Apuntes de clase

José Antonio de la Rosa Cubero

Grupos: Definición y Ejemplos

Un grupo G es un conjunto no vacío junto con una operación interna $\cdot$ satisfaciendo:

1. Propiedad asociativa $(ab)c = a(bc)$ y muchas veces escribimos abc.

2. Existencia de elemento neutro 1 tal que $1a = a1 = a$.

3. Existencia de inversos para cada $a \in G$: un elemento a^{-1} tal que $aa^{-1} = a^{-1}a = 1$

Si además verifica la propiedad conmutativa $ab = ba$ entonces el grupo es abeliano o conmutativo.

Proposición 1. *Sea G un grupo. Entonces:*

1. *En G hay un único elemento neutro: la unidad o el uno de G.*

   Demostración. Supongamos que hay otro, e. $1 = 1e = e$ □

2. *Cada elemento tiene un único inverso.*

   Demostración. Supongamos que hay otro, a' inverso de a. $a' = a'1 = a'aa^{-1} = a^{-1}$. □

3. *Para cada $a \in G$, $(a^{-1})^{-1} = a$.*

4. *Para cualesquiera $a, b \in G$, las ecuaciones $ax = b$ y $ya = b$ tienen ecuación y además es única: $x = a^{-1}b$ y $y = ba^{-1}$.*

5. *Si a es un elemento tal que $aa = a$, entonces $a = 1$.*

6. *Sea $n \geq 1$ y $a_1, \ldots, a_n$. Definimos:*

$$\prod_{i=1}^{1} a_i = a_1$$

$$\prod_{i=1}^{n} a_i = a_n \prod_{i=1}^{n-1} a_i$$

Proposición 2 (Propiedad asociativa generalizada)**.** *Sea $n \geq 2$, entonces para cada m con $1 \leq m < n$ tenemos*

$$\prod_{i=1}^{n} a_i = \prod_{i=1}^{m} a_i \prod_{i=m+1}^{n} a_i$$

Demostración. El caso inicial es la propiedad asociativa.

El caso general se demuestra por inducción. □

Proposición 3. *Para $n \geq 1$, tenemos que*

$$\left(\prod_{i=1}^{n} a_i\right)^{-1} = \prod_{i=1}^{n} a_{n+1-i}^{-1}$$

Demostración. Por inducción. El caso base es trivial. Veamos el caso $n+1$.

$$\prod^{n+1} a_i \prod^{n+1} a_{n+2-i}^{-1} = \prod^{n} a_i a_{n+1} a_{n+1}^{-1} \prod_{i=2}^{n+1} a_{n+2-i} = \prod^{n} a_i \prod_{i=1}^{n} a_{n+1-i} = 1$$

□

Definición 1.

$$a^n = \prod_{i=1}^{n} a$$

Proposición 4. *Se verifica las siguientes propiedades de las potencias:*

1. *Sean $r, s > 0$, se verifica*

$$a^r a^s = a^{r+s}$$

2. *Para todo $n \geq 1$ se verifica*

$$(a^n)^{-1} = (a^{-1})^n$$

Lo llamaremos a^{-n}.

3. *Para cualesquiera $r, s \in \mathbb{Z}$ se cumple:*

$$a^r a^s = a^{r+s}$$

$$(a^r)^s = a^{rs}$$