AMPLIACIÓN DE MATEMÁTICAS

SUBCUERPOS.

Ejemplos de cuerpos que ya hemos estudiado son los siguientes.

Ejemplos 1. *(**de Cuerpos**).*

- $\mathbb{Q} \nsubseteq \mathbb{R} \nsubseteq \mathbb{C}$.
- *Si p es primo $(\mathbb{Z}_p, +, \times)$ es un cuerpo.*
- *Si $\mathbb{F}$ es un cuerpo y $f \in \mathbb{F}[x]$ es un polinomio irreducible del anillo de polinomios con coeficientes en $\mathbb{F}$, entonces el anillo cociente $\mathbb{F}[x]/f$ es un cuerpo y $\mathbb{F} \subset \mathbb{F}[x]/f$.*
- *Si $(\mathbb{A}, +, \times)$ es un dominio de integridad, su cuerpo de fracciones*

$$\mathbb{A}(x) = \{\frac{p}{q} \ : \ p, q \in \mathbb{A} \ y \ q \neq 0 \ \}$$

es un cuerpo tal que $\mathbb{A} \subset \mathbb{A}(x)$ (identificando p con $\frac{p}{1}$ para todo $p \in \mathbb{A}$).

La definición de **subcuerpo** es análoga a la de subgrupo, subanillo o subespacio vectorial.

Definición 1. *(**Extensiones de Cuerpos**).*

a: *Un subconjunto $U \subset \mathbb{F}$ de un cuerpo $\mathbb{F}$ se llama **subcuerpo** del cuerpo $\mathbb{F}$ si $(U, +, \times)$, con las misma operaciomes de $\mathbb{F}$, es a su vez un cuerpo.*

b: *Si $U \neq \mathbb{F}$ y U es un subcuerpo de $\mathbb{F}$, se dice que es un subcuerpo **propio.***

c: *$(\mathbb{F}, +, \times)$ se llama un cuerpo de **extensión** del subcuerpo $(U, +, \times)$.*

d: *Un cuerpo se llama **primo** si no tiene subcuerpos propios.*

Teorema 1. *Salvo isomorfismo, los únicos cuerpos primos distintos que existen son: $\mathbb{Q}$ y $\mathbb{Z}_p$ con p primo.*

Demostración: Sea $\mathbb{P}$ un cuerpo primo y tomamos $1 \in \mathbb{P}$. Consideramos la aplicación

$$\begin{array}{rccl} \psi & : & \mathbb{Z} & \to & \mathbb{P} \\ & & m & \to & \psi(m) = 1+1+....{}_{m-\text{veces}}..+1 \text{ ó } -1-1-....{}_{-m-\text{veces}}..-1. \end{array}$$

ψ es un homomorfismo de anillos. LLamamos $C = Img\psi$. C es claramente un dominio de integridad. Ahora

- Si el núcleo de la aplicación $ker\psi = \{0\}$, entonces ψ es un isomorfismo sobre la imagen C. Así el cuerpo de fracciones sobre C (ver la definición de cuerpo de fracciones en la Teoría de Anillos) es el menor cuerpo que contiene a C, es decir en nuestro caso a $\mathbb{Z}$. Luego este cuerpo es el cuerpo de los números racionales

  $$\mathbb{Q} \subseteq \mathbb{P}.$$

  Como $\mathbb{P}$ es primo se sigue que $\mathbb{Q} = \mathbb{P}$.
- Si $ker\psi \neq \{0\}$, entonces existe $k \in \mathbb{N}$, con $k > 1$, de modo que

  $$ker\psi = k\mathbb{Z} \qquad (\text{ideal de } \mathbb{Z}).$$

  Claro, sea

  $$A = \{\, k > 1 \;:\; k \times 1 = 0 \,\} \subset \mathbb{N}.$$

  Si $ker\psi \neq \{0\}$, entonces A es no vacío y existe $k = \text{mín}\, A$. Para cualquier otro $k' \in A$, se tiene que

  $$k' = qk + r \qquad \text{con} \qquad 0 \leq r < k.$$

  Así

  $$0 = k' \times 1 - (qk) \times 1 = r \times 1$$

  Así $r \in A$, y si $r > 1$, esto contradice la elección de k. Por tanto $r = 0$ y así $k|k'$. Ahora por el Teorema de Isomorfía de Anillos (ver el Tema de Teoría de Anillos)

  $$\mathbb{Z}_k = \mathbb{Z}/k\mathbb{Z} \simeq C,$$

  es decir, C es isomorfo a un anillo cociente $\mathbb{Z}_k$. Como C es un dominio de integridad, y por tanto $\mathbb{Z}_k$ también. Esto solo es posible si k es primo y por tanto $\mathbb{Z}_k$ es un cuerpo. Ahora tenemos que $\mathbb{Z}_k$ es un subcuerpo de $\mathbb{P}$ y como $\mathbb{P}$ es primo no queda mas remedio que $\mathbb{Z}_k = \mathbb{P}$. Observemos, además, que en este caso $Char.\mathbb{P} = k$ $\square$

Observación 1. *Si en la prueba anterior nos olvidamos de que el cuerpo* $\mathbb{F}$ *es primo, podemos observar que en ella se prueba que*

- *si* $Char.\mathbb{F} = 0$, *entonces* $\mathbb{Q}$ *es un subcuerpo de* $\mathbb{F}$,
- *y si* $Char.\mathbb{F} = k$, *entonces* $\mathbb{Z}_k$ *es un subcuerpo de* $\mathbb{F}$.

Corolario 1. *Si* $\mathbb{P}$ *es un cuerpo primo, entonces*

- *si* $Char.\mathbb{P} = 0$, *entonces* $\mathbb{Q}$ *es un isomorfo a* $\mathbb{P}$,
- *y si* $Char.\mathbb{P} = k$, *entonces* $\mathbb{Z}_k$ *es isomorfo a* $\mathbb{P}$.

Ejemplo 1. *Un cuerpo* $\mathbb{F}$ *con característica* $p \in \mathbb{N}$, *finita, no tiene por que ser finito.*

Sea $\mathbb{Z}_p$, con p primo. Así $\mathbb{Z}_p$ es un cuerpo con característica p. Si consideramos $\mathbb{Z}_p[x]$ es un dominio de integridad con característica p. Si considereramos su cuerpo de fracciones, éste será infinito como el anillo de polinomios y como éste tendrá característica igual a p $\square$.

Observación 2. *Si* $\mathbb{F}$ *es un* ***subcuerpo*** *de* $\mathbb{K}$ *o equivalentemente si* $\mathbb{K}$ *es una* ***extensión de cuerpo*** *de* $\mathbb{F}$, *entonces* $\mathbb{K}$ *es un espacio vectorial con respecto al cuerpo* $\mathbb{F}$.

En efecto, si consideramos en $\mathbb{K}$ su **suma** y para todo $r \in \mathbb{F}$ y para todo $a \in \mathbb{K}$ $r \times a$ el producto de ambos en $\mathbb{K}$ lo consideramos un **producto por escalares**, es fácil ver que efectivamente que $\mathbb{K}$ es un espacio vectorial con respecto al cuerpo $\mathbb{F}$ $\square$

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain
E-mail address: Cesar_Ruiz@mat.ucm.es