MA1101-3 Introducción al Álgebra
Profesor: Pablo Dartnell R.
Auxiliar: Felipe Atenas M.

Resumen Control 5

A continuación se presenta un resumen de los contenidos del control 5 del curso Introducción al Álgebra. Ojo que es un resumen, por lo que puede no contener todo lo necesario para el control, pero sí lo esencial. Mi consejo es que ustedes mismos elaboren su propio resumen, porque son ustedes mismos los que saben qué cosas manejan bien y las que no manejan tan bien. Consideraremos que A es un conjunto no vacío.

Estructuras Algebraicas

1. Ley de composición interna (l.c.i.): es una función

$$\begin{aligned} * : A \times A &\to A \\ (x, y) &\mapsto x * y \end{aligned}$$

   En simples palabras, es una operación que deja el resultado en el conjunto original.

2. Estructura algebraica: si $*$ es una lci definida en A, al par $(A, *)$ se le denomina estructura algebraica. También se puede definir una segunda operación $\triangle$ y consideramos la estructura algebraica con ambas operaciones, $(A, *, \triangle)$.

3. Propiedades básicas: diremos que

   - $*$ es asociativa si $(\forall x, y, z \in A)\ (x * y) * z = x * (y * z)$
   - $e \in A$ es elemento neutro para $*$ si $(\forall x \in A)\ e * x = x * e = x$
   - $x \in A$ tiene inverso, cuando $e \in A$ es elemento neutro para $*$, si existe $y \in A$ tal que $x * y = y * x = e$. En tal caso, y es un inverso de x y viceversa.
   - $*$ es conmutativa si $(\forall x, y \in A)\ x * y = y * x$
   - un elemento $a \in A$ será un elemento absorvente si $(\forall x \in A)\ x * a = a * x = a$
   - un elemento $a \in A$ será un elemento idempotente si $a * a = a$
   - un elemento $x \in A$ es cancelable, si para $y, z \in A$ se tiene que

$$x * y = x * z \Rightarrow y = z$$
$$y * x = z * x \Rightarrow y = z$$

   - $\triangle$ distribuye con respecto a $*$, cuando $(A, *, \triangle)$ es una estr. algbr., si

$$(\forall x, y, z \in A)\ x \triangle (y * z) = (x \triangle y) * (x \triangle z)$$
$$(\forall x, y, z \in A)\ (y * z) \triangle x = (y \triangle x) * (z \triangle x)$$

4. Unicidad del neutro: una estructura $(A, *)$ posee a lo más un elemento neutro (podría no tener neutro).

5. Propiedad: si la estr. algbr. $(A, *)$ tiene neutro e y $*$ asociativa, entonces los inversos son únicos (si es que existen). En este caso, al inverso de x lo denotamos x^{-1}.

6. Propiedades: sea $(A, *)$ una estr. algbr. asociativa y con neutro $e \in A$. Entonces se cumple:

   - Si $x \in A$ posee inverso, entonces x^{-1} también. De hecho, $(x^{-1})^{-1} = x$.
   - Si $x, y \in A$ poseen inversos, entonces $x * y$ también posee inverso y $(x * y)^{-1} = y^{-1} * x^{-1}$.
   - Si $x \in A$ posee inverso, entonces es cancelable.

7. La estructura $\mathbb{Z}_n$: se definen las operaciones suma $+_n$ y producto $\cdot_n$ de la siguiente manera:
$$[x]_n +_n [y]_n = [x+y]_n$$
$$[x]_n \cdot_n [y]_n = [x \cdot y]_n$$

8. Prop.: Sean $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ tales que $x_1 \equiv_n x_2$ y $y_1 \equiv_n y_2$. Entonces se tiene que
$$(x_1 + y_1) \equiv_n (x_2 + y_2) \ \wedge \ (x_1 \cdot y_1) \equiv_n (x_2 \cdot y_2)$$
Con esto, si $[x_1]_n = [x_2]_n$ y $[y_1]_n = [y_2]_n$, entonces
$$[x_1 + y_1]_n = [x_2 + y_2]_n \ \wedge \ [x_1 \cdot y_1]_n = [x_2 \cdot y_2]_n$$

Grupos

1. Grupo: Sea $(G, *)$ una estr. algbr.. Diremos que es un grupo si:
   - $*$ es asociativa
   - $(G, *)$ posee neutro $e \in G$
   - Todo elemento $x \in G$ posee inverso $x^{-1} \in G$

   Si además $*$ es conmutativa, llamamos a $(G, *)$ grupo abeliano.

2. Propiedades: Dado $(G, *)$ grupo, se tiene que:
   - Para todo $a, b \in G$, las ecuaciones $a * x_1 = b$ y $x_2 * a = b$ tienen solución única cada una: $x_1 = a^{-1} * b$ y $x_2 = b * a^{-1}$.
   - El único elemento idempotente de G es su neutro.

3. Subgrupos: Sea $(G, *)$ un grupo y sea $H \subseteq G$, $H \neq \emptyset$. Diremos que H es subgrupo de G si $(H, *)$ es también grupo. Notar acá que los neutros en G y H coinciden, ya que $H \subseteq G$. Lo mismo vale para los inversos.

4. Subgrupos triviales del grupo $(G, *)$: $(G, *)$ y $(\{e\}, *)$ (donde $e \in G$ es el neutro).

5. Caracterización de los subgrupos (forma compacta): Sea $\emptyset \neq H \subseteq G$. Entonces
$$(H, *) \text{ es subgrupo de } (G, *) \Leftrightarrow (\forall x, y \in H)\, x * y^{-1} \in H$$

6. Propiedad: para $n \geq 2$, $(\mathbb{Z}_n, +_n)$ es un grupo.

7. Teorema de Lagrange: Sea $(G, *)$ un grupo finito y $(H, *)$ un subgrupo cualquiera de él. Entonces $|H|$ divide a $|G|$. Ojo que esto no nos dice que todos los divisores del orden de G tienen un subgrupo asociado, sino que los posibles (candidatos) órdenes de subgrupos de G, son los divisores del orden de G.

8. Corolario: para $p \in \mathbb{N}$ primo, los únicos subgrupos de $(\mathbb{Z}_n, +_n)$ son los triviales.

Morfismos

1. Morfismo: Sean $(A, *)$ y $(B, \triangle)$ dos estructuras algebraicas, y sea $f : A \to B$ una función. Decimos que f es un morfismo u homomorfismo si $(\forall x, y \in A)\, f(x * y) = f(x) \triangle f(y)$.

2. Isomorfismo: Si $f : A \to B$ es un morfismo y además una función biyectiva, entonces le llamamos isomorfismo.

   Si existe un isomorfismo $f : A \to B$, diremos que $(A, *)$ y $(B, \triangle)$ son estructuras isomorfas, denotado por $(A, *) \cong (B, \triangle)$.

3. Morfismos sobreyectivos: Sean $(A, *)$ y $(B, \triangle)$ dos estructuras algebraicas, y sea $f : A \to B$ un morfismo sobreyectivo. Se tiene que:
   - Si $*$ es asociativa/conmutativa, entonces $\triangle$ también es asociativa/conmutativa (respectivamente).

- Si $(A, *)$ tiene neutro $e \in A$, entonces $(B, \triangle)$ también tiene neutro: $f(e)$.
- Sea $(A, *)$, con $*$ asociativa y neutro e, y sea $a \in A$. Si a posee inverso a^{-1}, entonces $f(a)$ también posee inverso, y más aún, $(f(a))^{-1} = f(a^{-1})$.

Anillos

1. Sea $(A, +, \cdot)$ una estr. algbr.. Diremos que es un anillo si:
   - $(A, +)$ es grupo abeliano
   - $\cdot$ es asociativa
   - $\cdot$ distribuye con respecto a $+$
2. Si la operación $\cdot$ posee neutro en A (denotado por 1), diremos que $(A, +, \cdot)$ es un anillo con unidad.
3. Si la operación $\cdot$ es conmutativa, diremos que $(A, +, \cdot)$ es un anillo conmutativo.
4. Proposición: $(\mathbb{Z}_n, +_n, \cdot_n)$ es un anillo conmutativo con unidad.
5. Divisores de cero: Sea un anillo $(A, +, \cdot)$. Si existen $x, y \in A$ **no nulos** tales que $x \cdot y = 0$, entonces x e y son llamados divisores de cero.
6. Propiedad: Sea un $(A, +, \cdot)$ un anillo y $a \in A \setminus \{0\}$. Entonces: a es divisor de $0 \iff a$ no es cancelable.

Cuerpos

1. Sea $(K, +, \cdot)$ una estr. algbr.. Diremos que es un cuerpo si:
   - $(K, +, \cdot)$ es anillo conmutativo con unidad.
   - Todo elemento de $K \setminus \{0\}$ es invertible para $\cdot$.

   Notar que, equivalentemente, $(K, +, \cdot)$ es un cuerpo ssi:
   - $(K, +)$ es grupo abeliano
   - $(K \setminus \{0\}, \cdot)$ es grupo abeliano
   - $\cdot$ distribuye con respecto a $+$
2. Propiedad: Un cuerpo **no** tiene divisores de cero.
3. Propiedad: Sea $(A, +, \cdot)$ un anillo conmutativo con unidad tal que $|A|$ es **finito**. Entonces:
   $$(A, +, \cdot) \text{ no tiene divisores de cero} \iff (A, +, \cdot) \text{ es cuerpo}$$
4. Teorema: Sea $n \in \mathbb{N}$ con $n \geq 2$. Entonces, las siguientes afirmaciones son equivalentes:
   - $(\mathbb{Z}_n, +_n, \cdot_n)$ es un cuerpo
   - $(\mathbb{Z}_n, +_n, \cdot_n)$ no tiene divisores de cero
   - n es un número primo.

Cualquier comentario o consulta a felipe.e.atenas@gmail.com
Éxito en el estudio!