ROBERTO CADENA VEGA

MATEMÁTICAS

Índice general

Todo list

1
Álgebra abstracta

1.1 Grupos

Definiciones

Definición 1.1.1. Un grupo es un conjunto no vacio G en el que esta definida la operacion $\star$, tal que:

$$\begin{aligned} \star\colon G, G &\rightarrow G \\ (a, b) &\rightarrow (a \star b) \end{aligned} \tag{1.1.1}$$

Existen definiciones parciales de grupo dependiendo de las propiedades que cumple su operación:

Cerradura $a \star b \in G \quad \forall a, b \in G$

Asociatividad $a \star (b \star c) = (a \star b) \star c \quad \forall a, b, c, \in G$

Identidad $\exists e \in G \ni a \star e = e \star a = a \quad \forall a \in G$

Inverso $\exists b \in G \ni a \star b = b \star a = e \quad \forall a \in G$

Cuando se cumplen las propiedades de *cerradura* y *asociatividad* se le llama *semigrupo*; si adicionalmente se cumple la propiedad de *existencia de identidad* se le llama *monoide*; si adicionalmente se cumple la propiedad de *existencia de inverso* se le llama *grupo*.

Ejercicio 1.1.1. Demostrar que el grupo cimpuesto por las matrices de la forma:

$$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}, \quad \forall \theta \in \mathbb{R}$$

es un grupo.

Definición 1.1.2. Se dice que un grupo G es abeliano si:

$$a \star b = b \star a \tag{1.1.2}$$

Ejemplo 1.1.1. El conjunto $\mathbb{Z}/n\mathbb{Z}$

Ejercicio 1.1.2. Consideremos a $\mathbb{Z}$ con el producto usual ¿Es este un grupo?

Ejercicio 1.1.3. Consideremos a $\mathbb{Z}^+$ con el producto usual ¿Es este un grupo?

Ejercicio 1.1.4. Sea $G = \mathbb{R} \setminus \{0\}$. Si definimos $a \star b = a^2 b$ ¿G es un grupo?

Definición 1.1.3. Orden de un grupo es el numero de elementos que tiene dicho grupo y se denota por $|G|$.
Un grupo G será finito si tiene orden finito, de lo contrario será infinito.

Ejemplo 1.1.2. Si $G = \{e\}$, su orden será $|G = \{e\}| = 1$

Ejemplo 1.1.3. El orden del conjunto de numeros reales es infinito $|\mathbb{R}| = \infty$.

Proposición 1.1.1. *Si G es un grupo, entonces:*

1. *El elemento identidad es único.*
2. *El elemento inverso $a^{-1} \quad \forall a \in G$ es único.*
3. *El elemento inverso del inverso del un elemento del grupo es el mismo elemento $\left(a^{-1}\right)^{-1} = a \quad \forall a \in G$.*
4. *El elemento inverso de la operación de dos elementos del grupo es la operacion de los inversos de los elementos en orden inverso $(a \star b)^{-1} = b^{-1} \star a^{-1}$*
5. *En general lo anterior se cumple para cualquier numero de elementos $(a_1 \star a_2 \star \ldots \star a_n)^{-1} = a_n^{-1} \star \ldots \star a_2^{-1} \star a_1^{-1}$.*

Demostración.

1. Dados e_1 y e_2 identidades del grupo, son identicos. Si aplicamos la identidad e_2 a e_1, tenemos como resultado e_1, y si aplicamos la identidad e_1 a e_2 obtenemos como resultado e_2:

$$e_1 = e_2 \star e_1 = e_1 \star e_2 = e_2$$

por lo que podemos ver que ambas identidades son la misma.

2. Sean b, c inversos de a, entonces:

$$\begin{aligned} b \star a &= e \\ a \star c &= e \end{aligned}$$

por lo que podemos ver que:

$$b = b \star e = b \star (a \star c) = (b \star a) \star c = e \star c = c$$

3. Sabemos que existe un inverso a^{-1} tal que:

$$a \star a^{-1} = a^{-1} \star a = e \quad \forall a \in G$$

asi pues, se sigue que:

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

y como sabemos que el elemento que operado con el inverso sea la identidad es el elemento mismo tenemos que:

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

4. Si operamos por la izquierda el termino $b^{-1} \star a^{-1}$ con $a \star b$:

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

de la misma manera si operamos por la derecha:

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

por lo tanto:

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

$\square$

Reglas de cancelación

Proposición 1.1.2. *Sea G un grupo y $a, b, c \in G$, tendremos que:*

$$\begin{aligned} a \star b = a \star c &\implies b = c \\ b \star a = c \star a &\implies b = c \end{aligned} \tag{1.1.3}$$

Demostración. Si tomamos en cuenta que $a \star b = a \star c$:

$$b = e \star b = \left(a^{-1} \star a\right) \star b = a^{-1} \star (a \star b) = a^{-1} \star (a \star c) = \left(a^{-1} \star a\right) \star c = e \star c = c$$

de la misma manera para $b \star a = c \star a$:

$$b = b \star e = b \star \left(a \star a^{-1}\right) = (b \star a) \star a^{-1} = (c \star a) \star a^{-1} = c \star \left(a \star a^{-1}\right) = c \star e = c$$

□

Subgrupos

Definición 1.1.4. Un subconjunto no vacio H de un grupo G se llama subgrupo si H mismo forma un grupo respecto a la operación de G. Cuando H es subgrupo de G se denota $H < G$ o $G > H$.

Observación 1.1.1. Todo grupo G tiene automaticamente dos subconjuntos triviales, el mismo G y la identidad $\{e\}$.

Proposición 1.1.3. *Un subconjunto no vacio $H \subset G$ es un subgrupo de G si y solo si H es cerrado respecto a la operación de G y $a \in H \implies a^{-1} \in H$.*

Demostración. Teniendo que H es un subgrupo de G tenemos que H es un grupo, por lo que automaticamente se cumple la cerradura y la existencia del inverso dentro del subgrupo.

Teniendo que H es cerrado, no vacio y $a^{-1} \in H \quad \forall a \in H$. Sabemos que $a^{-1} \star a = e \in H$ debido a que H es cerrado. Ademas para $a, b, c \in H$ sabemos que $a \star (b \star c) = (a \star b) \star c$ debido a que se cumple en G y H hereda esta propiedad.

Por lo que H es un grupo, y por lo tanto subgrupo de G. □

Ejemplo 1.1.4. Sea $G = \mathbb{Z}$ con la suma usual y sea H el conjunto de los enteros pares, es decir:

$$H = \{2n | n \in \mathbb{Z}\}$$

¿Es H un subgrupo de G?

Empecemos con dos elementos $a, b \in H$, por lo que tenemos que:

$$\begin{aligned} a &= 2q \quad q \in \mathbb{Z} \\ b &= 2q' \quad q' \in \mathbb{Z} \end{aligned}$$

y al sumarlos tenemos que:

$$a + b = 2q + 2q' = 2(q + q') = 2q'' \quad q'' \in \mathbb{Z}$$

por lo que $a + b \in H$.

Por otro lado, para $a \in H$ existe un $q \in \mathbb{Z}$ tal que $a = 2q$. Su inverso será:

$$-a = -2q = 2(-q)$$

por lo que existe $q' = -q \in \mathbb{Z}$ tal que:

$$2q' = -a \in H$$

y por lo tanto $H < \mathbb{Z}$.

Ejemplo 1.1.5. Consideremos $G = \mathbb{C}^* = \mathbb{C} \setminus \{0\}$ con el producto usual, y un subconjunto $\mathcal{U}$

$$\mathcal{U} = \{z \in \mathbb{C}^* \,||z| = 1\}$$

¿Es $\mathcal{U}$ un subgrupo de G?

Dados dos elementos $z_1, z_2 \in \mathcal{U}$ sabemos que $|z_1| = |z_2| = 1$, por lo tanto:

$$|z_1 z_2| = |z_1||z_2| = 1$$

por lo que $z_1 z_2 \in \mathcal{U}$.

Por otro lado, para $z \in \mathcal{U}$ tenemos que $|z| = 1$, y por lo tanto:

$$|z^{-1}| = |z|^{-1} = \frac{a}{|z|} = 1$$

por lo que $z^{-1} \in \mathcal{U}$ y $\mathcal{U} < \mathbb{C}^*$

Subgrupo Normal

Homomorfismos de grupo

1.2 Anillos

Definiciones

Homomorfismos de anillo

Ideales

1.3 Dominios Enteros

Definiciones

Máximo Común Divisor

mínimo común multiplo

Algoritmo de la división de Euclides

2
Álgebra lineal

3
Ecuaciones diferenciales