AMPLIACIÓN DE MATEMÁTICAS

CONGRUENCIAS SOBRE ANILLOS.

Ejemplo 1. *En $(\mathbb{Z}, +, \times)$, el subconjunto de los multiplos de n, $n\mathbb{Z}$, genera una relación de equivalencia*

$$k_1 \sim_{n\mathbb{Z}} k_2 \qquad \Leftrightarrow \qquad k_1 - k_2 \in n\mathbb{Z} \qquad \Leftrightarrow \qquad k_1 \equiv k_2 \ \textit{mód}\ n.$$

Las congruencias "normales". Vimos que el conjunto cociente

$$(\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n, +, \times)$$

con la suma y producto en congruencias forma de nuevo un anillo y en algunos casos un cuerpo (cuando n es primo).

¿Y que son las **congruencias** en general?

Definición 1. *Sea $(\mathbb{A}+, \times)$ un anillo. Una relación de equivalencia $\sim$ sobre $\mathbb{A}$ se dice que es una* ***congruencia*** *si para todo $a, a', b, b' \in \mathbb{A}$ con $a \sim a'$ y $b \sim b'$ se tiene que*

$$\begin{array}{rcl} a+b & \sim & a'+b' \\ ab & \sim & a'b'. \end{array}$$

Hay una relación natural entre congruencia e ideales (en el caso de Grupos con los subgrupos normales).

Teorema 1. *Sean $(\mathbb{A}, +, \times)$ un anillo y $\sim$ una congruencia sobre $\mathbb{A}$.*

- **a:** *Sea $I = [0]_\sim$ la clase del cero respecto de la congruencia $\sim$. I como subconjunto de $(\mathbb{A}, +, \times)$ es un* ***ideal****.*
- **b:** *Sea I un ideal del anillo. La relación sobre $\mathbb{A}$ definida por*

$$a \sim_I a' \qquad \Leftrightarrow \qquad a - a' \in I$$

es una ***congruencia****. En este caso $[0]_{\sim_I} = I$.*

Demostración:

a: Sean $s, s' \in I$ y sea $a \in \mathbb{A}$. Ahora, usando que $\sim$ es una congruencia,

$$[0] = [s' - s'] = [s'] + [-s'] = [0] + [-s'] \Rightarrow [-s'] = [0].$$

Luego

$$[s - s'] = [0] \qquad \text{y} \qquad [ss'] = [0] \Rightarrow s - s', ss' \in I.$$

Así I es un subanillo. Por otro lado

$$[sa] = [0a] = [0] \Rightarrow sa \in I.$$

Concluimos por tanto que I es un ideal.

b: Que $\sim_I$ es una relación de equivalencia y más una congruencia se ve igual que en el caso de $I = n\mathbb{Z}$ en $\mathbb{Z}$. Por último, $s \sim_I 0$ si y solo si $s \in I$. Por tanto, $[0]_{\sim_I} = I$ □

Definición 2. *Sean* $(\mathbb{A}, +, \times)$ *un anillo y* $\sim$ *una congruencia sobre* $\mathbb{A}$. *Sea el ideal* $I = [0]_\sim$. *Al conjunto cociente respecto de la relación le denotamos por*

$$\mathbb{A}/\sim = \mathbb{A}/\sim_I = \mathbb{A}/I.$$

Sobre el conjunto cociente definimos dos operaciones; así para todo $[a], [b] \in \mathbb{A}/I$

- ***la suma:*** $[a] + [b] = [a + b]$
- ***el producto:*** $[a] \times [b] = [ab]$.

Teorema 2. $(\mathbb{A}/I, +, \times)$ *es un anillo. Se denomina* ***anillo cociente****.*

Demostración: Es la misma que la que vimos al construir $(\mathbb{Z}_n, +, \times)$. Las operaciones están bien definidas por la definición de congruencia. Así las propiedades de anillo pasan a las operaciones del conjunto cociente. La clase [0]=I es el elemento neutro de la suma. $-[s] = [-s]$. Si $\mathbb{A}$ es conmutativo también lo es el cociente $\mathbb{A}/I$. Si existe $1 \in \mathbb{A}$ el elemento neutro del producto, [1] lo es del producto en congruencias □

La importancia de la construcción del anillo cociente es que en ciertas condiciones llegamos a construir hasta un cuerpo. Recordemos el caso "habitual".

Ejemplo 2. *$\mathbb{Z}$ es un dominio de integridad. Sus ideales son $n\mathbb{Z}$ ($n \geq 2$), todos ellos ideales principales. Vimos que*

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$$

y que este anillo cociente es un cuerpo si y solo si

$$n \text{ es primo} \qquad \Leftrightarrow \qquad n\mathbb{Z} \text{ es un ideal maximal.}$$

Teorema 3. *Sea $(\mathbb{A}, +, \times)$ un anillo conmutativo y con unidad. Sea I un ideal de $\mathbb{A}$. Entonces I es un ideal maximal si y solo si el anillo cociente $\mathbb{A}/I$ es un cuerpo.*

Demostración: $(\mathbb{A}/I, +, \times)$ es un anillo conmutativo con unidad.

Si I es un **ideal maximal** hay que probar que para todo $a \in \mathbb{A}/I$ existe su inverso a^{-1}. Para ello tomemos el ideal I' generado por $I \bigcup \{a\}$. Por un lado $I' = \mathbb{A}$ ya que I es maximal. Por otro veamos que

$$I' = \{ s + ra \ : \ s \in I \text{ y } r \in \mathbb{A} \}.$$

Claro, el conjunto entre llaves es fácil ver que es un ideal y también que está incluido en I'. Por tanto se dá la igualdad.

Ahora $1 \in \mathbb{A} = I'$, y así existen $s_0 \in I$ y $r_0 \in \mathbb{A}$ de modo que

$$[1] = [s_0 + r_0 a] = [s_0] + [r_0][a] = [0] + [r_0][a] = [r_0][a],$$

por tanto $a^{-1} = [r_0]$.

Si suponemos ahora que $(\mathbb{A}/I, +, \times)$ es un **cuerpo**, para todo $a \in \mathbb{A}^*$ existe $r \in \mathbb{A}$ de modo que

$$[r][a] = [ra] = [1]$$

por lo tanto ra y 1 están relacionados

$$1 - ra \in I.$$

Si I' es otro ideal que contiene a I, entonces para todo $a \in I' \backslash I$ se tiene que $1 - ar \in I \subset I'$ y, como $a \in I'$, se sigue que $1 \in I'$. Por tanto, $I' = \mathbb{A}$. Luego I es un ideal maximal $\square$

Ejemplo 3. *Si $\mathbb{F}$ es un cuerpo, $\mathbb{F}[x]$ es un dominio de integridad. Veremos que sus ideales son de la forma (p) ($p \in \mathbb{F}[x]$), todos ellos ideales principales. Los anillos cocientes*

$$\mathbb{F}[x]/(p)$$

son un cuerpo si y solo si (p) *es un ideal maximal. Y veremos que esto es equivalente a que el polinomio* p *sea irreducible (que no sea divisible por otro polinomio de menor grado).*

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain

E-mail address: Cesar_Ruiz@mat.ucm.es