[Tema 1]. ELEMENTOS DE ÁLGEBRA ABSTRACTA
(Notas incompletas de clase)
—*Incompletas* y por tanto, *imperfectas*—

[Versión: 1.4.2.alpha2- D:20140425195654+02'00'][0]

«¿Puede alguien pensar que porque seamos ingenieros, no nos preocupa la belleza o que no intentamos construir estructuras bellas, sólidas y permanentes? ¿No están las genuinas funciones de fuerza siempre en coordinación con condiciones no escritas de armonía?... Además, existe una atracción, un particular encanto en lo colosal al que las teorías ordinarias del arte no se aplican». Alexandre Gustave EIFFEL (1832-1923). En (en inglés): *Remaking the World: Adventures in Engineering* (Henry Petroski, 1998, p. 173).

7. ESTRUCTURAS ALGEBRAICAS

7.1. Ley de composición interna

Definición 7.1.-
Sea un conjunto $A \neq \emptyset$. Se entiende por ***ley de composición interna*** *en A a cualquier aplicación $* : A \times A \longrightarrow A$.*

Definición 7.2.-
Una ***operación n-aria*** *sobre A es una aplicación de A^n en A. Si $n = 2$ se tiene una* operación binaria*, si $n = 3$ una operación* ternaria*, si $n = 4$,* cuaternaria*, etc. Una ley de composición interna en un conjunto A es una operación binaria sobre A —y una relación ternaria sobre A (*vid. supra *def. 3.31)—.*

Definición 7.3.-
Dados un conjunto $A \neq \emptyset$ y $* : A \times A \longrightarrow A$ una operación binaria sobre A, son frecuentes tres notaciones para el resultado de operar dos elementos $x, y \in A$:
a) ***prefijo****: $*xy$ o $*(x, y)$;*
b) ***infijo****: $x * y$;*
c) ***sufijo*** *o* ***postfijo****: $xy*$ o $(x, y)*$.*
Para el caso de una operación n-aria $* : A^n \longrightarrow A$ y n elementos de A, $x_1, x_2, \ldots, x_n$, es similar: prefijo*: $*x_1x_2 \ldots x_n$ o $*(x_1, x_2, \ldots, x_n)$,* infijo*: $x_1 * x_2 * \cdots * x_n$ y* postfijo*: $x_1x_2 \ldots x_n*$ o $(x_1, x_2, \ldots, x_n)*$.*

Definición 7.4.-
Dados un conjunto $A \neq \emptyset$ y $* : A^n \longrightarrow A$ una operación n-aria sobre A, se dice que un subconjunto $B \subseteq A$ es ***parte estable*** *de $(A; *)$ —o que B es* ***cerrado*** *para $*$—, precisamente si:*

$$(\forall x_1, x_2, \ldots, x_n \in B)\,(x_1 * x_2 * \cdots * x_n \in B)$$

Definición 7.5.-
Sean un conjunto $A \neq \emptyset$ y $* : A \times A \longrightarrow A$ una operación binaria sobre A. Sean $a, b \in A$. Se dice que:
a) a y b son ***elementos permutables****, en A para $*$ (o que a permuta con b, o viceversa), precisamente si $a * b = b * a$;*
b) a es un ***elemento central****, en A para $*$, precisamente si permuta con todo elemento de A;*
c) el ***centro*** *de A para $*$, es el conjunto de todos los elementos centrales de A.*

Ejemplo 7.1.-
Sean los conjuntos $\mathbb{N}$ y $\mathbb{Z}$ y las aplicaciones $+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ (suma de números enteros) y $- : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ (diferencia de números enteros).

a) $+$ y $-$ son operaciones binarias sobre $\mathbb{Z}$;
b) su notación es infija;
c) $\mathbb{N}$ es parte estable para $+$ pero no lo es para $-$ ($\exists x, y \in \mathbb{N}, x - y \notin \mathbb{N}$, por ejemplo, $x = 3, y = 7$);
d) cualesquiera dos números naturales o dos números enteros son permutables para $+$ ($+$ es conmutativa sobre $\mathbb{N}$ y sobre $\mathbb{Z}$);
e) el único elemento central en $\mathbb{N}$ y en $\mathbb{Z}$ para $+$ es el cero (elemento neutro de $+$), es decir, el centro de $\mathbb{N}$ y de $\mathbb{Z}$ para $+$ es $\{0\}$. No existen elementos centrales para $-$, ni en $\mathbb{N}$ ni en $\mathbb{Z}$, es decir, el centro de $\mathbb{N}$ y de $\mathbb{Z}$ para $-$, es $\emptyset$.

7.2. Estructura algebraica

Definición 7.6.-
Se dice que un conjunto $A \neq \emptyset$ posee una ***estructura algebraica****, precisamente si sobre él se define un número finito de leyes de composición, internas o externas*[1]*. Suele decirse que el conjunto A es el* ***soporte*** *de la estructura.*

Observación 7.1.-
Podríamos comparar una estructura algebraica con el esqueleto humano, considerándolo como la estructura básica del cuerpo humano. Si en este momento nos comparamos, apreciaremos grandes diferencias entre nosotros, pero si nos pudiésemos comparar dentro de 10,000 *años, nos veríamos prácticamente iguales. Aunque la apariencia externa sea diferente, la estructura interna es la misma. De igual forma, las estructuras matemáticas representan esta semejanza subyacente en situaciones que aparentemente son distintas. La utilidad de la formalización de las estructuras radica en la generalización resultante; a partir de tal formalización, se deducen unas propiedades, características comunes a todos los ejemplos de la misma estructura, que servirán para demostrar otros hechos (consecuencias). Estos nuevos hechos, se verificarán en cualquier caso particular de esa misma estructura. Si en el ejemplo del esqueleto decimos «la tibia y el peroné están unidos», no necesitaríamos confirmar de nuevo esto en todas las personas, pues todas tienen la misma estructura. La idea, por tanto, es que una estructura matemática es una abstracción de propiedades comunes encontradas en diversas situaciones.*

Observación 7.2.-
En este tema se estudian algunas estructuras básicas: magma (grupoide), semigrupo, monoide, grupo, semianillo, anillo, dominio de integridad *y* cuerpo*, todas dependientes del concepto de ley de composición interna. En temas posteriores se estudiarán otras estructuras algebraicas, como* espacios vectoriales[2]*,* módulos[3] *o* álgebras[4]*, dependientes además del concepto de* ley de composición externa —vid. infra *def. 14.1*—.

[0] Utilizamos una asignación de versiones similar al clásico versionado de software —*cfr.* http://es.wikipedia.org/wiki/Versión_de_software y http://es.wikipedia.org/wiki/Fases_del_desarrollo_de_software, con el añadido de la fecha, hora y zona mundial horaria de la puesta al día (D) del documento—.

[1] Ley de composición externa, *vid. infra* def. 14.1.

[2] http://es.wikipedia.org/wiki/Espacio_vectorial

[3] http://es.wikipedia.org/wiki/Módulo_(matemática)

[4] http://es.wikipedia.org/wiki/Álgebra_sobre_un_cuerpo

7.3. Magma o grupoide

Definición 7.7.-

Sean un conjunto $A \neq \emptyset$ y $* : A \times A \longrightarrow A$ una operación binaria en A. En tal caso, se dice que el par $(A;*)$ es un ***magma*** *(o* ***grupoide****).*

Definición 7.8.-

Sean $(A;*)$ un magma y $a \in A$. Se dice que a es ***idempotente*** *(en A para $*$), precisamente si $a * a = a$.*

Definición 7.9.-

Sean $(A;*)$ un magma y $s \in A$. Se dice que s es:

a) ***singular o absorbente por la izquierda*** *(en A para $*$), precisamente si $(\forall a \in A)\,(s * a = s)$;*

b) ***singular o absorbente por la derecha*** *(en A para $*$), precisamente si $(\forall a \in A)\,(a * s = s)$;*

c) ***singular o absorbente*** *(en A para $*$), precisamente si lo es por la izquierda y por la derecha.*

Ejemplo 7.2.-

a) Consideremos la interpretación $(\mathbb{N};\cdot)$:
   1) constituye un modelo de magma;
   2) existen dos elementos idempotentes: 0 y 1;
   3) solo existe un elemento absorbente: 0.

b) Las interpretaciones $(\mathbb{N};+)$, $(\mathbb{Z};+)$, $(\mathbb{Z};-)$, $(\mathbb{Z};\cdot)$, $(\mathbb{Q};+)$, $(\mathbb{Q};-)$, $(\mathbb{Q};\cdot)$, $(\mathbb{Q}\backslash\{0\};/)$, $(\mathbb{R};+)$, $(\mathbb{R};-)$, $(\mathbb{R};\cdot)$ y $(\mathbb{R}\backslash\{0\};/)$ son modelos de magma.

c) El par $(\mathbb{N};-)$ no es un monoide ($-$ no es una operación en $\mathbb{N}$). Tampoco lo son ni $(\mathbb{N};/)$ ni $(\mathbb{Z};/)$ ni $(\mathbb{Q};/)$ ni $(\mathbb{R};/)$.

d) Cualquiera de los conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$, con la operación binaria máximo, $a * b = \max(a,b)$, es un modelo de magma.

e) La interpretación $(\{33,77,99\},*)$, siendo $*$:

$$(\forall a,b \in \{33,77,99\})\,(a * b = \operatorname{mcd}(a,b))$$

no es un modelo de magma.

7.4. Semigrupo

Definición 7.10.-

Sea $(A;*)$ un magma. Se dice que $*$ es ***asociativa*** *en A, precisamente si:*

$$(\forall a,b,c \in A)\,((a * b) * c = a * (b * c))$$

en cuyo caso se dice que $(A;*)$ es un ***magma asociativo****.*

Definición 7.11.-

Se dice que $(A;*)$ es un ***semigrupo****, precisamente si es un magma asociativo.*

Teorema 7.1.-

Si $(A;*)$ es un semigrupo, entonces, el centro de A es parte estable de $(A;*)$.

Ejemplo 7.3.-

a) Las siguientes interpretaciones constituyen modelos de semigrupos: $(\mathbb{N};+)$, $(\mathbb{N};\cdot)$, $(\mathbb{Z};+)$, $(\mathbb{Z};\cdot)$, $(\mathbb{Q};+)$, $(\mathbb{Q};\cdot)$, $(\mathbb{R};+)$, $(\mathbb{R};\cdot)$.

b) Los magmas $(\mathbb{Z};-)$, $(\mathbb{Q};-)$ y $(\mathbb{R};-)$ no son semigrupos, pues $-$ no es asociativa en esos conjuntos (p. ej., $-4 = (1-2)-3 \neq 1-(2-3) = 2$). Tampoco son semigrupos los magmas $(\mathbb{Q}\setminus\{0\};/)$ y $(\mathbb{R}\setminus\{0\};/)$.

c) Cualquiera de los conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$, con la operación binaria máximo, $a * b = \max(a,b)$, es un modelo de semigrupo.

El elemento neutro en $\mathbb{N}$ para $\cdot$ es 1.

7.5. Monoide

Definición 7.12.-

Sean $(A;*)$ un magma y $e \in A$. Se dice que e es:

a) ***elemento neutro (unidad o identidad) por la izquierda*** *(en A para $*$), precisamente si $(\forall a \in A)\,(e * a = a)$;*

b) ***elemento neutro (unidad o identidad) por la derecha*** *(en A para $*$), precisamente si $(\forall a \in A)\,(a * e = a)$;*

c) ***elemento neutro, unidad o identidad*** *(en A para $*$), precisamente si lo es por la izquierda y por la derecha.*

Los elementos distintos del neutro suelen denominarse elementos no triviales*. Un magma (resp., semigrupo) con identidad se denomina* ***magma unitario*** *(resp.,* ***semigrupo unitario****).*

Definición 7.13.-

Se dice que $(A;*)$ es un ***monoide****, precisamente si es un semigrupo unitario.*

Teorema 7.2.-

Sean $(A;*)$ un monoide y $e \in A$ el elemento neutro para $*$. Se satisface que e es:

a) único: $(\forall e' \in A)((\forall a \in A)(e' * a = a * e' = a) \Rightarrow e = e')$;

b) idempotente: $e * e = e$.

Definición 7.14.-

Sea $(A;*)$ un magma unitario, con identidad $e \in A$ y sea $a \in A$. Se dice que a es:

a) ***simetrizable por la izquierda*** *(en A para $*$), precisamente si $(\exists b \in A)\,(b * a = e)$, denominándose a b, simétrico por la izquierda de a;*

b) ***simetrizable por la derecha*** *(en A para $*$), precisamente si $(\exists b \in A)\,(a * b = e)$, denominándose a b, simétrico por la derecha de a);*

c) ***simetrizable*** *(invertible o neutralizable) (en A para $*$), precisamente si lo es a la vez por la izquierda y por la derecha. En este caso, si $(\exists b \in A)\,(a * b = b * a = e)$, se dice que b es el* ***elemento inverso (simétrico o elemento neutralizador)*** *de a.*

Teorema 7.3.-

Si $(A;*)$ es un monoide, entonces, el simétrico de cualquier elemento simetrizable es único y el conjunto $Sim(A;*) \subseteq A$, de todos los elementos simetrizables de A, es parte estable de $(A;*)$.

Teorema 7.4.-

Sea $(A;*)$ un monoide. Si un elemento idempotente es simetrizable, entonces su simétrico también es idempotente.

Definición 7.15.-

Sean $(A;*)$ un monoide y $c \in A$. Se dice que c es:

a) ***regular o simplificable por la izquierda*** *(en A para $*$), precisamente si $(\forall a,b \in A)\,(c * a = c * b \Rightarrow a = b)$;*

b) ***regular o simplificable por la derecha*** *(en A para $*$), precisamente si $(\forall a,b \in A)\,(a * c = b * c \Rightarrow a = b)$;*

c) ***regular o simplificable*** *de $*$ en A (en A para $*$), precisamente si lo es por la izquierda y por la derecha.*

Teorema 7.5.-

En un monoide se satisface que el elemento neutro es regular y que todo elemento simetrizable es regular.

Ejemplo 7.4.-

a) Los magmas $(\mathbb{Z};-)$, $(\mathbb{Q};-)$ y $(\mathbb{R};-)$ tienen solo identidad por la derecha.

b) $(\mathbb{N};+)$, $(\mathbb{N};\cdot)$, $(\mathbb{Z};+)$, $(\mathbb{Z};\cdot)$, $(\mathbb{Q};+)$, $(\mathbb{Q};\cdot)$, $(\mathbb{R};+)$ y $(\mathbb{R};\cdot)$ son monoides conmutativos, cuyos elementos neutros son 0, 1, 0, 1, 0, 1, 0 y 1, respectivamente.

c) En $(\mathbb{N};+)$, el único elemento simetrizable es 0. En $(\mathbb{N};\cdot)$, el único elemento simetrizable es 1. En $(\mathbb{Z};+)$, $(\mathbb{Q};+)$, $(\mathbb{R};+)$, $(\mathbb{Q}\setminus\{0\};\cdot)$ y $(\mathbb{R}\setminus\{0\};\cdot)$, todos los elementos son simetrizables. En $(\mathbb{Z};\cdot)$ los únicos elementos simetrizables son 1 y -1.

d) En $(\mathbb{N};+)$, $(\mathbb{Z};+)$, $(\mathbb{Q};+)$, $(\mathbb{R};+)$, $(\mathbb{N}\setminus\{0\};\cdot)$, $(\mathbb{Z}\setminus\{0\};\cdot)$, $(\mathbb{Q}\setminus\{0\};\cdot)$ y $(\mathbb{R}\setminus\{0\};\cdot)$, todo elemento es regular.

7.6. Grupo

Definición 7.16.-

Un monoide $(A;*)$, se dice que es un ***grupo****, precisamente si todo elemento es simetrizable, esto es, precisamente si existe el inverso de cualquier elemento:*

$$(\forall a \in A)\,(\exists b \in A)\,(a * b = b * a = e)$$

Teorema 7.6.-

El elemento neutro de un grupo es único.

Teorema 7.7.-

Todo elemento de un grupo tiene un único inverso. Dicho único inverso de a suele representarse por a'.

Observación 7.3.-

Si la operación fuese conmutativa *—$\forall a, b \in A,\ a * b = b * a$— entonces se diría de la estructura $(A; *)$ que es* ***conmutativa o abeliana****. En este caso, es frecuente representar la operación por el símbolo $+$ (aditivamente). En este caso, suele representarse el neutro por 0 y el inverso de un elemento a por $-a$. El inverso aditivo de un elemento suele denominarse su* ***opuesto****. Si la operación se representa por $\cdot$ (multiplicativamente), entonces el neutro se representa por 1 y el inverso de un elemento a por a^{-1}. El inverso multiplicativo de un elemento suele denominarse su* ***recíproco****.*

Ejemplo 7.5.-

a) $(\mathbb{N}; +)$ *y* $(\mathbb{N}; \cdot)$ *no son grupos.*

b) $(\mathbb{Z}; +)$ *es grupo conmutativo;* $(\mathbb{Z}; \cdot)$ *no es grupo.*

c) $(\mathbb{Q}; \cdot)$ *no es grupo (0 no es simetrizable).* $(\mathbb{Q}; +)$ *y* $(\mathbb{Q}\setminus\{0\}; \cdot)$ *son grupos conmutativos.*

d) $(\mathbb{R}; \cdot)$ *no es grupo (0 no es simetrizable).* $(\mathbb{R}; +)$ *y* $(\mathbb{R}\setminus\{0\}; \cdot)$ *son grupos conmutativos.*

Teorema 7.8 (Algunas propiedades).-

Sean $(G; *)$ un grupo. Entonces, se satisface:

a) $(\forall a, b \in G)((a * b)' = b' * a')$

b) $(\forall a \in G)((a')' = a)$

7.6.1. Subgrupo

Definición 7.17.-

Sean $(G; *)$ un grupo y $S \subseteq G$. Se dice que $(S; *)$ es un ***subgrupo*** *del grupo $(G; *)$, precisamente si $(S; *)$ tiene estructura de grupo.*

Teorema 7.9 (Caracterización de subgrupo).-

Sean $(G; *)$ un grupo y $S \subseteq A, S \neq \emptyset$. Entonces, $(S; *)$ es subgrupo de $(G; *)$, precisamente si:

$$(\forall x, y \in S)(x * y' \in S)$$

Definición 7.18.-

Dado un grupo $(G; *)$, se denominan ***subgrupos impropios*** *a $(G; *)$ y $(\{e\}; *)$ y* ***subgrupo propio*** *a cualquier otro.*

Definición 7.19.-

Sean $(G; *)$ un grupo, $(S; *)$ un subgrupo suyo y $a \in G$. Se denomina ***clase de G a la izquierda módulo S*** *al conjunto:*

$$aS = \{x \in G : (\forall s \in S)(x = a * s)\}$$

y ***clase de G a la derecha módulo S*** *al conjunto:*

$$Sa = \{x \in G : (\forall s \in S)(x = s * a)\}$$

Definición 7.20.-

Sean $(G; *)$ un grupo $(S; *)$ un subgrupo suyo. Se dice que $(S; *)$ es un ***subgrupo normal o invariante*** *precisamente si:*

$$(\forall a \in G)(aS = Sa)$$

Definición 7.21.-

Se denomina ***grupo finito*** *a cualquier grupo que conste de un número finito de elementos.*

Definición 7.22.-

Se denomina ***orden de un grupo*** *al número de elementos del grupo.*

Definición 7.23.-

Sean $(G; *)$ un grupo y $a \in G$. Se denomina ***orden (finito) del elemento*** *a al menor $n \in \mathbb{N}$ tal que:*

$$(\overbrace{a * \cdots * a}^{n} = e)$$

Si no existe tal $n \in \mathbb{N}$ para $a \in G$, se dice que a es un ***elemento de orden infinito****.*

Teorema 7.10 (Teorema de Lagrange).-

El orden de un grupo finito es múltiplo del orden de cualquier subgrupo suyo.

Definición 7.24.-

Sean $(G; *)$ un grupo finito y $(S; *)$ un subgrupo suyo. Se denomina índice de S a:

$$\mathrm{i}(S) = \frac{\mathrm{o}(G)}{\mathrm{o}(S)}$$

Observación 7.4.-

Nótese que debido al teorema de Lagrange, el índice de cualquier subgrupo es un número natural.

Teorema 7.11.-

Sean $(G; *)$ un grupo finito y $(S; *)$ un subgrupo suyo. Entonces:

$$\mathrm{i}(S) = 2 \Rightarrow (S; *) \text{ es un subgrupo normal}$$

Definición 7.25.-

Sean $(G; *)$ un grupo y S un subconjunto finito de G. Se dice que $(G; *)$ es un ***grupo finitamente generado*** *por S precisamente si todo elemento de G puede obtenerse como resultado de la operación binaria sobre elementos de S o sobre elementos ya generados. Si S es de cardinal uno, se dice que $(G; *)$ es un* ***grupo monógeno****.*

Definición 7.26.-

Se dice que $(G; *)$ es un ***grupo cíclico*** *precisamente si es un grupo monógeno y finito.*

Teorema 7.12.-

Todo grupo cíclico es conmutativo.

Ejemplo 7.6.-

Sean la figura $\vee$ y el conjunto de rotaciones $R = \{R_0, R_{\pi/2}, R_\pi, R_{3\pi/2}\}$ en el plano euclideo E_2 (en sentido antihorario, el estándar en matemáticas). Estas rotaciones son un caso particular de transformaciones del plano euclideo, esto es, de aplicaciones $R : E_2 \to E_2$. Estas rotaciones, aplicadas a la figura $\vee$, originan las siguientes transformaciones isométricas por rotación de la misma (1ª columna) —si bien también mostramos las rotaciones sobre rotaciones (composición de rotaciones)—:

	$\vee$	$<$	$\wedge$	$>$
R_0	$\vee$	$<$	$\wedge$	$>$
$R_{\pi/2}$	$>$	$\vee$	$<$	$\wedge$
R_π	$\wedge$	$>$	$\vee$	$<$
$R_{3\pi/2}$	$<$	$\wedge$	$>$	$\vee$

Consideremos el conjunto $R = \{R_0, R_{\pi/2}, R_\pi, R_{3\pi/2}\}$ y la operación binaria $\circ$, composición de rotaciones sobre R. Se tiene que $(R; \circ)$ es un grupo cíclico de orden 4 que únicamente tiene un subgrupo propio.

Resolución. En efecto, tiene 4 elementos, luego, de ser grupo, es finito y ese es su orden. Veamos que es grupo. He aquí la *tabla de Cayley* de la operación $\circ$ sobre R:

$\circ$	R_0	$R_{\pi/2}$	R_π	$R_{3\pi/2}$
R_0	R_0	$R_{\pi/2}$	R_π	$R_{3\pi/2}$
$R_{\pi/2}$	$R_{\pi/2}$	R_π	$R_{3\pi/2}$	R_0
R_π	R_π	$R_{3\pi/2}$	R_0	$R_{\pi/2}$
$R_{3\pi/2}$	$R_{3\pi/2}$	R_0	$R_{\pi/2}$	R_π

a) $\circ$ es asociativa (podrían comprobarse todas las tríadas, pero también puede razonarse a partir de la asociatividad de la composición de aplicaciones, pues las rotaciones son aplicaciones)[5];

b) $\circ$ es conmutativa (la tabla es simétrica respecto de la diagonal principal \);

c) el elemento neutro para $\circ$ en R es R_0;

d) todo elemento es simetrizable —en la tabla, para una rotación determinada, solo hay que buscar qué otra rotación compuesta con ella da el neutro (p. ej., el inverso de $R_{\pi/2}$ es $R_{3\pi/2}$ porque $R_{\pi/2} \circ R_{3\pi/2} = R_{3\pi/2} \circ R_{\pi/2} = R_0$)—.

[5] Más adelante, se expresará la composición de rotaciones como producto de matrices, por lo que podrá razonarse también que la composición de rotaciones es asociativa por serlo el producto de matrices.

Además, es un grupo monógeno, esto es, generado por uno de sus elementos, concretamente tanto $R_{\pi/2}$ como $R_{3\pi/2}$ son capaces de generar todo el grupo. Por ejemplo:

$$R_{\pi/2} \circ R_{\pi/2} = R_\pi$$
$$R_{\pi/2} \circ R_\pi = R_{3\pi/2}$$
$$R_{\pi/2} \circ R_{3\pi/2} = R_0$$

Por tanto, es un grupo cíclico de orden 4.

$R = \{R_0, R_{\pi/2}, R_\pi, R_{3\pi/2}\}$ y $\{R_0\}$ son subgrupos impropios. El único subgrupo propio es $S = \{R_0, R_\pi\}$ (no hay más subgrupos propios porque de contener cualquier subgrupo $(S', \circ)$ a $R_{\pi/2}$ o a $R_{3\pi/2}$, al ser estos generadores de $(R, \circ)$, todas las rotaciones de R estarían en S'.

El que $(S, \circ)$ sea un subgrupo de $(R, \circ)$ se deduce del teorema de caracterización de subgrupos —7.9—, ya que es cierto que $(\forall x, y \in S)(x * y' \in S)$, pues S solo tiene dos elementos, R_0 y R_π, siendo ambas sus propios inversos, $R_0^{-1} = R_0$ y $R_\pi^{-1} = R_\pi$, así que:

x	y	y'	$x * y'$
R_0	R_π	R_π	$R_0 \circ R_\pi = R_\pi$
R_π	R_0	R_0	$R_\pi \circ R_0 = R_\pi$

□

7.7. Semianillo

Definición 7.27.-
Sean $A \neq \emptyset$ y $\oplus$ y $\otimes$ dos operaciones binarias sobre A. Se dice que $\otimes$ es:

a) ***distributiva por la izquierda** respecto de $\oplus$, precisamente si $(\forall a, b, c \in A)(a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c))$;*
b) ***distributiva por la derecha** respecto de $\oplus$, precisamente si $(\forall a, b, c \in A)((a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c))$;*
c) ***distributiva**, precisamente si es distributiva por la izquierda y por la derecha.*

Definición 7.28.-
*Sean $A \neq \emptyset$ y $\oplus$ y $\otimes$ dos operaciones binarias sobre A. Se dice que $(A; \oplus, \otimes)$ tiene estructura de **semianillo**, precisamente si $(A; \oplus)$ es monoide abeliano, $(A; \otimes)$ es semigrupo y $\otimes$ es distributiva respecto a $\oplus$.*

Definición 7.29.-
*Se dice que un semianillo $(A; \oplus, \otimes)$, es un **semianillo abeliano o conmutativo**, precisamente si $\otimes$ es conmutativa, es decir, precisamente si:*

$$(\forall a, b, c \in A)(a \otimes b = b \otimes a)$$

Definición 7.30.-
*Un semianillo $(A; \oplus, \otimes)$ se dice que es un **semianillo unitario**, precisamente si $(A; \otimes)$ es monoide.*

Ejemplo 7.7.-
Las estructuras $(\mathbb{N}; +, \cdot)$, $(\mathbb{Z}; +, \cdot)$, $(\mathbb{Q}; +, \cdot)$ y $(\mathbb{R}; +, \cdot)$, con $+$ y $\cdot$ la suma y producto habituales, son semianillos conmutativos y unitarios.

7.8. Anillo

Definición 7.31.-
*Un semianillo $(A; \oplus, \otimes)$ se dice que es un **anillo**, precisamente si $(A; \oplus)$ es grupo abeliano.*

*Dicho de otro modo, si A es un conjunto no vacío y $\oplus$ y $\otimes$ dos operaciones binarias en A, se dice que la terna $(A; \oplus, \otimes)$ es un **anillo** si se satisface:*

a) *$(A; \oplus)$ es grupo abeliano;*
b) *$(A; \otimes)$ es un semigrupo;*
c) *$\otimes$ es distributiva con respecto a $\oplus$, esto es, $\forall x, y, z \in A$:*

$$x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$$
$$\wedge$$
$$(x \oplus y) \otimes z = (x \otimes z) \oplus (y \otimes z)$$

Teorema 7.13.-
En un anillo $(A; \oplus, \otimes)$, el elemento neutro de $\oplus$ en A es un elemento singular o absorbente para $\otimes$ en A, esto es:

$$(\forall a \in A)(e_\oplus \otimes a = a \otimes e_\oplus = e_\oplus)$$

Definición 7.32.-
*En un anillo $(A; \oplus, \otimes)$, puede definirse una nueva operación binaria, la **sustracción o diferencia**, que notaremos $\ominus$, como:*

$$a \ominus b = a \oplus (-b)$$

donde $-b$ es el elemento opuesto de b.

Definición 7.33.-
*Un anillo $(A; \oplus, \otimes)$ se dice que es un **anillo unitario**, precisamente si $(A; \otimes)$ es un monoide.*

Observación 7.5.-
En un anillo, el elemento neutro aditivo *$e_\oplus$ suele notarse por* 0. *En un anillo unitario, el* elemento neutro multiplicativo *$e_\otimes$ suele notarse por* 1.

Definición 7.34.-
*Sean $(A; \oplus, \otimes)$ un anillo y $a \in A$. Se dice que a es **nilpotente** precisamente si:*

$$(\exists n \in \mathbb{N}^+)(a \otimes \overset{n}{\cdots} \otimes a = 0)$$

Definición 7.35.-
*Si $(A; \oplus, \otimes)$ es un anillo unitario, entonces puede que existan elementos que tengan inversos multiplicativos, esto es, elementos $a \in A$ para los que exista un $b \in A$ tal que $a \otimes b = b \otimes a = 1$. Estos elementos del anillo que tienen inverso multiplicativo se denominan **unidades** del anillo.*

Ejemplo 7.8.-
$(\mathbb{Z}; +, \cdot)$, $(\mathbb{Q}; +, \cdot)$ y $(\mathbb{R}; +, \cdot)$, con $+$ y $\cdot$ la suma y producto habituales, son anillos conmutativos y unitarios.

7.8.1. Subanillo

Definición 7.36.-
*Sean $(A; \oplus, \otimes)$ un anillo y $S \subseteq A$. Se dice que $(S; \oplus, \otimes)$ es un **subanillo** del anillo $(A; \oplus, \otimes)$, precisamente si $(S; \oplus, \otimes)$ es anillo.*

Teorema 7.14 (Caracterización de subanillo).-
Sean $(A; \oplus, \otimes)$ un anillo y $S \subseteq A, S \neq \emptyset$. Entonces, $(S; \oplus, \otimes)$ es subanillo de $(A; \oplus, \otimes)$, precisamente si:

$$(\forall x, y \in S)(x \oplus (-y) \in S)$$
$$\wedge$$
$$(\forall x, y \in S)(x \otimes y \in S)$$

Ejemplo 7.9.-
Con $+$ y $\cdot$ la suma y producto habituales, $(\mathbb{Z}; +, \cdot)$ es subanillo de $(\mathbb{Q}; +, \cdot)$ y de $(\mathbb{R}; +, \cdot)$ y $(\mathbb{Q}; +, \cdot)$ es subanillo de $(\mathbb{R}; +, \cdot)$.

7.8.2. Ideal

Definición 7.37.-
Sea $(A; \oplus, \otimes)$ un anillo. Se dice que un subgrupo $(I; \oplus)$ de $(A; \oplus)$ es un:

a) ***ideal por la izquierda** de $(A; \oplus)$, precisamente si $\forall x \in I$, $\forall a \in A$, $a \otimes x \in I$;*
b) ***ideal por la derecha** de $(A; \oplus)$, precisamente si $\forall x \in I$, $\forall a \in A$, $x \otimes a \in I$;*
c) ***ideal**, precisamente si es un ideal por la izquierda y por la derecha.*

Definición 7.38.-
*Se dice que el ideal I es un **ideal propio** precisamente si $I \neq \{0\}$ e $I \neq A$.*

7.9. Semianillo o anillo íntegro o de integridad

Definición 7.39.-
Sean $(A; \oplus, \otimes)$ un semianillo y $x \in A$. Se dice que x es:

a) ***divisor de cero por la izquierda**, precisamente si $\exists y \neq 0, x \otimes y = 0$;*
b) *que x es **divisor de cero por la derecha**, precisamente si $\exists y \neq 0, y \otimes x = 0$;*
c) ***divisor de cero**, precisamente si es divisor de cero por la izquierda y por la derecha.*

Definición 7.40.-

Un semianillo (resp., anillo) $(A;\oplus,\otimes)$, se dice que es un ***semianillo (resp, anillo) íntegro o de integridad****, precisamente si no tiene divisores de cero, esto es, precisamente si:*

$$(\forall x,y\in A)(x\otimes y=0\Rightarrow x=0\vee y=0))$$

Ejemplo 7.10.-

Siendo $+$ y $\cdot$ la suma y producto habituales, $(\mathbb{N};+,\cdot)$ es un semianillo conmutativo, unitario e íntegro y $(\mathbb{Z};+,\cdot)$, $(\mathbb{Q};+,\cdot)$ y $(\mathbb{R};+,\cdot)$, son anillos conmutativos, unitarios e íntegros, es decir, si A denota cualquiera de ellos:

$$(\forall x,y\in A)(xy=0\Rightarrow x=0\vee y=0))$$

7.10. Dominio de integridad

Definición 7.41.-

Un anillo de integridad $(A;\oplus,\otimes)$, se dice que es un ***dominio de integridad****, precisamente si $(A;\otimes)$ es monoide abeliano, esto es, precisamente si es un anillo conmutativo, unitario y sin divisores de cero.*

Ejemplo 7.11.-

$(\mathbb{Z};+,\cdot)$, $(\mathbb{Q};+,\cdot)$ y $(\mathbb{R};+,\cdot)$, con $+$ y $\cdot$ la suma y producto habituales, son dominios de integridad —esto es, lo que habíamos dicho en el ejemplo 7.10, que son anillos conmutativos, unitarios e íntegros—.

7.11. Cuerpo

Definición 7.42.-

Un anillo unitario $(A;\oplus,\otimes)$, se dice que es un ***cuerpo****, precisamente si $(A\setminus\{0\};\otimes)$ es grupo.*

Dicho de otro modo, si A es un conjunto no vacío y $\oplus$ y $\otimes$ dos operaciones en A, se dice que la terna $(A;\oplus,\otimes)$ es un ***cuerpo*** *si se satisface:*

a) $(A;\oplus)$ es un grupo abeliano con elemento neutro e;
b) $(A\setminus\{0\};\otimes)$ es un grupo;
c) $\otimes$ es distributiva con respecto a $\oplus$: $\forall x,y,z\in A$, $x\otimes(y\oplus z)=(x\otimes y)\oplus(x\otimes z)$.

Decir que un cuerpo es abeliano o ***conmutativo*** *equivale a decir que $\otimes$ satisface la conmutativa.*

Ejemplo 7.12.-

$(\mathbb{Q};+,\cdot)$ y $(\mathbb{R};+,\cdot)$, con $+$ y $\cdot$ la suma y producto habituales, son cuerpos conmutativos[6]*.*

Teorema 7.15.-

Cualquier cuerpo y cualquier anillo unitario contenido en un cuerpo, son dominios de integridad.

7.11.1. Subcuerpo

Definición 7.43.-

Sean $(K;\oplus,\otimes)$ un cuerpo y $S\subseteq K$. Se dice que $(S;\oplus,\otimes)$ es un ***subcuerpo*** *del cuerpo $(K;\oplus,\otimes)$, precisamente si $(S;\oplus,\otimes)$ es cuerpo.*

Teorema 7.16 (Caracterización de subcuerpo).-

Sean $(K;\oplus,\otimes)$ un cuerpo y $S\subseteq K, S\neq\emptyset$. Entonces, $(S;\oplus,\otimes)$ es subcuerpo de $(K;\oplus,\otimes)$, precisamente si:

$$(\forall x,y\in S)(x\oplus(-y)\in S)$$
$$\wedge$$
$$(\forall x,y\in S\setminus\{0\})(x\otimes y^{-1}\in S\setminus\{0\}$$

7.11.2. Característica de un cuerpo

Definición 7.44.-

Se dice que $(\mathbb{K};\oplus,\otimes)$ es un ***cuerpo de característica*** *$p\in\mathbb{N}$ si p es el menor natural tal que $1\oplus\overset{p}{\cdots}\cdot\oplus 1=0$. Si no existe tal p se dice que el cuerpo tiene característica 0.*

Ejemplo 7.13.-

$(\mathbb{Q};+,\cdot)$ y $(\mathbb{R};+,\cdot)$, con $+$ y $\cdot$ la suma y producto habituales, son cuerpos de característica 0.

7.11.3. Cuerpo de cocientes de un dominio de integridad

Cualquier dominio de integridad puede ser encajado en un cuerpo, vía la estructura del cuerpo de cocientes, que precisamente resulta ser el cuerpo más pequeño que lo embebe.

Sea $(A;\oplus,\otimes)$ un dominio de integridad. En $A\times A^*$ se considera la relación:

$$(\forall(a,b),(c,d)\in A\times A^*)((a,b)E(c,d)\Leftrightarrow a\cdot d=b\cdot c)$$

que es de equivalencia.

Suele notarse $Q(A)$ el conjunto cociente:

$$Q(A)=A\times A^*/E$$

y $\frac{a}{b}$ la clase de equivalencia $[(a,b)]$.

Las operaciones binarias en $Q(A)$, se definen en función de las del dominio de integridad $(A;\oplus,\otimes)$: $\forall[(a,b)],[(c,d)]\in Q(A)$,

$$[(a,b)]\boxplus[(c,d)]=[(a\otimes d\oplus b\otimes c,b\otimes d)]$$
$$[(a,b)]\boxtimes[(c,d)]=[(a\otimes c,b\otimes d)]$$

Se demuestra que $(Q(A);\boxplus,\boxtimes)$ tiene estructura de cuerpo.

7.12. Homomorfismos

Definición 7.45.-

Dados dos magmas $(X;*)$ e $(Y;\circ)$, se dice que una aplicación $f:X\to Y$ es:

a) un ***homomorfismo****, precisamente si $\forall x,y\in X, f(x*y)=f(x)\circ f(y)$;*
b) ***monomorfismo****, precisamente si f es inyectiva;*
c) ***epimorfismo****, precisamente si f es sobreyectiva;*
d) ***isomorfismo****, precisamente si f es biyectiva;*
e) ***endomorfismo****, precisamente si $X=Y\wedge *\equiv\circ$;*
f) ***automorfismo****, precisamente si f es endomorfismo e isomorfismo.*

Teorema 7.17.-

Sean $(X;*)$ e $(Y;\circ)$ dos magmas y $f:X\to Y$ un homomorfismo. Entonces, $\forall x\in X$ se satisface que:

a) e es el neutro de $(X;*)\Rightarrow f(e)$ es el neutro de $(Y;\circ)$.
b) x' es el simétrico de x para $*\Rightarrow f(x')$ es el simétrico de $f(x)$ para $\circ$
c) f se descompone canónicamente como aplicación que es.

Teorema 7.18.-

La composición de homomorfismos es un homomorfismo.

Teorema 7.19.-

Dados dos magmas $(X;*)$ e $(Y;\circ)$ y $f:X\to Y$ un homomorfismo, se satisface que $f(X)=\{y\in Y:\exists x\in X, f(x)=y\}$ es parte estable *de $(Y;\circ)$.*

Definición 7.46.-

A la estructura algebraica $(f(X);\circ)$, se la denomina ***imagen homomorfa*** *de $(X;*)$.*

7.12.1. Homomorfismo de grupos

Definición 7.47.-

Sean $(G_1;*)$ y $(G_2;\circ)$ dos grupos y $f:G_1\to G_2$ una aplicación. Se dice que f es un ***homomorfismo de grupos****, precisamente si lo es como homomorfismo de magmas, esto es, precisamente si $\forall a,b\in G_1$ se satisface:*

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

Definición 7.48.-

Sean $(G_1;*)$ y $(G_2;\circ)$ dos grupos y $f:G_1\to G_2$ un homomorfismo de grupos. Se denomina ***núcleo de f****, representándose por $\ker f$, al conjunto:*

$$\ker f=\{x\in G_1:f(x)=e_\circ\}$$

Teorema 7.20.-

Sean $(G_1;*)$ y $(G_2;\circ)$ dos grupos y $f:G_1\to G_2$ un homomorfismo de grupos. Entonces, $\forall a\in G_1$ se satisface que:

a) e es el neutro de $(G_1;*)\Rightarrow f(e)$ es el neutro de $(G_2;\circ)$.

[6] En realidad, se puede demostrar que $(\mathbb{Q};+,\cdot)$ es el menor cuerpo que extiende al anillo $(\mathbb{Z};+,\cdot)$, estando determinado únicamente salvo isomorfismo. De manera similar, puede completarse cualquier anillo de integridad —generando su cuerpo de cocientes (*vid. infra* §7.11.3)—.

b) x' es el simétrico de x para $*$ $\Rightarrow$ $f(x')$ es el simétrico de $f(x)$ para $\circ$.
c) $(f(G_1);\circ)$ es grupo.
d) f es monomorfismo $\Leftrightarrow \ker f = \{e\}$.

7.12.2. Homomorfismo de anillos

Definición 7.49.-
*Sean $(A_1;\oplus,\otimes)$ y $(A_2;\boxplus,\boxtimes)$ dos anillos y $f : A_1 \to A_2$ una aplicación. Se dice que f es un **homomorfismo de anillos**, precisamente si $\forall a, b \in A_1$ se satisfacen:*

$$f(a \oplus b) = f(a) \boxplus f(b)$$
$$f(a \otimes b) = f(a) \boxtimes f(b)$$

Teorema 7.21.-
Sean $(A_1;\oplus,\otimes)$ y $(A_2;\boxplus,\boxtimes)$ dos anillos y $f : A_1 \to A_2$ un homomorfismo de anillos. Se satisface que toda imagen (resp., contraimagen) de un subanillo de A_1 (resp., A_2) es un subanillo de A_2 (resp., A_1).

Definición 7.50.-
*Sean $(A_1;\oplus,\otimes)$ y $(A_2;\boxplus,\boxtimes)$ dos anillos y $f : A_1 \to A_2$ un homomorfismo de anillos. Se denomina **núcleo de f**, representándose por $\ker f$, al subconjunto de A_1:*

$$\ker f = \{x \in A_1 : f(x) = e_{\boxplus}\}$$

*Se denomina **imagen** de f, representándose por $\operatorname{im} f$ (o por $f(A_1)$) al subconjunto de A_2:*

$$\operatorname{im} f = \{y \in A_2 : \exists x \in A_1, f(x) = y\}$$

Teorema 7.22.-
Sean $(A_1;\oplus,\otimes)$ y $(A_2;\boxplus,\boxtimes)$ dos anillos y $f : A_1 \to A_2$ un homomorfismo de anillos. Se satisface que $\ker f$ es un ideal de $(A_1;\oplus,\otimes)$ y que $\operatorname{im} f$ es un subanillo de $(A_2;\boxplus,\boxtimes)$.

Teorema 7.23.-
Sean $(A_1;\oplus,\otimes)$ y $(A_2;\boxplus,\boxtimes)$ dos anillos. Se satisface:
a) $f : A_1 \to A_2$ es monomorfismo $\Leftrightarrow \ker f = \{e_{\oplus}\}$;
b) $f : A_1 \to A_2$ es epimorfismo $\Leftrightarrow \operatorname{im} f = A_2$.

7.12.3. Homomorfismo de cuerpos

Definición 7.51.-
*Sean $(K_1;\oplus,\otimes)$ y $(K_2;\boxplus,\boxtimes)$ dos cuerpos y $f : K_1 \to K_2$ una aplicación. Se dice que f es un **homomorfismo de cuerpos**, precisamente si lo es como homomorfismo de anillos.*

7.13. Ejercicios

7.1.- *Considérese como figura el trípode —tres segmentos a 90, 210 y 330 grados ($\pi/2$, $7\pi/6$ y $11\pi/6$ radianes, respectivamente)—, el conjunto de rotaciones $R = \{R_0, R_{2\pi/3}, R_{4\pi/3}\}$ (esto es, de 0, 120 y 240 grados) y, representando por $F_{y=ax+b}$ la reflexión de eje la recta $y = ax + b$, el conjunto de reflexiones $F = \left\{F_{x=0}, F_{x=y\sqrt{3}}, F_{x=-y\sqrt{3}}\right\}$ (esto es, el conjunto de reflexiones según sus tres segmentos). Considérese la operación binaria $\circ$, composición de transformaciones (rotaciones o reflexiones) sobre $R \cup F$. Demuéstrese* —vid. supra *ejemplo 7.6— que $(R \cup F;\circ)$ es un grupo y estúdiese. Obsérvese, por ejemplo, que el trípode presenta simetría axial (especular) para cada uno de sus segmentos considerados como ejes de simetría:*

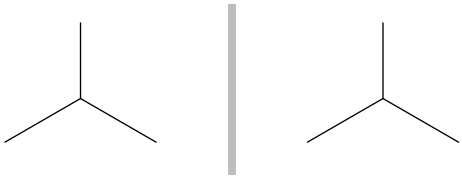

Imagen Espejo Trípode

7.2.- ...
Resolución. □

Nombres propios

► ...
Más nombres propios y biografías, en:
◦ ...
◦ John J. O'Connor y Edmund F. Robertson (2014): «The MacTutor History of Mathematics archive», http://turnbull.mcs.st-and.ac.uk/history/, [último acceso: 25 de abril de 2014]. © gratisOA.
◦ Edward N. Zalta (2014): «Stanford Encyclopedia of Philosophy», http://plato.stanford.edu/, [último acceso: 25 de abril de 2014]. © gratisOA.
◦ ...

Para saber más

- Ernesto de Jesús Alcañiz. *Teoría de grupos aplicada a la simetría*. Disponible en: http://www2.uah.es/edejesus/resumenes/DECI/tema_1.pdf
- Colaboradores de Wikipedia (2014): «Álgebra de Boole», http://es.wikipedia.org/wiki/Álgebra_de_Boole, [último acceso: 25 de abril de 2014]. © CC BY-SA 3.0 Unported.
- Colaboradores de Wikipedia (2014): «Euclidean plane isometry», http://en.wikipedia.org/wiki/Euclidean_plane_isometry, [último acceso: 25 de abril de 2014]. © CC BY-SA 3.0 Unported.
- Colaboradores de Wikipedia (2014): «Grupo diedral», http://es.wikipedia.org/wiki/Grupo_diedral, [último acceso: 25 de abril de 2014]. © CC BY-SA 3.0 Unported.
- Colaboradores de Wikipedia (2014): «Retículo (orden)», http://es.wikipedia.org/wiki/Retículo_(orden), [último acceso: 25 de abril de 2014]. © CC BY-SA 3.0 Unported.
- Springer y EMS (2014): *Encyclopedia of Mathematics*, http://www.encyclopediaofmath.org, [último acceso: 25 de abril de 2014]. © CC BY-SA 3.0 Unported.
- ...

Más bibliografía en:
◦ ...
◦ Juanmiguel León-Rojas (2014): «Álgebra Lineal para la Edificación», http://cala.unex.es/cala/cala/course/view.php?id=289#section-1, [último acceso: 25 de abril de 2014]. © CGL, CC0, CC BY.
◦ ...

Apéndice: Lo básico en GNU Octave

- ...
- Juanmiguel León-Rojas (2014): «Prácticas con Software (P. 1.1: Introducción a GNU OCtave - MatLab) (Notas incompletas de clase)», http://cala.unex.es/cala/cala/file.php/289/08-Practicas-con-software/08-Practicas-con-software-Parte-01-01.pdf, [último acceso: 25 de abril de 2014]. © CGL, CC0, CC BY.
- Juanmiguel León-Rojas (2014): «Prácticas con Software (P. 1.2: Estructuras de control de flujo. Programas y funciones) (Notas incompletas de clase)», http://cala.unex.es/cala/cala/file.php/289/08-Practicas-con-software/08-Practicas-con-software-Parte-01-02.pdf, [último acceso: 25 de abril de 2014]. © CGL, CC0, CC BY.
- Juanmiguel León-Rojas (2014): «Prácticas con Software (P. 1.3: Iteración y Recursión) (Notas incompletas de clase)», http://cala.unex.es/cala/cala/file.php/289/08-Practicas-con-software/08-Practicas-con-software-Parte-01-03.pdf, [último acceso: 25 de abril de 2014]. © CGL, CC0, CC BY.
- ...