Apuntes de clase

José Antonio de la Rosa Cubero

Proposición 1. *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:*
$$a^r a^s = a^{r+s}$$
$$(a^r)^s = a^{rs}$$

Demostración. Probemos el último resultado.

$$a^{-r} a^{-s} = (a^{-1})^r (a^{-1})^s = (a^{-1})^{r+s} = a^{-r-s}$$

Para $r \geq s$:
$$a^r a^{-s} = a^{r-s} a^s a^{-s} = a^{r-s}$$

Y para $s > r$:
$$a^r a^{-s} =$$

$\square$

CUIDADO: a veces emplearemos la notación aditiva en lugar de la multiplicativa. Las potencias se escriben como múltiplos, $\prod$ pasa a ser $\sum$...

Proposición 2. *Sea G un conjunto no vacío tal que hay definida una operación.*

1. *Es asociativa.*

2. *Hay un neutro a la izquierda.*

3. *Cada elemento tiene un inverso a la derecha.*

Entonces G es un grupo.

Anillo: $(A, +, \cdot)$ es un grupo abeliano y con respeto al producto se verifica la asociatividad, existencia de elemento neutro y propiedad distributiva.

El anillo es conmutativo si el producto lo es.

Si A es un anillo, $A, +$ es un grupo abeliano y $A^{\times}, \cdot$ es un grupo, siendo $A^{\times} = \mathcal{U}(A) = \{u \in A : \exists u^{-1} \in A\}$. El grupo es abeliano si el anillo es conmutativo.

En el caso de los números complejos no nulos usaremos la notación módulo argumento.

Sea $\mathcal{M}_n(\mathbb{K})$ el anillo de matrices cuadradas de orden n sobre el cuerpo $\mathbb{K}$. Nos da lugar a dos grupos abelianos $(\mathcal{M}_n(\mathbb{K}))$.

$$GL_n(\mathbb{K}) := \mathcal{M}_n(\mathbb{K})^{\times} = \{B \in \mathcal{M}_n(\mathbb{K}) : \det B \neq 0\}$$

es un grupo no abeliano.

Si $\mathbb{K}$ es un cuerpo finito, $GL_n(\mathbb{K})$ es también finito.

Al número de elementos de un grupo se le llama orden del grupo. Lo denotaremos por $|G|$.

Si son pocos, se puede describir con la tabla de Cayley (las típicas tablas de sumas y productos).

$\mathbb{Z}_n = \mathbb{Z}/(n\mathbb{Z})$. Tenemos dos grupos: el de la suma y el del producto de las unidades.

$$\mathbb{Z}^{\times} = \{k \in \mathbb{Z}_n : \gcd(k, n) = 1\}$$

Donde además $|\mathbb{Z}_n^{*}| = \phi(n)$.

$\mu_n := \{z \in \mathbb{C}^{\times} : z^n = 1\}$ es el conjunto de las raíces n-ésimas de la unidad. Es un grupo abeliano.