Apuntes álgebra abstracta

Thomas Gomez Serpa

1 de febrero de 2024

Índice general

Capítulo 1

The First Chapter

1.1. Operaciones binarias y grupos

Definición 1 *Sea G un conjunto. Una operación binaria (tambien llamada* ***ley de composición interna*** *en G es una función de la forma:*

$$\begin{gathered} * : G \times G \longrightarrow G \\ (g, h) \mapsto *(g, h) \coloneqq g * h \end{gathered} \tag{1.1}$$

Solemos denotar $(G, *)$ cuando indicamos que en G existe la operación binaria $*$. El par $(G, *)$ se le llama ***magma****, además decimos que $*$ es:*

1. *Asociativa si $\forall g, h, k \in G$ se tiene $(g * h) * k = g * (h * k)$*

2. *Conmutativa si $\forall g, h g * h = h * g$*

Note que por definición toda operación binaria es ***cerrada***
Ejemplo
Considere $\mathbb{Z}^+ = \{1, 2, ...\}$ junto con :

$$\begin{gathered} + : \mathbb{Z}^+ \times \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+ \\ (n, m) \longmapsto n + m \end{gathered} \tag{1.2}$$

Siendo $+$ la suma usual. Entonces $(\mathbb{Z}^+, +)$ es un magma. Además $+$ es asociativa y conmutativa. De igual forma $(\mathbb{Z}^+, \cdot)$ (siendo $\cdot$ la multiplicación usual), es un magma con operación asociativa y conmutativa. Claramente en ambos ejemplos podemos reemplazar $\mathbb{Z}^+$ por $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
Los magmas donde la operación es asociativa son llamados **semigrupos**

Definición 2 *Sea $(G, *)$ un semigrupo. Un* ***elemento identidad*** *o* ***elemento neutro*** *en G es un elemento $e \in G$ tal que:*

$$g * e = e * g = g \quad \forall g \in G \tag{1.3}$$

En este caso decimos que $(G, *)$ *es un* ***monoide***

Tenemos las siguientes observaciones:

1. En un monoide el elemento identidad es único. En efecto, si $e, e' \in G$ son identidades para G , es decir:

$$\begin{aligned} g * e = e * g = g, \quad \forall g \in G \\ g * e' = e' * g = g, \quad \forall g \in G \end{aligned} \tag{1.4}$$

   en particular $e = e * e'$ por que e' es identidad, de igual manera $e' = e * e'$ porque e es la identidad. Igualando expresiones se tiene que $e' = e$

   $\square$

2. Por definición un monoide es no vacío

3. Para un monoide $(G, *)$ con identidad e solemos escribir $(G, *, e)$ para destacar la identidad. Sin embargo,muchas veces,cuando es claro quién es $*$ y e, nos referimos al monoide simplemente como G

Definición 3 *Sea* $(G, *, e)$ *un monoide. Decimos que* $(G, *, e)$ *es un* ***grupo*** *si* $\forall g \in G \exists g' \in G$ *(llamado* ***inverso bilátero*** *de* g*), tal que:*

$$g * g' = g' * g = e \tag{1.5}$$

En resumen, un grupo es un conjunto con una operación binaria cerrada que es asociativa, tiene elemento neutro y posee inversos para todos los elementos del grupo. Si además la operación es conmutativa decimos que el grupo es ***abeliano***

Ejemplos

1. $(\mathbb{Z}, +, 0)$ es un grupo. $\mathbb{Z}$ se puede remplazar por $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

2. $(\mathbb{Z}, *, 1)$ es un monoide pero no un grupo (0 no tiene inverso). Lo mismo se aplica para $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

3. Si denotamos $\mathbb{Q}^* := \mathbb{Q} \backslash \{0\}$ entonces $(\mathbb{Q}, *, 1)$, note que esto no se cumple para $\mathbb{Z}^*$ ya que por ejemplo 2 no tiene inverso múltiplicativo.

Antes de dar más ejemplos de grupos, vamos a ver algunas de sus propiedades básicas. Aunque la mayoría se enuncien para **grupos** , la mayoría de resultados no usan toda la estructura, pudiendo entonces también ser válidos para semigrupos, monoides, etc.

Notación

Para un grupo $(G, *, e)$ resulta inconveniente, cuando se hacen cuentas, escribir la operación $*$ todo el tiempo. Por lo tanto, cuando no haya lugar a confusión, en vez de $g * h$ escribimos simplemente gh, para $g, h \in G$. Por otro lado la operación $*$ se remplazará por $\cdot$ y se escribirá un grupo de la forma $(G, *, e)$. La anterior notación es conocida como **notación multiplicativa**.

Definición 4 *Sea G un grupo. El orden de G es su cardinalidad $|G|$. Decimos que G es un grupo finito si su orden lo es, en caso contrario, decimos que G es un grupo infinito*

Teorema 1 *Sea $(G, \cdot, e)$ entonces:*

1. *$\forall g \in G$, el inverso es único (y será denotado en adelante por g^{-1})*

2. *$\forall g \in G \quad (g^{-1})^{-1} = g$*

3. *(Ley asociativa generalizada) Para cualesquiera $g_1, g_2, ..., g_n$ el valor de $g_1 g_2 ... g_n$ es independiente de cómo se apliquen paréntesis en la expresión. Debido a esta ley, de ahora en adelante se podran escribir productos de la forma $g_1, g_2, ..., g_n$ sin necesidad de incluir paréntisis*

4. *$\forall g, h \in G \quad (gh)^{-1} = h^{-1} g^{-1}$*

5. *Si $c \in G$ es tal que $cc = c$ (idempotencia) entonces $c = e$*

6. *(Ley cancelativa izquierda y derecha). Para $g, h, k \in G$ se tiene que*

$$\begin{aligned} gh = gk \longrightarrow h = k \\ hg = kg \longrightarrow h = k \end{aligned} \tag{1.6}$$

7. *$\forall g, h \in G$ las ecuaciones $gx = h$ y $yg = h$ tienen como única solución en G a $x = g^{-1} h$ y $y = hg^{-1}$*

Demostración:

1. *Supongamos que para $g \in G$ se tienen 2 inversos g' y g''. Es decir*

$$\begin{aligned} gg' = g'g = e \\ gg'' = g''g = e \end{aligned} \tag{1.7}$$

   Por lo tanto:

$$g' = g'e = g'(gg'') = (g'g)g'' = eg'' = g'' \tag{1.8}$$

   $\square$

2. *Por definición $gg^{-1} = g^{-1}g = e$ por lo que el inverso de g^{-1} es g, es decir $(g^{-1})^{-1} = g$*

   $\square$

3. *Por inducción fuerte:*

   Caso Base: Note que de manera trivial se tiene que la hipótesis es válida para $n = 1, n = 2, n = 3$ (para $n = 3$ se tiene la propiedad asociativa ordinaria).

   Ahora suponga que el enunciado se cumple para $n < n + 1$. Es decir $\forall g_1, g_2, ..., g_n \in G$ el valor de $g_1 g_2 ... g_n$ es independiente de cómo se apliquen los paréntisis en la expresión.

   Paso inductivo: Considere ahora $g_1 g_2 ... g_n g_{n+1}$ para $g_1, g_2, ... g_n, g_{n+1} \in G$. Note que al aplicar paréntesis de manera arbitraría en la expresión, siempre nos quedan expresiones aisladas con un número de términos menores a $n + 1$, cada una de estas expresiones aisladas tiene un valor bien definido debido a la hipótesis de inducción. Por lo anterior la expresión original se nos reduce a una serie de términos de longitud menor a $n + 1$, aplicando la hipótesis de inducción nos queda que el valor de $g_1 g_2 ... g_n g_{n+1}$ para $g_1, g_2, ... g_n, g_{n+1} \in G$ es independiente de como se apliquen paréntisis en la expresión.

   $\square$

4. *Note que por la ley generalizada de asociatividad se cumple:*

$$(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = geg^{-1} = gg^{-1} = e \tag{1.9}$$

   Análogamente $(h^{-1}g^{-1})(gh) = e$ por lo tanto $(gh)^{-1} = h^{-1}g^{-1}$

5. *Como G es un grupo* c^{-1} *existe. Así*

$$c^{-1}(cc) = (c^{-1}c)c = ec = c \tag{1.10}$$

Pero por hipótesis $cc = c$ *luego*

$$c^{-1}(cc) = c^1 c = e \tag{1.11}$$

Igualando se obtiene lo deseado

□

6. *Si tenemos* $gh = gk$ *se puede multiplicar por* g^{-1} *a la izquierda en ambos lados. Luego*

$$\begin{aligned} g^{-1}(gh) &= g^{-1}(gk) \\ (g^{-1}g)h &= (g^{-1}g)k \\ eh &= ek \\ h &= k \end{aligned} \tag{1.12}$$

Análogamente se prueba la otra ley cancelativa.

□

7. *Es claro que la solución de la ecuación* $gx = h$ *es* $g^{-1}h$ *ya que al remplazarse se cumple la igualdad. Que sea la única solución se sigue de la unicidad de* g^{-1}*. Análogamente se demuestra la solución y la unicidad de la otra ecuación.*

Definición 5 *Para cualquier grupo* $(G, \cdot, e)$*, dado* $g \in G$ *se define*

$$g^n := \underbrace{gg...g}_{n}, \quad \forall n \in \mathbb{Z}^+ \tag{1.13}$$

Tambien se define $g^0 := e$ *y* $g^{-n} := (g^{-1})^n$

Hasta ahora , se ha simplificado la notación de un grupo G denotando la operación como $\cdot$ y las operaciones por gh. Como ya hemos dicho esta notación es la notación multiplicativa. Esta notación se suele reservar para grupos no abelianos.
Sin embargo para grupos abelianos arbitrarios se suele emplear **notación aditiva**, donde la operación se denota como $+$ y el elemento identidad como 0 (llamado en algunos libros como elemento cero). Por lo tanto las cuentas son de la forma $g + h$ y los inversos de la forma $-g$. Se usa la convención $g - h := g + (-h)$.

Definición 6 *En notación aditiva, para cualquier grupo $(G, +, 0)$ dado $g \in G$ se define*

$$n \cdot g \coloneqq \underbrace{g + g ... + g}_{n}, \quad n \in \mathbb{Z}^{+} \tag{1.14}$$

Tambien se define $0 \cdot g \coloneqq 0$ y $(-n) \cdot g \coloneqq n \cdot (-g) \quad \forall n \in \mathbb{Z}^{+}$

Teorema 2 *Sea G un grupo en notación multiplicativa, entonces para cualquier $g \in G \wedge n, m \in \mathbb{Z}^{+}$, se cumplen las siguientes propiedades*

1. $(g^{n})^{m} = g^{nm}$
2. $g^{n}g^{m} = g^{n+m}$
3. $(g^{n})^{-1} = g^{-n}$

Demostración:

1. *Note que por definición $g^{n} \coloneqq \underbrace{gg...g}_{n}, \forall n \in \mathbb{Z}^{+}$, por ende:*

$$(g^{n})^{m} = (\underbrace{gg...g}_{n})^{m} = \underbrace{\underbrace{gg...g}_{n} \cdot \underbrace{gg...g}_{n} ... \cdot \underbrace{gg...g}_{n}}_{m} = \underbrace{gg...g}_{nm} = g^{nm} \tag{1.15}$$

$\square$

2. *De nuevo por la definición se tiene:*

$$g^{n}g^{m} = \underbrace{gg...g}_{n} \cdot \underbrace{gg...g}_{m} = \underbrace{gg...g}_{n+m} = g^{n+m} \tag{1.16}$$

$\square$

3. *Se debe probar que la inversa de g^{n} es g^{-n} para cualquier $n \in \mathbb{Z}^{+}$*

   Por inducción:

   Caso base: La hipótesis se cumple de manera trivial para $n = 1$

   Paso inductivo: Suponga válida la hipótesis para n, tenga en cuenta que $g^{-m} \coloneqq (g^{-1})^{m} \quad \forall m \in \mathbb{Z}^{+}$ así:

$$g^{n+1} \cdot g^{-n-1} = g^{n+1} \cdot (g^{-1})^{n+1} = g^{n}g^{1}g^{-1}g^{-n} = g^{n}g^{-n} = e \tag{1.17}$$

$\square$

El anterior resultado permite escribir el teorema en notación aditiva

Teorema 3 *Sea G un grupo en notación de suma, entonces para cualquier $g \in G \wedge n, m \in \mathbb{Z}^+$, se cumplen las siguientes propiedades*

1. $m(ng) = (nm)g$
2. $ng + mg = (n + m)g$
3. $-(ng) = (-n)g$

Teorema 4 *Sea $(G, \cdot)$ un semigrupo. Entonces, G es un grupo si y solo si, se satisfacen las siguientes condiciones:*

1. *(Elemento identidad a la izquierda)* $\exists e \in G : eg = g \quad \forall g \in G$
2. *(Inversos a izquierda)* $\forall g \in G \quad \exists g' \in G : g'g = e$

Demostración:
$\longrightarrow$:
Si G es un grupo entonces se satisfacen por definición de grupo las 2 propiedades
$\longleftarrow$:
Sea G un semigrupo y supongamos las condiciones 1 y 2. Tomemos $g \in G$. Por 2 existe g' tal que $g'g = e$. Pero a su vez, existe, de nuevo por 2 un g'' tal que $g''g' = e$. Así

$$gg' = e(gg') = (g''g')(gg') = g''(g'g)g' = g''eg' = g''g' = e \tag{1.18}$$

Así g' es un inverso bilátero para g. Veamos que e es elemento identidad bilátero:

$$ge = g(g'g) = (gg')g = eg = g \tag{1.19}$$

□

El anterior resultado es simétrico, es decir en las condiciones 1 y 2 basta considerar elemento identidad a la derecha e inversos a la derecha respectivamente. Sin embargo no se pueden intercalar las lateralidades

Teorema 5 *Sea $(G, \cdot, e)$ un semigrupo. Entonces G es un grupo si y sólo si, para cualesquiera $g, h \in G$ las ecuaciones $gx = h$ y $yg = h$ tienen solución en G.*
Demostración:

$\longrightarrow$:
Suponga que G un grupo, entonces existen inversos para todos los elementos, además son inversos biláteros, entonces $\forall g, h \in G$ existen soluciones en G para las ecuaciones $gx = h$ y $yg = h$, más precisamente $x = g^{-1}h$ y $y = hg^{-1}$.
$\longleftarrow$:
Por contrarecíproca:
Suponga que $(G, \cdot, e)$ es un semigrupo (que no es un grupo), entonces el semigrupo puede ser un monoide o no. Si el semigrupo es un monoide, significa que es un monoide y no es un grupo, por ende debe existir un elemento $g \in G$ tal que no existe $x \in G$ que cumpla $gx = g$ y $xg = g$(No existe en general el neutro). Por otro lado si G es un semigrupo y no es un monoide, debe existir un elemento $g, h \in G$ tal que no existe $x \in G$ que cumpla $gx = e$ y $xg = e$(no existe en general el inverso). En ambos $\exists g \in G$ tal que no existen soluciones en G para las ecuaciones $gx = h$ y $yg = h$.
$\square$

1.2. Ejemplos grupos

Los **espacios vectoriales** V bajo la operación de $+$ forman un grupo conmutativo $(V, +, \mathbf{0})$,
El **grupo lineal general** definido como
$GL_n(\mathbb{R})\{A \in M_{n\times n} : A \text{ } es \text{ } invertible\}$, es un grupo no abeliano bajo la multiplicación usual de matrices.
Grupo de enteros módulo n
Sea $n \in \mathbf{Z}^+$ Definimos la relación en Z:

$$a \sim b \longleftrightarrow n \text{ } divide \text{ } a \text{ } b - a \tag{1.20}$$

1.3. Ejercicios

1. Determine cual de las siguientes operaciones binarias (tambien llamadas ley de composición interna) son asociativas (es decir son semigrupos)
   (a) La operación * en $\mathbb{Z}$ definida como $a * b = a - b$
   (b) La operación * en $\mathbb{R}$ definida como $a * b = a + b + ab$
   (c) La operación * en $\mathbb{Q}$
   (d) La operación * en $\mathbb{Z} \times \mathbb{Z}$

(e) La operación * en $\mathbb{Q} - \backslash\{0\}$

Solución:

(a)

No es un semigrupo (la operación o ley de composición interna no es asociativa)

Contraejemplo:

Sea $(1 * -1) * 1 = (1 - (-1)) * 1 = 2 * 1 = 2 - 1 = 1$ y
$1 * (-1 * 1) = 1 * (-1 - 1) = 1 * -2 = 1 - (-2) = 3$

(b)

Es un semigrupo (la operación o ley de composición interna es asociativa)

Demostración:

Suponga que $a, b \in \mathbb{R}$

Capítulo 2

The Second Chapter