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 $\mathbb{Z}/n\mathbb{Z}$

Falta escribir ejemplo

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:

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

□

Reglas de cancelación

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

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

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 $\mathcal{U}$

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

¿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 $\mathcal{U} < \mathbb{C}^*$

Ejemplo 1.1.6. Sea G un grupo, a un elemento del grupo y $C(a) = \{g \in G \mid g \star a = a \star g\}$ ¿Es $C(a)$ subgrupo de G?

Primero notamos que $C(a)$ es no vacio debido a que al menos tiene a la identidad.

$$e \star a = a \star e \implies e \in C(a)$$

Ahora tomemos dos elementos $g_1, g_2 \in C(a)$, para los cuales:

$$\begin{aligned} g_1 \star a &= a \star g_1 \\ g_2 \star a &= a \star g_2 \end{aligned}$$

Ahora, si operamos estos dos elementos tendremos:

$$(g_1 \star g_2) \star a = g_1 \star (g_2 \star a) = g_1 \star (a \star g_2) = (g_1 \star a) \star g_2 = (a \star g_1) \star g_2 = a \star (g_1 \star g_2)$$

por lo que $g_1 \star g_2 \in C(a)$.

Por ultimo, podemos ver que:

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

En donde para que el elemento inverso exista en $C(a)$, se debe de cumplir que $g^{-1} \star a = a \star g^{-1}$:

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

Por lo que $C(a) < G$.

Ejercicio 1.1.5. Sea X un conjunto no vacio. Consideremos $G = \delta X$. Sea $a \in X$, $H(a) = \{f \in \delta X \mid f(a) = a\}$. Verificar que $H \subset G$ es un subgrupo bajo la composición de funciones. Note que $H(a)$ es no vacio, debido a que $\mathrm{id}_X \in H(a)$.

Definición 1.1.5. Sea G un grupo y $a \in G$. El conjunto

$$A = \langle a \rangle = \left\{ a^i \mid i \in \mathbb{Z} \right\} \tag{1.1.4}$$

es un subgrupo de G.
A es no vacio, puesto que $a^0 = e \in A$.
Por otro lado, para dos elementos $a^i, a^j \in A$ tenemos que:

$$a^i a^j = a^{i+j} \in A$$

y para un elemento $a^i \in A$, tenemos que:

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

por lo que $\langle a \rangle$ es un subgrupo. A este se le llama subgrupo cíclico de G generado por a.

Definición 1.1.6. Sea G un grupo, decimos que G es cíclico si $G = \langle a \rangle$ para algun $a \in G$.

Ejemplo 1.1.7. Dado el grupo $G = \{e\}$, tenemos que el subgrupo cíclico generador de G es:

$$\langle e \rangle = \left\{ e^i \in G \mid i \in \mathbb{Z} \right\}$$

al operar este subgrupo tenemos:

$$\begin{aligned} e^1 &= e \\ e^2 &= e \star e = e \\ e^3 &= e \star e \star e = e \end{aligned}$$

por lo que obtenemos todos los elementos del grupo.

Ejemplo 1.1.8. Dado el grupo $G = \{a, e\}$, y la siguiente tabla para la operación del grupo:

$\star$	e	a
e	e	a
a	a	e

con esto, tenemos que el subgrupo ciclico generador de G es:

$$\langle a \rangle = \left\{ a^i \in G \mid i \in \mathbb{Z} \right\}$$

y al operar este subgrupo tenemos:

$$\begin{aligned} a^1 &= a \\ a^2 &= a \star a = e \end{aligned}$$

y obtenemos todos los elementos del grupo.

Ejercicio 1.1.6. Dado el grupo $G = \{e, a, b\}$ y la operación:

$\star$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Encontrar el subgrupo cíclico generador.

Ejercicio 1.1.7. Dado el grupo $\mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2 = \{[0], [1]\}$ con la operación $[a] + [b]$; encontrar el subgrupo cíclico generador.

Ejercicio 1.1.8. Sea G un grupo en el que $x^2 = e$ para todo $x \in G$. Verificar que G es abeliano, es decir $a \star b = b \star a$.

Definición 1.1.7. Sea G un grupo, H un subgrupo de G ($H < G$), para $a, b \in G$, decimos que a es congruente con b mód H, denotado por:

$$a \cong b \mod H \tag{1.1.5}$$

si

$$a \star b^{-1} \in H \tag{1.1.6}$$

De aqui en adelante se deja la notación de la operación $\star$ para la operación genérica del grupo, sin que por esto se entienda que la operación es siempre el producto usual.

Ejercicio 1.1.9. Demostrar que $\cong$ es una relación de equivalencia.

Definición 1.1.8. Si H es un subgrupo de G y $a \in G$, entonces

$$Ha = \{ha \mid h \in H\} \tag{1.1.7}$$

se llama clase lateral derecha de H en G.

Lema 1.1.1. *Para todo $a \in G$ se tiene que:*

$$Ha = \{x \in G \mid a \cong x \mod H\} \tag{1.1.8}$$

Demostración. Sea un conjunto definido como $[a] = \{x \in G \mid a \cong x \mod H\}$, por verificar que $Ha = [a]$. Para verficar esto, tenemos que verificar que $Ha \subseteq [a]$ y despues que $[a] \subseteq Ha$.

Para verificar que $Ha \subseteq [a]$ definimos un elemento $h \in H$ y $ha \in Ha$, si ahora operamos a con $(ha)^{-1}$ y verificamos que esta en H, podemos decir que $a \cong ha \mod H$:

$$a(ha)^{-1} = a(a^{-1}h^{-1}) = (aa^{-1})h^{-1} = h^{-1} \in H$$

por lo que podemos concluir que $a \cong ha \mod H$, lo que implica que $ha \in [a]$; pero como ha es un elemento arbitrario de Ha, tenemos que:

$$Ha \subseteq [a]$$

Para verificar que $[a] \subseteq Ha$ empezamos con un elemento $x \in [a]$, es decir $a \cong x \mod H$, lo cual implica $ax^{-1} \in H$, en particular nos interesa:

$$(ax^{-1})^{-1} = xa^{-1} \in H$$

Por otro lado, sea $h = xa^{-1} \in H$, entonces tenemos que:

$$ha = (xa^{-1})a = x(a^{-1}a) = x \in Ha$$

por lo que podemos decir que:

$$[a] \subseteq Ha$$

y por lo tanto

$$[a] = Ha$$

□

Teorema 1.1.1. *Sea G un grupo finito y $H \subset G$, entonces el orden de H divide al orden de G*

$$|H|/|G| \tag{1.1.9}$$

y esto implica que existe una $k \in \mathbb{Z}$ tal que:

$$|G| = k|H| \tag{1.1.10}$$

A esto se le conoce como Teorema de Lagrange.

Demostración. Dado $[a] = Ha$, las clases de equivalencia forman una partición de G:

$$\begin{aligned} [a_1] \cup [a_2] \cup \cdots \cup [a_k] &= G \\ [a_i] \cap [a_j] &= \varnothing \quad i \neq j \end{aligned}$$

Por otro lado, las clases laterales derechas forman una partición:

$$\begin{aligned} Ha_1 \cup Ha_2 \cup \cdots \cup Ha_k &= G \\ Ha_i \cap Ha_j &= \varnothing \quad i \neq j \end{aligned}$$

Establezcamos una biyección:

$$\begin{aligned} Ha_i &\to H \\ ha_i &\to h \end{aligned}$$

es decir, el orden de Ha_i es el orden de H

$$|Ha_i| = |H| \quad \forall 1 \leq i \leq k$$

entonces:

$$\begin{aligned} |G| &= |Ha_1| + |Ha_2| + \cdots + |Ha_k| \\ &= |H| + |H| + \cdots + |H| \\ |G| &= k|H| \end{aligned}$$

pero $k \in \mathbb{Z}$, entonces:

$$|H|/|G|$$

□

Definición 1.1.9. Si G es finito y H es un subgrupo de G lllamamos $\frac{|G|}{|H|}$ el indice de H en G y lo denotamos por $i_G(H)$.

Definición 1.1.10. Si G es finito y $a \in G$, llamamos orden de a al mínimo entero positivo n tal que $a^n = e$ y lo denotamos por $O(a)$, por lo que se sigue que:

$$a^{O(a)} = e \tag{1.1.11}$$

Proposición 1.1.4. *Si G es finito y $a \in G$, entonces el orden de a divide al orden de G:*

$$O(a) \big/ |G| \tag{1.1.12}$$

Demostración. Supongamos $H = \langle a \rangle$, entonces $O(a) = |H|$. Podemos ver ahora, por el teorema de Lagrange:

$$|H| \big/ |G| \implies O(a) \big/ |G|$$

□

Corolario 1.1.1. *Si G es un grupo finito de orden n, entonces:*

$$a^n = e \quad \forall a \in G \tag{1.1.13}$$

Demostración. Por la proposición anterior tenemos que:

$$O(a) \big/ |G| = O(a) \big/ n$$

esto equivale a decir que existe un $k \in \mathbb{Z}$, tal que $n = kO(a)$, entonces podemos decir:

$$a^n = a^{kO(a)} = \left(a^{O(a)}\right)^k = e^k = e \quad \forall a \in G$$

□

Subgrupo Normal

Definición 1.1.11. Un grupo N de G se dice que es un subgrupo normal de G denotado por $N \triangle G$, si para todo $g \in G$ y para todo $n \in N$ se tiene que:

$$gng^{-1} \in N \tag{1.1.14}$$

Lema 1.1.2. *N es un subgrupo normal de G si y solo si:*

$$gNg^{-1} = N \quad \forall g \in G \tag{1.1.15}$$

Demostración. Si $gNg^{-1} = N \quad \forall g \in G$, entonces en particular tenemos que:

$$gNg^{-1} \subseteq N$$

por lo que se tiene que $gng^{-1} \in N \quad \forall n \in N$, por lo tanto $N \triangle G$.

Por otro lado, si N es un subgrupo normal de G, entonces tenemos que:

$$gng^{-1} \in N$$

para todo $g \in G$ y para todo $n \in N$, esto implica que:

$$gNg^{-1} \subseteq N$$

Por ultimo, podemos ver que $g^{-1}Ng = g^{-1}N\left(g^{-1}\right)^{-1} \subseteq N$, ademas:

$$N = eNe = g\left(g^{-1}Ng\right)g^{-1} \subseteq gNg^{-1}$$

por lo tanto, podemos concluir que $gNg^{-1} = N$ □

Lema 1.1.3. *El subgrupo N de G, es un subgrupo normal de G ($N \triangle G$), si y solo si toda clase lateral izquierda de N en G es una clase lateral derecha de N en G.*

Demostración. Sea $aH = \{ah \mid h \in H\}$ la clase lateral izquierda de H.

Si N es un subgrupo normal de G, para todo $g \in G$ y para todo $n \in N$, tenemos que:

$$gNg^{-1} = N$$

entonces tenemos que:

$$gN = gNe = gN\left(g^1g\right) = \left(gNg^{-1}\right)g = Ng$$

por lo que toda clase lateral izquierda coincide con la clase lateral derecha.

Por otro lado, si ahora suponemos que las clases laterales coinciden, entonces:

$$gNg^{-1} = (gN)g^{-1} = Ngg^{-1} = N$$

por lo que podemos concluir que se trata de un subgrupo normal.

□

Definición 1.1.12. Denotamos G/N a la colección de las clases laterales derechas de N en G.

$$G/N = \{Na \mid a \in G\} \tag{1.1.16}$$

Teorema 1.1.2. *Si G es un grupo y N es un subgrupo normal de G, entonces G/N es tambien un grupo y se denomina grupo cociente.*

Demostración. Para demostrar la existencia de identidad primero verificamos que para un elemento $x \in G/N$, el elemento tiene la forma $x = Na \quad a \in G$, por lo que podemos ver que:

$$\begin{aligned} xNe = xN = NaN = NNa = Na &= x \\ Nex = Nx = NNa = Na &= x \end{aligned}$$

□

Para demostrar la existencia de un inverso definimos un elemento $x \in G/N$ y $Na^{-1} \in G/N$, y queremos demostrar que $x^{-1} = Na^{-1}$ es el inverso de $x = Na$. Al operar estos elementos por la derecha y la izquierda tenemos:

$$\begin{aligned} xx^{-1} = NaNa^{-1} = NNaa^{-1} = Ne &= N \\ x^{-1}x = Na^{-1}Na = NNa^{-1}a = Ne &= N \end{aligned}$$

por lo tanto $Na^{-1} = x^{-1}$ es el inverso de x. Por lo tanto, G/N es un grupo.

Homomorfismos de grupo

Definición 1.1.13. Sea una aplicación $\varphi\colon G \to \bar{G}$, G un grupo con operacion $\circ$ y $\bar{G}$ un grupo con operación $\diamond$. Se dice que φ es un homomorfismo si para $a, b \in G$ cualesquiera se tiene que:

$$\varphi(a \circ b) = \varphi(a) \diamond \varphi(b) \tag{1.1.17}$$

1.2 *Anillos*

Definiciones

Falta escribir apunte

Homomorfismos de anillo

Falta escribir apunte

Ideales

Falta escribir apunte

1.3 Dominios Enteros

Definiciones

Falta escribir apunte

Máximo Común Divisor

Falta escribir apunte

mínimo común multiplo

Falta escribir apunte

Algoritmo de la división de Euclides

Falta escribir apunte

2
Álgebra lineal

3
Ecuaciones diferenciales