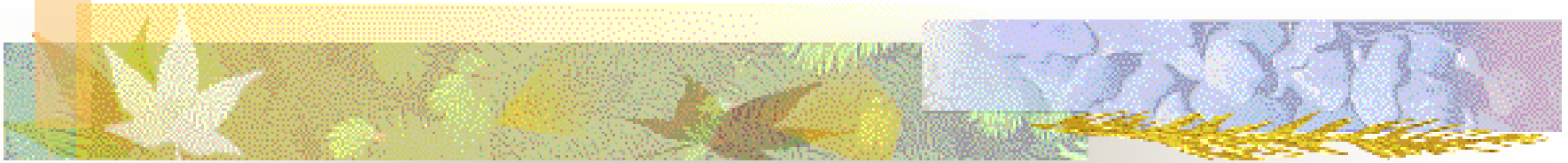
Estructuras Algebraicas



UCR – ECCI

CI-1204 Matemática Discretas

Prof. M.Sc. Kryscia Daviana Ramírez Benavides

Estructuras Algebraicas

- Sea E un conjunto no vacío, una función f

$$f : E \times E \mapsto E$$

se llama **ley de composición interna** (operación) sobre E. Además, la imagen $f(a,b)$ se llama el operado de a y b.

- Es usual representar las operaciones internas con algunos símbolos especiales, en vez de letras, como *, Δ, $\perp$, entre otros.
- Por definición, si * es una ley de composición interna sobre E, entonces es **cerrada** sobre E, es decir, se cumple que

$$\forall a,b \in E\left[a * b \in E\right]$$

Estructuras Algebraicas (cont.)

- Si * es una ley de composición interna sobre E, se dice que (E,*) posee una **estructura algebraica**.
- Una **estructura algebraica** es una n-tupla $(a_1,a_2,...,a_n)$, donde a_1 es un conjunto dado no vacío, y $\{a_2,...,a_n\}$ un conjunto de operaciones aplicables a los elementos de dicho conjunto.
- Si * es una ley de composición interna sobre E, se dice que *:
  - Es **asociativa:** para cualesquiera elementos del grupo no importa el orden en que se operen las parejas de elementos, mientras no se cambie el orden de los elementos, siempre dará el mismo resultado. Si $\forall a,b \in E$ se cumple $(a*b)*c = a*(b*c)$

Estructuras Algebraicas (cont.)

- Si * es una ley de composición interna sobre *E*, se dice que *:
  - Posee **elemento neutro o elemento identidad** (comúnmente denotado como *e*, letra inicial de la palabra alemana ***einheit***, que significa "unidad"): existe un elemento que al ser operado con cualquier otro, no lo modifica (como el cero en la suma o el 1 en la multiplicación). La unicidad del elemento neutro es fácilmente demostrable. $\text{Si } \exists e \in \forall a \in E \text{ tal que } a * e = e * a = a$
  - Tiene **elementos opuestos o inversos**: todos los elementos del grupo tienen un elemento opuesto (o inverso), con el que al operarse dan por resultado el elemento neutro *e*. El elemento inverso de uno dado es único.

$$\text{Si } \forall a \in E \wedge \exists b \in E \text{ tal que } a * b = b * a = e$$

$$\text{en cuyo caso se escribe } a^{-1} = b$$

Estructuras Algebraicas (cont.)

- Si * es una ley de composición interna sobre *E*, se dice que *:
  - Es **conmutativa**: para cualesquiera elementos del grupo no importa el orden de los elementos siempre dará el mismo resultado. Si $\forall a, b \in E$ se cumple $a * b = b * a$
- Un elemento *h* es **absorbente** por la izquierda si *h* * *a* = *h* y lo es por la derecha si *a* * *h* = *h* para todo *a*. Se dice que es el elemento absorbente si lo es por la derecha y por la izquierda.

Estructuras Algebraicas (cont.)

- En el caso que *E* sea un conjunto finito, es decir, E = $\{a_1, a_2, \ldots, a_n\}$, la operación * se puede representar en una **tabla**, en la cual la entrada *i,j* denota el elemento $a_i * a_j$:

*	a_1	a_2	…	a_j	…	a_n
a_1	$a_1 * a_1$		…		…	
a_2	$a_2 * a_1$	$a_2 * a_2$	…	$a_2 * a_j$	…	$a_2 * a_n$
…	…	…	…	…	…	…
a_i	$a_i * a_1$	$a_i * a_2$	…	$a_i * a_j$	…	$a_i * a_n$
…	…	…	…	…	…	
a_n	$a_n * a_1$	$a_n * a_2$	…	$a_n * a_j$	…	$a_n * a_n$

Estructuras Algebraicas (cont.)

- Un elemento *a* es **idempotente** si $a * a = a$ para todo *a*.
- Un elemento *a* es **involutivo** si $a * a = e$ para todo *a*.
- Un elemento *a* es **central** si conmuta con todos los elementos de *E*, el conjunto formado por todos los elementos centrales se llama el **centro de *E*** y se denota por $C(E)$.
  - $(C(E),*)$ es un subgrupo de $(E,*)$.

$$C(E) = \{a \in E \mid ab = ba, \forall b \in E\}$$

Grupos

- Si G es un conjunto no vacío y * es una operación interna definida sobre G. Se dice que $(G,*)$ es:
  - Un **semigrupo** si * es asociativa.
  - Un **monoide** si es un semigrupo con elemento neutro.
  - Un **grupo** si es un monoide que cumple la propiedad de los inversos, es decir, $(G,*)$ es un grupo si * es cerrada, asociativa, posee elemento neutro y cada elemento tiene inverso.
  - Un **grupo abeliano** o **grupo conmutativo** si es un grupo y se cumple la conmutatividad. En el caso de que no sea un grupo, se dice que la estructura algebraica es conmutativa.

Grupos (cont.)

- Notaciones:
  - La notación multiplicativa $\otimes$.
    - Operación: $*$, $\times$, $\bullet$, llamada producto.
    - Elemento neutro: 1.
    - Elemento inverso: x^{-1}.
  - La notación aditiva $\oplus$.
    - Operación: +, llamada suma.
    - Elemento neutro: 0.
    - Elemento opuesto de un elemento x del grupo: $-x$.

Grupos (cont.)

- Si $(G,*)$ es un monoide, se tiene que $a^0 = e$, y para n natural, con $n \geq 1$:

$$a^n = a * a^{n-1}$$

$$a^n = \underbrace{a * a * a * \ldots * a}_{n \text{ veces } a}$$

- Si además cumple con la propiedad de los inversos, los exponentes negativos se definen como:

$$a^{-n} = \left(a^{-1}\right)^n$$

Grupos (cont.)

- **Teorema 1.** Si $(G,*)$ es un grupo, en general se tiene que

$$(a*b)^{-1} = b^{-1}*a^{-1} \qquad (1)$$

$$\left(a^{-1}\right)^{-1} = a \qquad (2)$$

- **Demostración.** (1)

$$(a*b)*(a*b)^{-1} = e$$

$$(a*b)*\left(b^{-1}*a^{-1}\right) = a*\left(b*b^{-1}\right)*a^{-1}$$

$$= a*e*a^{-1}$$

$$= a*a^{-1}$$

$$= e$$

(2)

$$\left(a^{-1}\right)^{-1} = \left(a^{-1}\right)^{-1}*e$$

$$= \left(a^{-1}\right)^{-1}*\left(a^{-1}*a\right)$$

$$= \left(\left(a^{-1}\right)^{-1}*a^{-1}\right)*a$$

$$= e*a$$

$$= a$$

Grupos (cont.)

- Notar que si el grupo es abeliano se puede escribir

$$(a * b)^{-1} = a^{-1} * b^{-1}$$

- En caso contrario se debe respetar (1) del teorema 1.
- Si el grupo es finito, su **orden** se denota por $o(G)$ y corresponde a la cardinalidad como conjunto.
- Para $n \in N$ con $n \geq 2$, y la relación $\Re$ definida sobre Z por $a \Re b \Leftrightarrow [\exists k \in Z \text{ tal que } a - b = nk]$ se define al conjunto $Z_n = Z/\Re$, es decir, Z_n es el conjunto de clases residuales módulo n.
- Sobre estos conjuntos Z_n, se definen las operaciones usuales de suma $\oplus$ y multiplicación $\otimes$ de clases.

Grupos (cont.)

- Para todo $n \geq 2$, $(Z_n, \oplus)$ es grupo abeliano y $o(Z_n) = n$.
- $(Z_n^*, \otimes)$ es grupo abeliano si y sólo si n es un número primo. Además, $o(Z_n^*) = n - 1$.
- Sea G un grupo, y un elemento $x \in G$. se dice que G es un **grupo cíclico** generado por x si para cada elemento $y \in G$ existe un $n \in Z$ tal que $y = x^n$.

Grupos (cont.)

- **Teorema 2.** Si *G* es cíclico entonces es grupo abeliano, y si *G* es generado por *x* entonces también es generado por su inverso x^{-1}.
- **Demostración.**

(1)

$$y, z \in G \Rightarrow \exists n, m \in Z \text{ tal que } y = x^n \wedge z = x^m$$

$$yz = x^n x^m = x^{n+m} = x^{m+n} = x^m x^n = zy$$

Es grupo abeliano

(2)

$$y \in G \Rightarrow \exists n \in Z \text{ tal que } y = x^n$$

Es decir, $y = \left(x^{-1}\right)^{-n} \wedge -n \in Z$

G es generado por x^{-1}

Grupos (cont.)

- Para el conjunto $X = \{1, \ldots, n\}$, se define el **grupo simétrico** $\boldsymbol{S_n}$ como el conjunto de todas las funciones biyectivas de X en X, dotado con la composición de funciones como operación interna.
- El orden de S_n es $n!$, $o(S_n) = n!$.
  - Al asignar la imagen al primer elemento se tienen n posibilidades al fijar una de éstas, para asignar la imagen del segundo elemento se tienen $n - 1$ posibilidades; así, al fijar las imágenes para hacer la función biyectiva, el número de funciones que se obtiene es $n!$.
- Si p es un número primo y G un grupo, se dice que G es un ***p*-grupo** si su orden es una potencia de p.

Subgrupos

- Algunos conjuntos que poseen estructura de grupo, poseen subconjuntos que también tienen esta misma estructura de grupo.
- Si $(G,*)$ es un grupo, $H \subseteq G$ con $H \neq \emptyset$, H se llamará **subgrupo** de G, y se denota por $H < G$, si y sólo si $(H,*)$ es un grupo.
  - Un subgrupo es un subconjunto no vacío del grupo que sea grupo con la operación restringida a sus elementos.

Subgrupos (cont.)

- **Teorema 3 (De Lagrange).** El orden del subgrupo es un divisor del orden del grupo. (Buscar demostración)
- **Teorema 4.** Sea $(G,*)$ un grupo, con $H \subseteq G$ con $H \neq \varnothing$, entonces $H < G \Leftrightarrow \forall a,b \in H\left[a * b^{-1} \in H\right]$
- **Demostración.** Ver libro en la página 322.
- **Teorema 5.** Sea $(G,*)$ un grupo finito, con $H \subseteq G$ con $H \neq \varnothing$, entonces $H < G \Leftrightarrow \forall a,b \in H\left[a * b \in H\right]$
- **Demostración.** Ver libro en la página 323,

Subgrupos (cont.)

- El teorema 3 determina la cantidad de elementos que debe tener un subgrupo, en caso de que el grupo tenga orden finito.
- Los teoremas 4 y 5 dan la condición necesaria y suficiente para el caso que se quiera demostrar, o verificar, que un subconjunto de un grupo es o no un subgrupo de él.
- Además, al ser de equivalencia en ambos teoremas, en el caso de que no se cumpla la condición de cerradura planteada, se concluye que el subconjunto no es subgrupo.

Subgrupos (cont.)

- **Teorema 6.** Un subgrupo de un *p*-grupo es un *p*-grupo.
- **Demostración.**

$$H < G \wedge G \text{ es un } p\text{-grupo} \Rightarrow o(G) = p^{\alpha}$$

$$\text{Teorema de Lagrange}: o(H) \text{ divide } o(G) = p^{\alpha} \Rightarrow o(H) = p^{\alpha'}, \alpha' < \alpha$$

$$H \text{ es } p\text{-grupo}$$

Subgrupos (cont.)

- Una condición necesaria para que $(Z_n^*, \otimes)$ sea grupo es que p sea primo. Así, en el caso que p no es primo no se obtiene la deseada estructura de grupo.
  - Al considerar el subconjunto de Z_n^* formado por las clases residuales que son relativamente primos con n, se obtiene un grupo abeliano.
- El conjunto U_n, definido por $U_n = \{\dot{a} \in Z_n^* / m.c.d.(a,n) = 1\}$ es un grupo abeliano.

Homomorfismos de Grupo

- Si $(G,*)$ y $(F,\perp)$ son dos grupos. Se dice que una aplicación $f : G \to F$ es un **homomorfismo de grupos** si para todo a y b en G se satisface que $f(a * b) = f(a) \perp f(b)$. Si, además de ser homomorfismo,
  - f es sobreyectiva, entonces f es un **epimorfismo**.
  - f es inyectiva, entonces f es un **monomorfismo**.
  - f es biyectiva, entonces f es un **isomorfismo**.
  - $G = F$, entonces f es un **endomorfismo**.
  - $G = F$ y biyectiva, entonces f es un **automorfismo**.

Homomorfismos de Grupo (cont.)

- Para un homomorfismo de grupos $f : G \rightarrow F$ se define el **núcleo de *f*** como el conjunto $N_f = f^{-1}(\{e'\})$, donde e' es el elemento neutro de F.
  - El núcleo de un homomorfismo está formado por los elementos cuya imagen es el neutro.
    - $ker_f = N_f = \{x \in G \mid f(x) = e'\}$

Homomorfismos de Grupo (cont.)

- **Teorema 7.** Si $f : G \to F$ es un homomorfismo de grupos, si e es el elemento neutro de G y además e' es el elemento neutro de F, entonces se cumple que

$$f(e) = e' \qquad (1)$$

$$f(x^{-1}) = [f(x)]^{-1} \qquad (2)$$

- **Demostración.**

(1)

$$f(x) = f(x * e) = f(x) \perp f(e)$$
$$f(x) = f(x) \perp f(e) = f(x) \perp e'$$
$$f(e) = e'$$

(2)

$$f(e) = e' \Rightarrow f(x * x^{-1}) = f(x) \perp f(x^{-1})$$
$$f(x) \wedge f(x^{-1}) \text{ son inversos entre sí}$$
$$f(x^{-1}) = [f(x)]^{-1}$$

Homomorfismos de Grupo (cont.)

- **Teorema 8.** Sea $f : G \to F$ es un homomorfismo de grupos, con e el elemento neutro de G y e' el elemento neutro de F, si $N_f = \{e\}$ entonces f es inyectiva.
- **Demostración.**

$$f(a) = f(b) \Rightarrow f(a)[f(b)]^{-1} = e'$$
$$\Rightarrow f(a)f(b^{-1}) = e'$$
$$\Rightarrow f(ab^{-1}) = e'$$
$$\Rightarrow ab^{-1} \in N_f = \{e\}$$
$$\Rightarrow ab^{-1} = \{e\}$$
$$\Rightarrow a = b$$

f es inyectiva

Anillos

- Un **anillo** es una estructura algebraica formada por un conjunto y dos operaciones que están relacionadas entre sí, mediante la propiedad distributiva, de manera que generalizan las nociones de número, especialmente en el sentido de su "operabilidad".
  - En un anillo se tienen un conjunto no vacío *A*, y dos operaciones binarias + y •.

Anillos (cont.)

- Un anillo es un triple $(A,*,\circ)$, lo cual es una estructura algebraica en la cual A es un conjunto no vacío y $*,\circ: A \times A \rightarrow A$ son dos operaciones binarias definidas sobre A que satisfacen las condiciones siguientes:
  - $(A,*)$ es un grupo abeliano.
  - $(A,\circ)$ es un semigrupo.
  - La operación $\circ$ es distributiva respecto a la operación $*$. Esto es, para todo $a,b \in A$

$$\begin{cases} a \circ (b * c) = (a \circ b) * (a \circ c) \\ (a * b) \circ c = (a \circ c) * (b \circ c) \end{cases}$$

Anillos (cont.)

- Cuando $(A,\circ)$ es un monoide se dice que A es un **anillo unitario** o **anillo con unidad** que representaremos por 1 (elemento neutro del producto).
- Cuando $(A,\circ)$ es un semigrupo conmutativo, se dice que A es **anillo conmutativo** o **anillo abeliano**.

Anillos (cont.)

- Para trabajar con una notación más familiar, el anillo $(A,+,\bullet)$, en el cual:
  - El neutro de $(A,+)$ se denota 0, y para todo $x \in A$, a su inverso (para la operación +) se denotará $-x$.
  - Si la operación $\bullet$ posee neutro en A, éste se denotará por 1 y se dice que $(A,+,\bullet)$ es un **anillo con unidad**.
  - Si $x \in A$ posee inverso para la operación $\bullet$, éste se denotará por x^{-1}. Si $\bullet$ es conmutativa, $(A,+,\bullet)$ se llamará **anillo conmutativo**.

Anillos (cont.)

- El ejemplo más sencillo y representativo de estructura de anillo se encuentra en $(Z,+,\bullet)$, el anillo de los enteros. Este anillo tiene unidad y es conmutativo.
- Por similitud con $(Z,+,\bullet)$, cuando tratemos con un anillo unitario cualquiera, en general se refiere a la suma y al producto como primera y segunda operación, respectivamente, y se utiliza el 0 y el 1 como neutros respectivos.
  - Para abreviar la notación, se escribe ab en lugar de $a \bullet b$.

Anillos (cont.)

- Los axiomas de anillo son una abstracción del comportamiento de los números enteros respecto de las operaciones aritméticas elementales: la suma y el producto.
- Otra clase importante de anillos abelianos unitarios finitos es $(Z_n,+,\bullet)$ el anillo de los enteros módulo n.

Anillos (cont.)

- Sea $(A,+,\bullet)$ un anillo, entonces:
  - $(\forall x \in A)\ 0 \bullet x = x \bullet 0 = 0$.
  - $(\forall x,y \in A)\ -(x \bullet y) = (-x) \bullet y = x \bullet (-y)$.
  - $(\forall x,y \in A)\ (-x) \bullet (-y) = x \bullet y$.
  - Si el anillo posee unidad, entonces $(\forall x \in A)\ -x = (-1) \bullet x = x \bullet (-1)$.
- La **ley de simplificación** es otra propiedad importante que cumplen los números enteros, es decir, para todo $a,b,c \in Z^* = Z - \{0\}$ se verifica $ab = ac \Rightarrow b = c$.

Anillos (cont.)

- La propiedad de ley de cancelación está relacionada con la definición:
  - El anillo $(A,+,\bullet)$ admite divisores de cero si existen $a,b \in A^* = A - \{0\}$ tales que $ab = 0$.
    - Los elementos [2] y [3] de Z_6 son dos divisores de cero.
    - Los divisores de cero de un anillo Z_n son aquellas clases cuyos elementos no son primos relativos de n ($mcd(n,a) \neq 1$).
- **Teorema.** Sea el anillo $(A,+,\bullet)$, entonces es válida la ley de cancelación si y sólo si no tiene divisores de cero.
  - Se llama **dominio de integridad**, a un anillo conmutativo unitario que no contiene divisores de cero.

Referencias Bibliográficas

- Murillo, Manuel. “Introducción a la Matemática Discreta”. 2da edición, Editorial Tecnológica de Costa Rica. Cartago, 2007.
- Wikipedia. “Estructura algebraica”. URL: http://es.wikipedia.org/wiki/Estructura_algebraica. Modificado 22 de febrero del 2009.
- “Anillos y cuerpos”. URL: http://www.edicionsupc.es/ftppublic/pdfmostra/ME02405M.pdf.
- Wikipedia. “Anillos”. URL: http://es.wikipedia.org/wiki/Anillo_(matem%C3%A1tica). Modificado 18 de septiembre del 2008.