# 0. CAMPOS

En este capítulo veremos resultados básicos de campos, así como algunos ejemplos. Para poder definir el concepto de campo, necesitamos primero saber que es una operación binaria sobre un conjunto $A$.

**Definición 0.1**
Sea $A$ un conjunto, una *operación binaria* en $A$ es una función

$$\mu : A \times A \to A$$

que asigna a cada pareja ordenada $(a_1, a_2) \in A \times A$ un único elemento de $A$ denotado $\mu(a_1, a_2)$.

**Ejemplos 0.1**
Los siguientes son ejemplos de operaciones binarias.

1. La suma y producto de números enteros (racionaeles, reales).
2. Sea $A$ un conjunto y $\mu : \mathcal{P}(A) \times \mathcal{P}(A) \to \mathcal{P}(A)$ la función definida como $\mu(B, C) = B \cap C$, donde $\mathcal{P}(A)$ denota al conjunto potencia de $A$.

Ahora que ya sabes lo que es una operación binaria, da otros ejemplos.

**Definición 0.2**
Un *campo* consiste de un conjunto $F$ y dos operaciones binarias en $F$

$$+ : F \times F \to F \quad \text{donde } +(a, b) := a + b$$

$$\star : F \times F \to F \quad \text{donde } \star(a, b) := a \star b$$

llamadas suma y producto respectivamente y que satisfacen las siguientes propiedades, llamadas **Axiomas de Campo**.

- S1. La suma es asociativa.
  $(a+b)+c = a+(b+c)$ para cada $a, b, c \in F$.

- S2. La suma es conmutativa.
  $a+b = b+a$ para cada $a, b \in F$.

- S3. Existencia de neutro aditivo.
  Existe $e \in F$ tal que $a+e = a = e+a$ para cada $a \in F$, el elemento $e$ se llama un neutro aditivo de $F$.

- S4. Existencia de inversos aditivos.
  Para cada $a \in F$ existe $a' \in F$ tal que $a+a' = e = a'+a$, el elemento $a'$ se llama un inverso aditivo de $a$.

- P1. El producto es asociativo.
  $a \star (b \star c) = (a \star b) \star c$ para cada $a, b, c \in F$.

- P2. El producto es conmutativo.
  $a \star b = b \star a$ para cada $a, b \in F$.

- P3. Existencia de neutro multiplicativo.
  Existe $u \in F$ tal que $u$ no es neutro aditivo y para cada $a \in F$, $a \star u = a = u \star a$, el elemento $u$ se llama un neutro multiplicativo de $F$.

- P4. Existencia de inversos multiplicativos.
  Para cada $a \in F$ tal que $a$ no es un neutro aditivo, existe $d \in F$ tal que $a \star d = u = d \star a$, el elemento $d$ se llama un inverso multiplicativo de $a$.

- D. Ley Distributiva.
  $a \star (b+c) = a \star b + a \star c$ para cada $a, b, c \in F$.

Observa que los axiomas S3 y P3 garantizan que en un campo, hay al menos un neutro aditivo y un neutro multiplicativo y que son distintos, asimismo, el axioma S4 nos dice que cada elemento del campo tiene al menos un inverso aditivo y el axioma P4 que cada elemento del campo que no es un neutro aditivo, tiene al menos un inverso multiplicativo. Nuestro siguiente objetivo es probar la unicidad de estos elementos.

**Nota**.
En lugar de escribir el producto como $a \star b$, omitimos el símbolo $\star$ y escribimos $ab$.

**Teorema 0.1** Leyes de Cancelación. Sea $F$ un campo.

1. Ley de la cancelación para la suma.
   Si a+b=a+c donde $a, b, c \in F$ entonces $b = c$.

2. Ley de la cancelación para el producto.
   Si $ab = ac$ donde $a, b, c \in F$ y $a$ no es un neutro aditivo, entonces $b = c$.

**demostración:**

1. Por S4, existe $a' \in F$ un inverso aditivo de $a$. Entonces, usando la asociatividad de la suma obtenemos

$$b = a' + (a + b) = a' + (a + c) = c$$

2. Por P4, existe $d \in F$ un inverso multiplicativo de $a$. Usando la asociatividad del producto obtenemos

$$b = d(ab) = d(ac) = c$$

**Teorema 0.2**
Sea $F$ un campo, entonces

1. $F$ tiene un único neutro aditivo.

2. $F$ tiene un único neutro multiplicativo.

demostración:

1. Supongamos que $e$ y $e'$ son neutros aditivos de $F$, entonces

$$e' = e + e' = e$$

2. Supongamos que $u$ y $u'$ son neutros multiplicativos de $F$, entonces

$$u' = uu' = u$$

Ahora que ya hemos probado que un campo tiene un único inverso aditivo y un único inverso multiplicativo, podemos asignarles un símbolo para representarlos. Denotamos por $0_F = 0$ al neutro aditivo de $F$ y lo llamamos el cero de $F$. Denotamos por $1_F = 1$ al neutro multiplicativo de $F$ y lo llamamos el uno de $F$.

Observemos que decir que un elemento $a$ de $F$ no es neutro aditivo es lo mismo que escribir $a \neq 0$.

**Teorema 0.3**
Sea $F$ un campo.

1. Cada elemento $a \in F$ tiene un único inverso aditivo.
2. Cada elemento $a \in F$, $a \neq 0$, tiene un único inverso multiplicativo.

**demostración:**

1. Sea $a \in F$ y supongamos que $a'$ y $a''$ son inversos aditivos de $a$, entonces

$$a' = a' + 0 = a' + (a + a'') = (a + a') + a'' = 0 + a'' = a''$$

2. Sea $a \in F$, $a \neq 0$ y supongamos que $d$ y $d'$ son inversos multiplicativos de $a$, entonces

$$d' = d'1 = d'(ad'') = (d'a)d'' = 1d'' = d''$$

**Nota**
Sea $a$ un elemento de un campo $F$, denotamos con el símbolo $-a$ al inverso aditivo de $a$, si $a \neq 0$ denotamos con el símbolo $a^{-1}$ al inverso multiplicativo de $a$.

**Teorema 0.4**
Sea $F$ un campo y $a, b, c \in F$. los siguientes enunciados son equivalentes

1. Si $ab = ac$ y $a \neq 0$ entonces $b = c$.
2. Si $ab = 0$ y $a \neq 0$ entonces $b = 0$

La demostración se deja como ejercicio al lector. A continuación veremos propiedades aritméticas de la suma y el producto en un campo.

**Teorema 0.5**
Sea $F$ un campo, entonces

1. $0_F a = 0_F$ para cada $a \in F$.
2. $-1_F a = -a$ para cada $a \in F$.
3. $-(-a) = a$ para cada $a \in F$.
4. $-(ab) = -a(b) = a(-b)$ para cada $a, b \in F$.

**demostración:**

1. Como $0_F$ es neutro aditivo y por la ley distributiva, tenemos que

$$0_F + 0_F a = 0_F a = (0_F + 0_F)a = 0_F a + 0_F a$$

   Por la ley de la cancelación para la suma, podemos concluir que $0_F a = 0_F$.

2. Debemos mostrar que $-1_F a$ es el inverso aditivo de $a$, así que por la unicidad del inverso aditivo de $a$, basta probar que $-1_F a + a = 0_F$. Por la ley distributiva obtenemos

$$-1_F a + a = -1_F a + 1_F a = (-1_F + 1_F)a = 0_F a = 0_F$$

3. Por la unicidad del inverso aditivo de $-a$, basta probar que $-a + a = 0_F$, pero esto es cierto ya que $-a$ es el inverso aditivo de $a$.

4. Probaremos que $-(ab) = -a(b)$, la otra igualdad se prueba de forma similar. Por la unicidad del inverso aditivo de $ab$, basta probar que $a(-b) + ab = 0_F$. Por la ley distributiva obtenemos

$$a(-b) + ab = a(-b + b) = a0_F = 0_F$$

**Teorema 0.6**
Sea $F$ un campo y $x, y, x_1, \ldots, x_n$ elementos de $F$ distintos de $0 = 0_F$, entonces

1. $xy \neq 0$ y $(xy)^{-1} = x^{-1}y^{-1}$.
2. $(x_1 x_2 \ldots x_n)^{-1} = x_1^{-1} x_2^{-1} \ldots x_n^{-1}$.
3. $(x^{-1})^{-1} = 1$
4. $1^{-1} = 1$; $(-1)^{-1} = -1$; $(-1)(-1) = 1$.

La demostración se deja como ejercicio al lector.

**Definición 0.3**
Sea $F$ un campo y $x \in F, x \neq 0$, definimos la $n$-ésima potencia de $x$ recursivamente

$$x^0 = 1, x^1 = x \text{ y para } n \geq 2, x^n = x^{n-1}x$$

Para cada $n \in \mathbb{N}$, definimos $x^{-n} = (x^{-1})^n$.

**Teorema 0.7**
Leyes de los exponentes.

1. $x^m x^n = x^{m+n}$ para cada $m, n \in \mathbb{Z}$.
2. $(x^m)^n = x^{mn}$ para cada $m, n \in \mathbb{Z}$.
3. $(xy)^m = x^m y^m$ para cada $m \in \mathbb{Z}$
4. $x^{-m} = (x^{-1})^m = (x^m)^{-1}$

**demostración:**
Probaremos el primer inciso, los otros 3 se dejan como ejercicio.

Si $m = 0$ y $n$ es cualquier número natural, entonces $x^0 x^n = 1x^n = x^n = x^{0+n}$. De forma análoga si $n = 0$ y $m$ es cualquier número natural. Si $m = 0 = n$ entonces $x^0 x^0 = 1$ y $x^{0+0} = x^0 = 1$.

Sea $m$ un número natural fijo, probaremos que para cualquier número natural $n$, se cumple que $x^m x^n = x^{m+n}$. Para ello, procedemos por inducción sobre $n$.

Base de la inducción: para $n = 1$ hay que probar que $x^m x^1 = x^{m+1}$. La igualdad anterior es cierta por definición de las potencias de $x$.

Hipótesis de inducción: supongamos que es cierto para $n$, es decir que $x^m x^n = x^{m+n}$, debemos probar que es cierto para $n + 1$, esto es, $x^m x^{n+1} = x^{m+(n+1)}$. Tenemos que

$$x^m x^{n+1} = x^m (x^n x^1) = (x^m x^n) x^1 = x^{m+n} x = x^{(m+n)+1} = x^{m+(n+1)}$$

donde la tercera igualdad es cierta por hipótesis de inducción.

Hasta aquí, hemos probado que para cada $m, n$ enteros no negativos, $x^m x^n = x^{m+n}$.
Por otro lado, para cada $m, n \in \mathbb{N}$,

$$x^{-m-n} = x^{-(m+n)} = (x^{-1})^{m+n} = (x^{-1})^m (x^{-1})^n = x^{-m} x^{-n}$$

En consecuencia, la igualdad es cierta para cada par de números enteros $m, n$.

En clase vimos que el conjunto de números racionales (reales, complejos) con la suma y producto de números racionales (reales, complejos) son campos. También

construímos un campo con dos elementos.

Finalizamos esta sección con otro ejemplo.
Sea $\mathbb{Q}(i) = \{x + iy \in \mathbb{C} | x, y \in \mathbb{Q}\}$ el conjunto de números complejos con coordenadas racionales. Prueba que $\mathbb{Q}(i)$ es un campo con la suma y producto de números complejos.