Campos

Definición 1. *Un campo es un conjunto F en el cual se definen dos operaciones binarias denotadas $+$ llamada suma, y $\cdot$ llamada multiplicación de modo que para cualquier par de x,y en F existen elementos únicos $x+y$, $x \cdot y$ en F que se comportan de acuerdo con los siguientes axiomas*

Axiomas de la suma

(A1) $\forall \ x, y \in \ F$ x+y=y+x — *Ley conmutativa para la suma*
(A2) $\forall \ x, y, z \in \ F$ x+(y+z)=(x+y)+z — *Ley asociativa para la suma*
(A3) $\exists\, 0 \in \ F$ *tal que* $x + 0 = x \ \ \forall\, x \in \ F$ — *Existencia de una identidad para la suma*
(A4) $\forall\, x \in \ F$ $\exists u \in \ F$ *tal que* $x + u = 0$ — *Existencia de inversos para la suma*

Axiomas de la multiplicación

(M1)$\forall \ x, y \in \ F$ x*y=y*x — Ley conmutativa para la suma
(M2) $\forall \ x, y, z \in \ F$ x*(y*z)=(x*y)*z — Ley asociativa para la multiplicación
(M3) $\exists\, 1 \in \ F$ tal que $x * 1 = x \ \ \forall\, x \in \ F$ — Existencia de una identidad para la multiplicación
(M4) $\forall\, x \in \ F$ $\exists u \in \ F$ tal que $x * u = 1$ — Existencia de inversos para la multiplicación

Axiomas de distribución

(D) $\forall \ x, y, z \in \ F$ x*(y+z)=(x*y)+(x*z) — Ley distributiva

Ejemplo Dado el conjunto $F = \{0, 1, 2, 3, 4\}$. Definimos la suma y la multiplicación

+	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

.	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

En este caso se satisfacen todos los axiomas y por tanto F es un campo

Ejemplo Dado el conjunto
$$F = \mathbb{R}^2 = \{(x, y) \mid x, y \ \in \mathbb{R}\}$$
y dos operaciones definidas como
$$Suma: \quad (x, y) + (u, v) = (x + u, y + v)$$
$$Producto: \quad (x, y) \cdot (u, v) = x \cdot u + y \cdot v$$
En este caso no se satisface M_0 pues
$$(x, y) \cdot (u, v) = x \cdot u + y \cdot v \notin F$$
por lo tanto F no es un campo

Consecuencias de los axiomas de campo

Teorema 1. *Ley de la cancelación En algún campo F, se satisface:*
(a) si $x+y=x+z$ entonces $y=x$
(b) si $xy=xz$ y $x\neq 0$, entonces $y=z$

Demostración. **(a)** Suponga que $y+z=z+x$. Entonces usando (A3) y (A4), $\exists\, u\in\ F$ tal que $x+u=0$, y $y=y+0=y+(x+u)=(y+x)+u=(z+x)+u=z+(x+u)=z+0=z\ \therefore\quad y=z$

(b) Tenemos que

$$x\neq 0\ \Rightarrow\ \exists\, u\ \in\ F\ \ni\ xu=ux=1$$

entonces

$$xy=xz\ \Rightarrow\ u(xy)=u(xz)\ \Rightarrow\ 1y=1z\ \Rightarrow\ y=z$$

□

Teorema 2. *Unicidad de los elementos identicos e inversos En algún campo F, se satisface:*
(a) En (A3) El neutro es único
(b) En (M3) El neutro es único
(c) En (A4) El elemento u es único
(d) En (M4) El elemento u es único

Demostración. **(a)** Suponga que 0 y $0'$ son elementos que satisfacen (A3). Entonces

$$\forall\, x\in\ F,\quad x+0=x,\quad y\ \ \forall\, x\in\ F,\ x+0'=x,\ \textit{entonces}\ 0=0+0'=0'+0=0'$$

$\therefore\ 0=0'$

(b) Suponga que 1 y $1'$ son elementos que satisfacen (A3). Entonces

$$\forall\, x\in\ F,\quad x\cdot 1=x,\quad y\ \ \forall\, x\in\ F,\ x\cdot 1'=x,\ \textit{entonces}\ 1=1\cdot 1'=1'\cdot 1=1'$$

$\therefore\ 1=1'$

(c) Sea $x\in F$. Suponga que u y v son elementos de F que satisfacen la propiedad (A4) entonces

$$x+u=0\ \ y\ \ x+v=0\ \Rightarrow\ x+u=x+v\ \Rightarrow\ u=v$$

(d) Sea $x\in F$. Suponga que u y u' son elementos de F que satisfacen la propiedad (M4) entonces

$$x\cdot u=1\ \ y\ \ x\cdot u'=1\ \Rightarrow\ u=u\cdot 1=u(x\cdot u')=(ux)\cdot u'=1\cdot u'=u'$$

□

En los teoremas anteriores vimos que los elementos neutros e inversos son únicos, usualmente para la suma denotamos al inverso aditivo de un elemento $x\in F$ como $u=-x\in F$ tal que $x+(-x)=0$.
En el caso de la multiplicación se tiene $x\neq 0\ \Rightarrow\ u=\dfrac{1}{x}=x^{-1}\in F$ tal que $x\cdot x^{-1}=1$