Números Enteros $\mathbb{Z}$

Definición 1. *El conjunto de números enteros de un campo ordenado F es el conjunto*

$$\mathbb{Z} = \{x \in F \mid x \in \mathbb{N}, \quad ó \quad -x \in \mathbb{N} \quad ó \quad x = 0\}$$

Este conjunto consta de los números naturales, e incluimos sus inversos aditivos y el cero. Los elementos no tienen un inverso multiplicativo, por lo que, $\mathbb{Z}$ no es un campo.
Vamos a comprobar que este conjunto es cerrado bajo la suma y la multiplicación.

Cerradura de la suma en $\mathbb{Z}$ Sean $x, y \in \mathbb{Z}$. Tenemos los siguientes casos

1. Si $x \in \mathbb{N}$ y $y \in \mathbb{N}$ entonces por la cerradura de $\mathbb{N}$ se tiene que $x + y \in \mathbb{Z}$
2. Si $x \in \mathbb{N}$ y $y \notin \mathbb{N}$ entonces puede ocurrir alguna de las siguientes
   a) $-y \in \mathbb{N}$ y $-y < x$ lo cual implicaría que $0 < x + y \in \mathbb{N}$
   b) $-y \in \mathbb{N}$ y $-y > x$ lo cual implicaría que $0 > x + y \notin \mathbb{N}$
   c) $-y \in \mathbb{N}$ y $-y = x$ lo cual implicaría que $0 = x + y$

   En cualquier caso $x + y \in \mathbb{Z}$
3. Si $x \notin \mathbb{N}$ y $y \notin \mathbb{N}$ entonces $-x \in \mathbb{N}$ y $-y \in \mathbb{N}$. Por lo que $-(x+y) \in \mathbb{N}$ en cuyo caso $(x+y) \notin \mathbb{N}$

concluimos entonces que si $x, y \in \mathbb{Z}$ entonces $(x + y) \in \mathbb{Z}$

Cerradura de la multiplicacióin en $\mathbb{Z}$ Sean $x, y \in \mathbb{Z}$. Tenemos los siguientes casos

1. Si $x \in \mathbb{N}$ y $y \in \mathbb{N}$ entonces por la cerradura de $\mathbb{N}$ se tiene que $x \cdot y \in \mathbb{N}$
2. Si $x \in \mathbb{N}$ y $y \notin \mathbb{N}$ entonces $x \cdot y \notin \mathbb{N}$
3. Si $x \notin \mathbb{N}$ y $y \notin \mathbb{N}$ entonces $x \cdot y \in \mathbb{N}$
4. Si $x = 0$ y $y = 0$ entonces $x \cdot y = 0$

concluimos entonces que si $x, y \in \mathbb{Z}$ entonces $(x \cdot y) \in \mathbb{Z}$

Definición 2. *Definimos $a^n, \ a \neq 0, \ \forall \ n \in \mathbb{Z}$ como:*

1. $a^0 = 1$
2. $a^n = \underbrace{a \cdot a \cdots a}_{n-veces}$
3. $a^{-n} = \dfrac{1}{a^n}$

Ejercicio Probar que con la definición anterior $\forall\ m, n \in \mathbb{Z}$

1. $a^m a^n = a^{m+n}$
2. $(a^m)^n = a^{mn}$
3. $(ab)^n = a^n b^n$
4. $\dfrac{a^m}{a^n} = a^{m-n}$

Solución Tenemos que

1. $a^{n+m} = \underbrace{a \cdot a \cdots a}_{n+m\ veces} = (\underbrace{a \cdot a \cdots a}_{n\ veces})(\underbrace{a \cdot a \cdots a}_{m\ veces}) = a^n a^m$
2. $(a^n)^m = (\underbrace{a \cdot a \cdots a}_{n\ veces})^m = \underbrace{(\underbrace{a \cdot a \cdots a}_{n\ veces}) \cdot (\underbrace{a \cdot a \cdots a}_{n\ veces}) \cdots (\underbrace{a \cdot a \cdots a}_{n\ veces})}_{m\ veces} = \underbrace{a \cdot a \cdots a}_{n \cdot m\ veces} = a^{nm}$
3. $(ab)^n = \underbrace{ab \cdot ab \cdots ab}_{n\ veces} = (\underbrace{a \cdot a \cdots a}_{n\ veces}) \cdot (\underbrace{b \cdot b \cdots b}_{n\ veces}) = a^n b^n$
4. $\dfrac{a^n}{a^m} = \dfrac{\overbrace{a \cdot a \cdots a}^{n\ veces}}{\underbrace{a \cdot a \cdots a}_{m\ veces}}$

   Tenemos dos casos

   a) si $n > m$ entonces
   $$\frac{a^n}{a^m} = \frac{\overbrace{a \cdot a \cdots a}^{m\ veces}\overbrace{a \cdot a \cdots a}^{n-m\ veces}}{\underbrace{a \cdot a \cdots a}_{m\ veces}} = \overbrace{a \cdot a \cdots a}^{n-m\ veces}$$

   b) si $n < m$ entonces
   $$\frac{a^n}{a^m} = \frac{\overbrace{a \cdot a \cdots a}^{n\ veces}}{\underbrace{a \cdot a \cdots a}_{n\ veces}\underbrace{a \cdot a \cdots a}_{m-n\ veces}} = \frac{1}{\underbrace{a \cdot a \cdots a}_{n-m\ veces}} = \frac{1}{a^{m-n}} = a^{-(m-n)} = a^{-m+n} = a^{n-m}$$

Números Racionales $\mathbb{Q}$

Definición 3. *El conjunto de números racionales de un campo ordenado F es el conjunto*

$$\mathbb{Q} = \left\{ x \in F \mid \exists\ m.n \in \mathbb{Z} \ \ tal \ \ que \ \ n \neq 0 \quad y \quad x = \frac{m}{n} \right\}$$

Es decir, los números racionales de F son cocientes de enteros de F, comúnmente llamados fracciones. Una de las características más significativas de los números racionales de F es que forman un campo dentro del campo F; es decir, un subcampo de F. Esto se resume en el siguiente teorema

Teorema 1. *Para cualquier campo F con el subconjunto positivo P, el conjunto del conjunto $\mathbb{Q}$ de elementos racionales de F es un campo ordenado relativo a las mismas operaciones + y $\cdot$ utilizadas en F y el conjunto positivo $P' = P \cap \mathbb{Q}$ ($\mathbb{Q}$ se llamará el subcampo racional de F)*

Demostración. Sea F un campo ordenado. Debemos mostrar que $\mathbb{Q}$, con las mismas operaciones + y $\cdot$ usadas en F y el P' de positivos, satisface los axiomas $(A_0)-(A_4)$, $(M_0)-(M_4)$ y $(O_1)-(O_3)$

(A_0) Sean $x, y \in \mathbb{Q}$. Entonces existen $m, n, m', n' \in \mathbb{Z}$ tal que $n, n' \neq 0$, $x = \dfrac{m}{n}$ y $y = \dfrac{m'}{n'}$. Así

$$\begin{aligned}
x + y &= \frac{m}{n} + \frac{m'}{n'} \\
&= m \cdot n^{-1} + m' \cdot n'^{-1} \\
&= m \cdot n^{-1} \cdot 1 + m' \cdot n'^{-1} \cdot 1 \\
&= m \cdot n^{-1} \cdot (n' \cdot n'^{-1}) + m' \cdot n'^{-1} \cdot (n \cdot n^{-1}) \\
&= m \cdot n' \cdot (n^{-1} \cdot n'^{-1}) + m' \cdot n \cdot (n'^{-1} \cdot n^{-1}) \\
&= m \cdot n' \cdot (n \cdot n')^{-1} + m' \cdot n \cdot (n \cdot n')^{-1} \\
&= (mn' + m'n) \cdot (n \cdot n')^{-1} \\
&= \frac{mn' + m'n}{n \cdot n'}
\end{aligned}$$

(A_1) propiedad hereditaria de F

(A_2) propiedad hereditaria de F

(A_3) se tiene que $0 \in \mathbb{Q}$ pues $0 = \dfrac{0}{1}$

(A_4) Sea $x \in \mathbb{Q}$. Entonces existen $m, n \in \mathbb{Z}$ tal que $n \neq 0$ y $x = \dfrac{m}{n}$ y $-x = \dfrac{-m}{n}$

(M_0) Sean $x, y \in \mathbb{Q}$. Entonces existen $m, n, m', n' \in \mathbb{Z}$ tal que $n, n' \neq 0$, $x = \dfrac{m}{n}$ y $y = \dfrac{m'}{n'}$. Así

$$\begin{aligned}
x \cdot y &= \frac{m}{n} \cdot \frac{m'}{n'} \\
&= m \cdot n^{-1} \cdot m' \cdot n'^{-1} \\
&= m \cdot m' \cdot (n^{-1} \cdot n'^{-1}) \\
&= m \cdot m' \cdot (n \cdot n')^{-1} \\
&= \frac{mm'}{nn'}
\end{aligned}$$

(M_1) propiedad hereditaria de F
(M_2) propiedad hereditaria de F
(M_3) se tiene que $1 \in' mathbbQ$ pues $1 = \frac{1}{1}$
(M_4) Sea $x \in \mathbb{Q}$ tal que $x \neq 0$. Entonces existen $m, n \in \mathbb{Z}$ tal que $n \neq 0$ y $x = \frac{m}{n}$ y $x^{-1} = \frac{n}{m}$ $\square$

Sean $a, b, c \in \mathbb{Q}$, entonces

A_0 $a + b \in \mathbb{Q}$ (Cerradura)

$$a = \frac{m}{n}, \quad b = \frac{m'}{n'} \quad \Rightarrow \quad a + b = \frac{m}{n} + \frac{m'}{n'} = \frac{mn' + m'n}{nn'} \in \mathbb{Q}$$

por las propiedades de los enteros
A_1 $a + b = b + a$ (Conmutatividad) es hereditaria de F
A_2 $a + (b + c) = (a + b) + c \in \mathbb{Q}$ (Asociatividad) es hereditaria de F
A_3 $\exists 0 \in \mathbb{Q}$ tal que $a + 0 = 0 + a = a$ (Neutro Aditivo)

$$a = \frac{m}{n}, \quad 0 = \frac{0}{1} \quad \Rightarrow \quad a + 0 = \frac{m}{n} + \frac{0}{1} = \frac{m \cdot 1 + n \cdot 0}{n \cdot 1} = \frac{m}{n} = a$$

A_4 Dado a $\exists - a \in \mathbb{Q}$ tal que $a + (-a) = 0$ (Inverso Aditivo)

$$a = \frac{m}{n}, \quad b = \frac{-m}{n} \quad \Rightarrow \quad a + b = \frac{m}{n} + \frac{-m}{n} = \frac{mn + (-mn)}{nn} = \frac{0}{nn} = 0 \in \mathbb{Q}$$

M_0 $a \cdot b = ab \in \mathbb{Q}$ (Cerradura)

$$a = \frac{m}{n}, \quad b = \frac{m'}{n'} \quad \Rightarrow \quad ab = \frac{m}{n} \cdot \frac{m'}{n'} = \frac{mm'}{nn'} \in \mathbb{Q}$$

por las propiedades de los enteros
M_1 $ab = ba \in \mathbb{Q}$ (Conmutatividad) es hereditaria de F
M_2 $(ab)c = a(bc) \in \mathbb{Q}$ (Asociatividad) es hereditaria de F
M_3 $\exists 1 \in \mathbb{Q}$ tal que $a1 = 1a = 1$ (Neutro Multiplicativo)

$$a = \frac{m}{n}, \quad 1 = \frac{1}{1} \quad \Rightarrow \quad a \cdot 1 = \frac{m}{n} \cdot \frac{1}{1} = \frac{m \cdot 1}{n \cdot 1} = \frac{m}{n} = a$$

M_4 Dado a $\neq 0 \exists a^{-1} \in \mathbb{Q}$ tal que $aa^{-1} = a^{-1}a = 1$ (Inverso Multiplicativo)

$$\forall\, x \in \mathbb{Q} \quad x = \frac{m}{n}, \quad \exists\, x^{-1} \in \mathbb{Q}, \quad x^{-1} = \frac{b}{a} \quad tal \quad que \quad x \cdot x^{-1} = \frac{a}{b} \cdot \frac{b}{a} = 1$$

Distrbutividad: $a(b + c) = ab + ac$ es hereditaria de F
Orden.
O_1, O_2 y O_3 son hereditarias de F
En conclusión $\mathbb{Q}$ si es un campo ordenado.
Si un campo ordenado contiene un elemento que no es un número racional (según nuestra definición), dicho elemento se llama elemento irracional de f.

Observación Se tiene que $\mathbb{N} \subset \mathbb{Q}$ y también $\mathbb{Z} \subset \mathbb{Q}$

Comprobaremos que existen elementos en F, que no estan, en $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$

Teorema 2. *No existe $x \in \mathbb{Q}$ tal que $x^2 = 2$*

Demostración. Por contradicción. Supongamos que $\exists\ x \in \mathbb{Q}$ tal que $x^2 = 2$. Entonces existen $m, n \in \mathbb{Z}$ tal que $n \neq 0$ y $x = \dfrac{m}{n}$.
Sin perdida de generalidad supondremos que m y n no tienen factores en común. Tenemos entonces

$$x^2 = 2 \;\Rightarrow\; \left(\frac{m}{n}\right)^2 = 2 \;\Rightarrow\; m^2 = 2n^2$$

Al ser m^2 divisible entre 2 se tiene que existe $k \in \mathbb{Z}$ tal que $m = 2k$. Por lo que

$$m^2 = 2n^2 \;\Rightarrow\; (2k)^2 = 2n^2 \;\Rightarrow\; 4k^2 = 2n^2 \;\Rightarrow\; 2k^2 = n^2$$

En la última igualdad observamos que n^2 es divisible por 2, por lo que, existe $k' \in \mathbb{Z}$ tal que $n = 2k'$. Esto es tanto el numerador como el denominador son ambos divisibles por 2 (esto es una contradicción). Por lo tanto $\nexists\ x \in \mathbb{Q}$ tal que $x^2 = 2$. □

En la prueba anterior usamos el lema

Lema 1. *Sea $n \in \mathbb{Z}$. Si n^2 es divisible por 2, entonces n es divisible por 2*

Demostración. Sea $n \in \mathbb{Z}$. Tal que n no es divisible por 2, esto implica que existe $k \in \mathbb{Z}$ tal que $n = 2k+1$ y por tanto

$$n = 2k + 1 \;\Rightarrow\; n^2 = 4k^2 + 4k + 1 \;\Rightarrow\; n^2 = 2(2k^2 + k) + 1$$

por lo tanto n^2 no es divisible por 2 □