22202 Álgebra I – Ayudantía 10

Estructura de Grupo

Viernes 15 de Enero de 2021

10.1. Operación Binaria

- Sean A, B, C conjuntos no vacío. Se define una **Operación Binaria** o **Ley de Composición** como una función:

$$* : A \times B \longrightarrow C \ , \ (a, b) \mapsto c$$

- En este caso, podemos escribir: $a * b = c$ (notación operativa) o bien $*(a, b) = c$ (notación funcional). Para este Curso, se hará de la primera forma.

- En particular, cuando la operación se define como:

$$* : A \times A \longrightarrow A \ , \ (a, b) \mapsto c$$

  se dice que la operación es **cerrada** en A, o bien que se trata de una **Ley de Composición Interna** si se cumple que:

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

  A primera vista, esta definición parece ser redundante (pues $c = a * b$ y ya se sabe que $c \in A$), pero ayuda a entender bien cómo funcionan las operaciones.

- (Suma natural) $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, +(a, b) = a + b$. Ya sabemos que es cerrada (de toda la vida, aunque no sepamos cómo demostrarlo, por ahora).

- (Producto natural) $\bullet : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \bullet(a, b) = a \cdot b$. Ya sabemos que es cerrada (de toda la vida, aunque no sepamos cómo demostrarlo, por ahora).

- (Resta natural) $- : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, -(a, b) = a - b$. Ya sabemos que **NO es cerrada** (basta con $2 - 5 = -3 \notin \mathbb{N}$).

- Suma y producto enteros, suma y producto racionales, suma y producto reales, suma y producto complejos.

10.2. Relación entre $\mathbb{Z}$ y $\mathbb{Z}_n$

- ($n = 5$) Si recordamos la relación definida en $\mathbb{Z} \times \mathbb{Z}$ dada por $aRb \iff a - b = 5k, k \in \mathbb{Z}$, y recordando que es de equivalencia, vemos que:

  - $5 \ R \ 0$, pues $5 - 0 = 5 = 5 \cdot 1, 1 \in \mathbb{Z}$.
  - $10 \ R \ 0$, pues $10 - 0 = 10 = 5 \cdot 2, 2 \in \mathbb{Z}$.
  - $(-5) \ R \ 0$, pues $(-5) - 0 = -5 = 5 \cdot (-1), (-1) \in \mathbb{Z}$.

- En general, cualquier múltiplo de 5 estará relacionado con 0. Luego, podemos hablar de un subconjunto de $\mathbb{Z}$ que estará formado por todos aquellos números relacionados con el 0; es decir, la **clase de equivalencia** del 0 bajo la relación R:

$$\boxed{[0]_R = \overline{0}_5 = \{\ldots, -10, -5, 0, 5, 10, \ldots\}}$$

- De forma análoga, podemos agrupar a los demás números **según el resto que dejan al dividirlos por 5**. Así, vemos por ejemplo que $6\ R\ 1$, $(-1)\ R\ 4$, $13\ R\ 3$, $-8\ R\ 2$. Se obtendrán entonces las 4 clases que nos hacen falta:

$$\boxed{[1]_R = \overline{1}_5 = \{\ldots, -9, -4, 1, 6, 11, \ldots\}}$$
$$\boxed{[2]_R = \overline{2}_5 = \{\ldots, -8, -3, 2, 7, 12, \ldots\}}$$
$$\boxed{[3]_R = \overline{3}_5 = \{\ldots, -7, -2, 3, 8, 13, \ldots\}}$$
$$\boxed{[4]_R = \overline{4}_5 = \{\ldots, -6, -1, 4, 9, 14, \ldots\}}$$

- Como observaciones importantes, vemos que ***todo número entero está en alguna de estas 5 clases*** y que ***todo número entero está en una única clase (es decir, no se repiten en dos clases distintas).*** En lenguaje matemático, si $a, b = 0, 1, 2, 3, 4$, se tiene que $\forall a, b \in \{0, 1, 2, 3, 4\}(\overline{a}_5 \cap \overline{b}_5 = \varnothing)$ y que $\bigcup_a \overline{a}_5 = \mathbb{Z}$

- Cuando describimos al conjunto $\mathbb{Z}$ de esta manera, lo estamos dividiendo en 5 clases de equivalencia a partir de la relación "módulo 5". En tal caso, hablaremos del **conjunto cuociente** de $\mathbb{Z}$ bajo la relación R y lo llamaremos $\mathbb{Z}_5$.

- Observar que $\mathbb{Z}_5$ tiene 5 elementos: $\boxed{\mathbb{Z}_5 = \{\overline{0}_5; \overline{1}_5; \overline{2}_5; \overline{3}_5; \overline{4}_5; \}}$

- Finalmente, todo lo hecho aquí será válido para cualquier $n \in \mathbb{N}, n > 1$.

10.3. Suma y Producto en $\mathbb{Z}_n$

- $(n = 5)$ La **suma módulo 5** y el **producto módulo 5** se definen formalmente como:

$$\boxed{\overline{a}_5 +_5 \overline{b}_5 = \overline{(a+b)}_5} \qquad \text{y} \qquad \boxed{\overline{a}_5 \bullet_5 \overline{b}_5 = \overline{(a \cdot b)}_5}$$

- Evidentemente, estas definiciones son poco prácticas. Por ello, la definiremos "con palabras" como sigue: ***se suman (o se multiplican) los valores de la clase y al resultado se le calcula el resto de dividirlo por 5, siendo ese el resultado***.
  Ej: $\overline{2}_5 +_5 \overline{4}_5 = \overline{6}_5 = \overline{1}_5$. $\quad \overline{2}_5 \bullet_5 \overline{4}_5 = \overline{8}_5 = \overline{3}_5$.

- A partir de esta definición "con palabras" y como son solamente 5 clases, podemos hacer $5 \cdot 5 = 25$ sumas (y, respectivamente, 25 productos). Por ello, las podemos agrupar en una Tabla, donde por simplicidad anotamos solo el valor de la clase:

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\bullet_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

- Como última observación, vemos que ***ambas operaciones son cerradas*** en $\mathbb{Z}_5$.
- Nuevamente, todo lo hecho aquí será válido para cualquier $n \in \mathbb{N}, n > 1$.

10.4. Estructura de Grupo

- Dados un conjunto $G \neq \varnothing$ y $* : G \times G \longrightarrow G$ una operación binaria, se dice que $(G, *)$ tiene **estructura de grupo** si se cumple:
  1. $*$ es una **Ley de Composición Interna** (es cerrada en G).
  2. $*$ es **asociativa** en G: $\boxed{\forall a, b \in G \; [a * (b * c) = (a * b) * c]}$
  3. $*$ tiene **elemento neutro por la izquierda** en G: $\boxed{\exists e \in G : \forall a \in G (e * a = a)}$
  4. Existe **inverso por la izquierda** bajo $*$ en G: $\boxed{\forall a \in G \; \exists a' \in G : (a' * a = e)}$
- Veamos a continuación que el inverso por la derecha de a es también a' (es decir, verificaremos si $a * a' = e$). Para ello, sabemos que $a' * a = e$, por lo que ahora abusaremos del inverso por la izquierda de a' (es decir, $(a')' * (a') = e$):

$$a * a' = e * (a * a') = [(a')' * a'] * (a * a') = (a')' * [a' * a] * a' = (a')' * (e * a') = (a')' * (a') = e$$

- Ahora, veamos que el neutro por la derecha también debe ser e (es decir, probaremos que $a * e = a$):

$$a * e = a * (a' * a) = (a * a') * a = e * a = a$$

- Por lo tanto, acabamos de ver que ***el inverso de*** a ***es el mismo tanto por derecha como por izquierda*** y que ***el neutro de*** G ***es el mismo tanto por derecha como por izquierda***.
- Además, se puede demostrar que esos elementos (neutro e inverso de a) son únicos.

10.5. Ejercicios propuestos

1. Decida si la estructura $(G, *)$ es un grupo. Si no lo es, diga cuál de las propiedades de grupo no se cumple:
   a. $G = \mathbb{Z}$ tal que $a * b = a \cdot b$ (producto usual en $\mathbb{Z}$)
   b. $G = \mathbb{Z}$ tal que $a * b = a - b$ (resta usual en $\mathbb{Z}$)
   c. $G = \mathbb{N}$ tal que $a * b = a^b$ (potencia con base y exponente en $\mathbb{N}$)
   d. $G = \mathbb{Z}_4$ tal que $a * b = \overline{a} \bullet_4 \overline{b}$ (producto módulo 4)

2. Decidir si $(\mathbb{Z}_5, +_5)$ es grupo.
3. Decidir si $(\mathbb{Z}_5, \bullet_5)$ es grupo.
4. Decidir si $(\mathbb{Z}_5 - \{0_5\}, \bullet_5)$ es grupo.
5. Completar tablas para la suma y el producto en $\mathbb{Z}_n$, con $n = 2, 3, 4, 6$ y decidir si es grupo, de forma similar a los ejercicios previos.