begin{array}{ccc} X & \longrightarrow & X \\ y & \longmapsto & h_x(y) \end{array} \end{array}$$

que sea homomorfismo, define una operación

$$\begin{array}{rcl} \blacklozenge : X \times X & \longrightarrow & X \\ (x, y) & \longmapsto & x \blacklozenge y = h_x(y) \end{array}$$

distributiva respecto a $*$ en X.

Demostración. Por la proposición 2, para todo elemento $x, y, z \in X$, se tiene que

$$x \blacklozenge (y * z) = (x \blacklozenge y) * (x \blacklozenge z)$$

Teniendo en cuenta que H es un homomorfismo de X en $E(X)$, entonces

$$H(x * y) = h_{x*y}, \quad y,$$

$$H(x * y) = H(x) * H(y) = h_x * h_y$$

con lo cual

$$h_{x*y} = h_x * h_y$$

Así, por la proposición 4 se tiene que

$$(x * z)\blacklozenge y = (x\blacklozenge y) * (z\blacklozenge y)$$

□

2. Operaciones distributivas externas

Hasta el momento, dado un conjunto finito X con una operación (interna) $*$ definida en él, hemos estudiado ciertos mecanismos, por medio de los cuales es posible construir otras operaciones (internas) $\circ$ que son distributivas respecto a $*$ en X. Ahora, dado un conjunto X dotado con una operación interna $*$, estudiaremos maneras de construir operaciones distributivas externas respecto a la operación $*$ en X.

Definición. Dadas dos estructuras algebraicas $(X, *), (Y, \circ)$, se dice que:

I Una operación externa

$$\begin{aligned} \bullet : X \times Y &\longrightarrow Y \\ (x, y) &\longmapsto x \bullet y \end{aligned}$$

es distributiva respecto a $\circ$ en Y si para todo $x \in X$ y todo $y, z \in Y$, se cumple que

$$x \bullet (y \circ z) = (x \bullet y) \circ (x \bullet z)$$

II Una operación externa

$$\begin{aligned} \triangleleft : X \times Y &\longrightarrow X \\ (x, y) &\longmapsto x \triangleleft y \end{aligned}$$

es distributiva respecto a $*$ en X si para todo $x, y \in X$ y todo $z \in Y$ se cumple que

$$(x * y) \triangleleft z = (x \triangleleft z) * (y \triangleleft z)$$

Aunque la anterior definición incluye todo tipo de conjuntos arbitrarios X e Y, nosotros nos centraremos en el estudio de las operaciones distributivas externas en conjuntos finitos.

Teniendo en cuenta los métodos de construcción de operaciones distributivas internas, formularemos métodos para la construcción de operaciones distributivas externas.

Proposición 7 (Construcción de operaciones distributivas externas a partir de *(i)*). *Sean $(X, *)$ e $(Y, \circ)$ dos estructuras algebraicas; cada función*

$$\begin{aligned} F : X &\longrightarrow E(Y) \\ x &\longmapsto f_x : Y \longrightarrow Y \end{aligned}$$

define una operación externa $\diamond$ distributiva respecto a $\circ$ en Y, a saber

$$x \diamond y = f_x(y)$$

Demostración. Para todo $x \in X, y, z \in Y$, se tiene que

$$\begin{aligned} x \diamond (y \circ z) &= f_x(y \circ z) && \text{Por definición de } \diamond \\ &= f_x(y) \circ f_x(z) && \text{Por ser } f_x \text{ endomorfismo de } Y \\ &= (x \diamond y) \circ (x \diamond z) && \text{Por definición de } \diamond \end{aligned}$$

Por tanto $x \diamond (y \circ z) = (x \diamond y) \circ (x \diamond z)$ □

Este método nos permitió diseñar la aplicación *Distributivas externas I* del software *APLICOP*, la cual permite encontrar todas las operaciones externas de $X \times Y$ en Y, que son distributivas a respecto a una operación definida en Y por el usuario.

Proposición 8 (Construcción de operaciones distributivas externas a partir de *(ii)*). *Sean $(X, *), (Y, \circ)$ dos estructuras algebraicas; cada función*

$$\begin{aligned} G : X &\longrightarrow X^Y \\ x &\longmapsto g_x : \begin{array}{ccc} Y & \longrightarrow & X \\ y & \longmapsto & g_x(y) \end{array} \end{aligned}$$

tal que

$$g_{x*z}(y) = g_x(y) * g_z(y) \tag{1}$$

define una operación $\bullet$ dada por

$$x \bullet y = g_x(y)$$

que es distributiva con respecto a $*$ en X.

Demostración. Para todo elemento $x, y, z \in X$, se tiene que

$$\begin{aligned} (x * z) \bullet y &= g_{x*z}(y) && \text{Por definición de } \bullet \\ &= g_x(y) * g_z(y) && \text{Por (1)} \\ &= (x \bullet y) * (z \bullet y) && \text{Por definición de } \bullet \end{aligned}$$

Por tanto $(x * z) \bullet y = (x \bullet y) * (z \bullet y)$. □

Este método nos dio pie para diseñar la aplicación *Distributivas externas II* del software *APLICOP*, la cual permite encontrar todas las operaciones externas de $X \times Y$ en X, que son distributivas a respecto a una operación definida en X por el usuario.

Se han expuesto diversos métodos para la construcción de operaciones distributivas tanto internas como externas, partiendo del hecho de que la distributividad es un caso particular de homomorfismos; utilizaremos este aspecto para construir en algunas estructuras finitas, operaciones análogas a la potenciación definida en el conjunto de los números reales ($\mathbb{R}$).

Para ello, observamos[2] cómo se construyen o definen las operaciones de potenciación en varios conjuntos numéricos. De esta observación, concluimos que las funciones recursivas es una forma de hacerlo, que el concepto de homomorfismo aparece de nuevo, y en particular, que la potenciación es distributiva a izquierda respecto a la multiplicación. Además observamos algunos ejemplos de operaciones distributivas definidas en conjuntos finitos (particularmente en $\mathbb{Z}_n$), de los cuales inferimos tales métodos.

3. Operaciones de Potenciación

A la operación de un monoide abeliano, $(X, *)$, la llamaremos **adición o suma** $(+)$; por ejemplo, la suma definida en los números naturales, enteros, racionales y reales.

Si en la misma estructura definimos una segunda operación $(\circ)$ que sea distributiva a derecha o a izquierda respecto a la adición, a tal operación la llamaremos

[2]Observaciones que omitimos es este escrito. Para más información, consultar el trabajo de grado "SOFTWARE PARA LA CONSTRUCCIÓN DE OPERACIONES ANÁLOGAS A LA POTENCIACIÓN, EN ALGUNAS ESTRUCTURAS FINITAS.

multiplicación ($\times$); por ejemplo la multiplicación definida en los números naturales, enteros, racionales y reales.

El estudio realizado de las operaciones distributivas, nos lleva a observar que no existe una única "multiplicación", es decir que no existe solamente una operación que sea distributiva con respecto a la "suma".

Ahora, si definimos una operación que sea distributiva a izquierda respecto a la multiplicación, a esta operación la llamaremos **potenciación**, la cual es una tercera operación[3], que viene a darnos resultados interesantes acerca de una estructura.

3.1. Potenciación en $\mathbb{Z}_n$

Se presentan a continuación, 5 métodos para construir operaciones de potenciación en $\mathbb{Z}_n$:

1. Hasta el momento, una operación que forma una estructura de monoide en algún conjunto, permite definir por recurrencia[4] o funciones recursivas, una operación distributiva respecto a ella. Consideremos entonces este camino para construir una operación distributiva respecto a la multiplicación en $\mathbb{Z}_n$.

   A partir de la función sucesor, definimos:

   $$\begin{aligned} a : \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ b &\longmapsto a(b) = a^b \end{aligned}$$

   donde:

   $$\begin{aligned} a(0) &= a^0 = 1 \\ a(1) &= a^1 = a^0 \times_n a \\ a(2) &= a^2 = a^1 \times_n a = (a^0 \times_n a) \times_n a = a \times_n a \\ &\vdots \\ a(k^+) &= a^{k^+} = a^k \times_n a \\ &\vdots \\ a(n-1) &= a^{n-1} = a^{n-2} \times_n a = (a^{n-2} \times_n a) \times_n a \end{aligned}$$

[3]Operación no en un sentido estricto, por cuanto existen elementos para los cuales tal operación no está definida, por ejemplo 0^0 en $\mathbb{R}$.

[4]Teniendo en cuenta que primero se debe definir en la estructura una función sucesor o un orden.

de ella se desprende que la expresión a^b significa poner a veces b y multiplicar, lo que significa reiterar la multiplicación módulo n.

Así la operación de potenciación[5] (g) en $\mathbb{Z}_n$ se puede definir como:

$$\begin{aligned} g : \mathbb{Z}_n \times \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ (a, b) &\longmapsto g(a, b) = a^b \end{aligned}$$

la cual es distributiva a izquierda respecto a $\times_n$.

La operación potenciación (g) define un homomorfismo entre los monoides $(\mathbb{Z}_n, +)$ y $(\mathbb{Z}_n, \times)$, es decir:

$$a^{b+c} = a^b + a^c$$

Su demostración se realiza con el mismo hecho que se utilizó para definir la potenciación (g), es decir la recurrencia. De igual manera la potenciación (g), cumple la propiedad $a^{b^c} = a^{b \times c}$ y su demostración se basa también en la recurrencia.

Definición. Dada la expresión $a^b = c$, donde $a, b, c \in \mathbb{Z}_n$, llamaremos a "a" **base**, a "b" **índice**[6] y a "c" **potencia**.

2. Otro método para construir operaciones de potenciación en anillos $(\mathbb{Z}_n, +_n, \times_n)$ es a partir de los homomorfismos entre $(\mathbb{Z}_n, +_n)$ y $(\mathbb{Z}_n, \times_n)$.

   Para cada a entre 0 y $n - 1$, sea

$$\begin{aligned} f_a : (\mathbb{Z}_n, +_n) &\longrightarrow (\mathbb{Z}_n, \times_n) \\ b &\longmapsto f_a(b) \end{aligned}$$

un homomorfismos entre $(\mathbb{Z}_n, +_n)$ y $(\mathbb{Z}_n, \times_n)$, donde $f_a(b) = a^b, a$ y b no son simultáneamente cero. Puesto que

$$f_a(0) = 1$$

[5]No es una operación en sentido estricto, ya que 0^0 no está definido, aspecto que no interfiere en el desarrollo del estudio.

[6]GAUSS, C. F., Disquisitiones Arithmeticae. Bogotá: Academia Colombiana de Ciencias exactas, físicas y naturales. 1995. p. 46.

y que

$$f_a(b^+) = f_a(b) +_n f_a(1)$$

entonces dando valores a $f_a(1)$, encontramos n homomorfismos que definen la operación de potenciación en $\mathbb{Z}_n$.

3. A través del estudio de operaciones isomorfas, podemos encontrar otro mecanismo para construir otras potenciaciones en $\mathbb{Z}_n$. Es decir que por ejemplo, si tomamos a $(\mathbb{Z}_n, +_n, \times_n, a^b)$, y construimos las operaciones $+'$, $\times'$ y $a^{b'}$ isomorfas a $+_n$, $\times_n$ y a^b respectivamente, por medio de una función biyectiva f, entonces $\times'$ será distributiva respecto a $+'$, y$a^{b'}$ será distributiva respecto a $\times'$. Reiteramos que a^b es una operación de potenciación.

4. Utilizando el método de construcción de operaciones distributivas a izquierda, podemos construir operaciones de potenciación, a partir de encontrar operaciones distributivas a izquierda respecto a la multiplicación en $\mathbb{Z}_n$.

5. Con base en la parte ii de la definición de operaciones distributivas externas entre las estructuras $(\mathbb{Z}_n, \times)$ y $(\mathbb{Z}_{n-1}, +, \times)$, podemos construir operaciones de potenciación externa, a partir del método de construcción correspondiente.

En adelante nos referiremos a la operación externa que es distributiva respecto a la multiplicación, que además, se asemeja a la operación de potenciación generada a partir de funciones recursivas (salvo el resultado de 0^0), como *potenciación externa*.

Hasta el momento hemos estudiado ciertas estructuras algebraicas de $\mathbb{Z}_n$ que nos permitieron construir métodos para definir operaciones de potenciación; ahora trabajaremos otras estructuras algebraicas de $\mathbb{Z}_n$, que nos servirán posteriormente, para obtener resultados acerca de la definición de operaciones equivalentes a la potenciación y análogas a la logaritmación de los números reales.

Proposición 9. *$(\Phi(n), \times_n)$ es un grupo cíclico, si y sólo si, $n = 2, 4, p^k$, 'o $2p^k$ donde p es un número primo impar, $k \in \mathbb{N}$ y $\Phi(n)$ es el conjunto de los primos relativos con n menores que n)*[7].

Como un corolario de la proposición anterior, se tiene:

Proposición 10. *Si p es un número primo, entonces $(\mathbb{Z}_P - \{0\}, \times_P)$ es un grupo* **cíclico**.

[7]PEREZ, E., Estructuras algebraicas, Bogotá: Universidad pedagógica, 2002. p.74

Los generadores de $\Phi(p)$, en adelante serán importantes, por cuanto nos permitirán definir una operación en algunas estructuras de $(\mathbb{Z}_n, +, \times)$, análoga a la logaritmación en $\mathbb{R}$.

Definición. Raíces primitivas

A los generadores de $\Phi(p)$ se les llama raíces primitivas[8] módulo p (les llamaremos también, raíces primitivas de $\mathbb{Z}_P$). Al conjunto de todos los generadores de $\Phi(p)$ lo notamos con $\mathbb{R}(\Phi(p))$.

La definición de raíces primitivas junto con la potenciación externa permitieron diseñar la aplicación *Raíces Primitivas* del software *APLICOP*, la cual permite determinar cuáles son las raíces primitivas de un $\mathbb{Z}_n$ dado, donde n es un primo impar, una potencia de tal, o dos veces tal potencia; además muestra las potencias de estas raíces primitivas a partir de la potenciación definida por funciones recursivas.

Con base en la **proposición 9**, podemos concluir que en $\mathbb{Z}_n$, con $n = 2, 4, p^k$, donde p es un primo impar y $k \in \mathbb{N}$ es posible encontrar raíces primitivas que nos permitan generar a $\Phi(n)$ por medio de la potenciación.

Estudiando los grupos cíclicos $(\Phi(n), \times_n)$, y sus raíces primitivas, observamos condiciones propicias[9], para la construcción y definición de operaciones[10] relacionadas con la potenciación externa en $\mathbb{Z}_n$, en el mismo sentido que lo es la logaritmación con la potenciación en el conjunto de los números reales, mostrando primero ejemplos de diversas maneras para definir el logaritmo en tal conjunto, como lo estudiaremos a continuación.

Observemos primero esta relación en $\mathbb{R}$, para luego definir la operación de indización, aquella que sería equivalente a la potenciación en $\mathbb{Z}_n$ y análoga a la logaritmación en $\mathbb{R}$

4. Una operación en $\mathbb{Z}_n$ análoga a la logaritmación en $\mathbb{R}$

En el conjunto de los números reales ($\mathbb{R}$), se tiene que la potenciación es equivalente a la logaritmación, en los casos en que logaritmo (log) está definido, es

[8] Ibid., p. 74.

[9] Condiciones propicias en el sentido de que cada elemento de $\Phi(p)$ se puede obtener a través de una potencia de una raíz primitiva y que cada raíz primitiva genera por completo a $\Phi(p)$.

[10] Estas operaciones están basadas en la teoría de índices de Gauss, F. para las congruencias módulo n.

decir que si $a, c \in \mathbb{R}^+$ ($\mathbb{R}^+$ el conjunto de los números reales positivos) y $b \in \mathbb{R}$ entonces

$$a^b = c \quad \text{es equivalente a} \quad b = \log_a c$$

La logaritmación se puede definir a partir de la siguiente función:

$$\begin{aligned} Log : \mathbb{R}^+ \times \mathbb{R}^+ &\longrightarrow \mathbb{R} \\ (a, b) &\longmapsto Log(a, b) = \log_a b = c \end{aligned}$$

la cual define un homomorfismo entre los monoides $(\mathbb{R}^+, \times)$ y $(\mathbb{R}^+, +)$, es decir

$$\log_a(b \times c) = \log_a b + \log_a c$$

como consecuencia del homomorfismo que cumple la potenciación, es decir:

$$x^{z+y} = x^z \times x^y$$

De igual forma que la potenciación no es estrictamente una operación, la logaritmación bajo las restricciones dadas, tampoco lo es. Nos parece interesante estudiar si las estructuras algebraicas $(\mathbb{Z}_n, +, \times)$ permiten construir una operación análoga a la logaritmación en $\mathbb{R}$, de manera similar a como se hizo en este conjunto, es decir a partir de la potenciación.

Como hemos observado en este trabajo, a lo largo del estudio de $\mathbb{Z}_n$ y sus estructuras con $+$ y $\times$, existen ciertos subconjuntos de $\mathbb{Z}_n$ que con $\times$ forman una estructura de grupo conmutativo, y además, bajo ciertas condiciones, dichos grupos son cíclicos. Puesto que en estos grupos cíclicos existen elementos (raíces primitivas) que generan a todo el conjunto, entonces éstas estructuras son *propicias* para definir tal operación análoga a la logaritmación, la cual llamaremos indización.

Con base en la **proposición 9**, sabemos las condiciones particulares de n para que $\Phi(n)$ sea un grupo cíclico. Además, sabemos que los $\mathbb{Z}_p$(p primo) con p elementos, son los conjuntos para los cuales el conjunto $\Phi(p)$ tiene el mayor número de elementos distintos, es decir $p - 1$, y por tanto el más cercano, en número de elementos, a $\mathbb{Z}_p$. En segunda instancia están los $\mathbb{Z}_n$ con $n = p^k$(p primo y k natural), para los cuales el conjunto $\Phi(n)$ tiene $p^{k-1}(p - 1)$ elementos.

En lo que sigue, definiremos la operación de indización, primero en los $\mathbb{Z}_p$ con p un primo impar y posteriormente sobre los demás $\mathbb{Z}_n$ para $n = p^k$(p primo y k natural).

4.1. Operaciones de la indización

Los $\mathbb{Z}_n$ que estudiaremos, serán para los cuales n es 2, 4, una potencia de un primo impar o dos veces dicha potencia.

1. Para el caso particular $n = 2, \Phi(2) = \{1\}$, luego 1 es una raíz primitiva que genera a todo el conjunto $\Phi(n) = \{1\}$, es decir que existe un único índice para 1 en base 1 que es 1.

2. Para el caso particular $n = 4, \Phi(4) = \{1, 3\}$, y allí 3 es la única raíz primitiva que genera todo $\Phi(4)$, donde $3^1 = 3$ y $3^2 = 1$, luego se puede definir la indización con respecto a la raíz 3 con la función:

$$\begin{aligned} ind_3 : \Phi(4) &\longrightarrow \mathbb{Z}_2 \\ 3 &\longmapsto 1 \\ 1 &\longmapsto 3 \end{aligned}$$

3. Para el caso en el cual $n = p^k$, o $n = 2 \times p^k$ donde p es un primo impar, y k es un número natural, $\Phi(n)$ (para ambos casos) es un conjunto con °linebreak$p^{m-1}(p-1)$ elementos, que posee $\phi(p^{m-1}(p-1))$ raíces primitivas, la operación de indización se define como:

$$\begin{aligned} Ind : \mathbb{R}(\Phi(n) &\longrightarrow \mathbb{Z}_{\phi(n)} \\ (a, b) &\longmapsto Ind(a, b) = ind_a b = c \end{aligned}$$

donde $a^c = b, \phi(n)$ indica la función ϕ de Euler, es decir el número de primos relativos con $n_{\text{¸}}$ menores que n.

Ejemplo. Sea $p = 3$, y $n = p^2 = 9$. Tomemos a $(\mathbb{Z}_9, +, \times)$ con la potenciación externa.

$$\Phi(9) = \{1, 2, 4, 5, 7, 8\}$$

$$\mathbb{R}(\Phi(9)) = \{2, 5\}$$

La operación de indización esta dada por:

$ind_a c$	1	2	4	5	7	8
2	0	1	2	5	4	3
5	0	5	4	1	2	3

Ejemplo. Sea $p = 5$, y $n = 2 \times p = 10$. Tomemos a $(\mathbb{Z}_{10}, +, \times)$ con la potenciación externa.

$$\Phi(10) = \{1, 3, 7, 9\}$$
$$\mathbb{R}(\Phi(10)) = \{3, 7\}$$

La operación de indización esta dada por:

$ind_a c$	1	3	7	9
3	0	1	3	2
7	0	3	1	2

Proposición 11. *La función*

$$ind_a : \Phi(n) \longrightarrow \mathbb{Z}_{\phi(n)}$$
$$b \longmapsto ind_a b = c$$

donde $a^c = b$*, es una función biyectiva.*

Para el grupo cíclico $(\Phi(n), \times)$ con la operación de indización ya definida, existen ciertas propiedades que permiten calcular índices en una base dada; dichas propiedades se enuncian a continuación:

Proposición 12. *La operación de indización, define el homomorfismo*

$$ind_a(x \times y) = ind_a x + ind_a y$$

Corolario. *La operación de indización cumple la igualdad*

$$ind_a \frac{x}{y} = ind_a x - ind_a y$$

Proposición 13. *La operación de indización cumple la igualdad*

$$ind_a(x^y) = y \times ind_a x$$

Proposición 14. *Dado un numero* $d \in \Phi(p)$*, y* $a, b \in \mathbb{R}(\Phi(p))$*, entonces*

$$ind_b d = ind_a d \times ind_b a$$

Ejemplo. Sea $p = 7$, y $n = 2 \times 7 = 14$. Tomemos a $(\mathbb{Z}_{14}, +, \times)$ con la potenciación externa.

$$\Phi(14) = \{1, 3, 5, 9, 11, 13\}$$
$$\mathbb{R}(\Phi(14)) = \{3, 5\}$$

Dada la raíz primitiva 3, encontramos que

$ind_a c$	1	3	5	9	11	13
3	0	1	5	2	4	3

A partir de ésta y de la **proposición 13**, podemos encontrar los índices correspondientes a la raíz primitiva 5, así:

Sabiendo que $ind_5 3 = 5$, entonces para cada $d \in \Phi(14)$ luego:

$ind_a c$	1	3	5	9	11	13
5	0	5	1	4	2	3

Con lo anterior, podemos resolver cierto tipo de ecuaciones en $\mathbb{Z}_n$, con n bajo las condiciones expuestas para poder definir la operación de indización, veamos:

Ejemplo. Resolvamos la ecuación

$$11 \times 5^x = 9^x \times 3$$

en el campo $(\mathbb{Z}_{14}, +, \times)$ con la potenciación externa. Aplicando la función de indización con la raíz primitiva 3, a los elementos 11×5^x y $9^x \times 3$, se tiene:

$$ind_3 11 \times 5^x + ind_3 9^x \times 3$$

y por **proposición 12**

$$ind_3 11 + x \times ind_3 5 = x \times ind_3 9 + ind_3 3$$

$$4 + (x \times 5) = (x \times 2) + 3$$

sumando a ambos lados el inverso aditivo de 4 y de $(x \times 2)$ en $\mathbb{Z}_{13}$, tenemos

$$x \times 5 - (x \times 2) = 1 + 2$$

$$x \times (5 - 2) = 3$$

$$x \times 3 = 3$$

De donde, $x = 1, 3$ o 5.

Con el estudio de las operaciones distributivas, particularmente las externas, fue posible definir una operación (no en sentido estricto) en estructuras de $\mathbb{Z}_n$, análoga a la potenciación en $\mathbb{R}$ con el uso de homomorfismos, y a partir de ésta y de la teoría de índices, una operación en algunas estructuras de $\mathbb{Z}_n$, análoga a la logaritmación en $\mathbb{R}$, que se denominó *indización*, la cual cumple con propiedades similares a las de la logaritmación y permite resolver ecuaciones como las expuestas en los ejemplos anteriores.

Bibliografía

[1] APÓSTOL. T., *Análisis matemático*. Barcelona: Ed. Reverté, 1988.

[2] ———,*Calculus*, Vol. I., Barcelona: Ed. Reverté, 1988.

[3] CAMPOS, A., *Axiomática y geometría desde Euclides hasta Hilbert y Bourbaki*. Tomo 24. Bogotá: Universidad Nacional, 1994.

[4] CHARTE, F., *Programación con Visual Basic.Net*. Ed. Anaya multimedia, 2002.

[5] DONADO, A.; LUQUE, C. y PÁEZ, J., *H-Conjuntos*. XIV coloquio Distrital de matemáticas y estadística. Universidad Pedagógica, 1997.

[6] DORRUNSORO, J. y HERNANDEZ, E., *Números, Grupos y Anillos*. Madrid: Addisón - Wesley, 1996.

[7] DUBREIL, P.; DUBREIL y JACOTIN, M., *Lecciones De Algebra Moderna*. Ed. Reverté 1965.

[8] FRALEIGH, J., *A First Course In Abstract Algebra*. Ed. Addison - Wesley, Sixth Printing 1974.

[9] GAUSS, C. F., *Disquisitiones Arithmeticae*. Bogotá: Academia Colombiana de Ciencias exactas, físicas y naturales. 1995.

[10] GENTILE, E., *Estructuras Algebraicas I*. OEA 1977.

[11] HALVORSON, M., *Microsoft Visual Basic.Net -Aprenda Ya-*. Ed. McGraw - Hill.

[12] LUQUE, C.; MORA, L. y PÁEZ, J.,*Actividades matemáticas para el desarrollo de procesos lógicos*. Universidad Pedagógica Nacional. Bogotá: Ediciones Ántropos Ltda., 2002.

[13] LUQUE, C.; DUQUE, O. y NEIRA, C., *¿Cómo Hacer Álgebra?* Parte 2. X Coloquio Distrital de Matemáticas y Estadística.

[14] MEN. *Proyecto de Incorporación de Nuevas Tecnologías al Currículo de Matemáticas de la Educación Media de Colombia*. ¡http://innovemos-p.unesco.cl/medios/Documentos/Innovaciones/eya/cecico.doc¿

[15] PEREZ, E., *Estructuras algebraicas*, Bogotá: Universidad pedagógica, 2002.

[16] STEIN S.,*Cálculo y geometría analítica*. México: McGraw- Hill, 1982.

[17] SUÁREZ, C., *Los Entornos Virtuales De Aprendizaje Como Instrumento De Mediación*. Universidad de Salamanca: ¡http://www3.usal.es/ ∼ teoriaeducacion/rev_numero_04/n4_art_suarez.htm¿

[18] TAKEUCHI Y.,*Sucesiones y series*. Tomo II.