AMPLIACIÓN DE MATEMÁTICAS

SUBANILLOS E IDEALES.

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

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

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).*

Observación 1. *Observemos que* $(n\mathbb{Z}, +, \times)$ *también es un anillo y que para todo* $m \in n\mathbb{Z}$ *y para todo* $r \in \mathbb{Z}$ *se tiene que* $r \times m \in n\mathbb{Z}$*.*

Todo lo anterior nos sugiere la noción abstracta de **ideal** con la cuál se pueden construir **anillos cocientes** y en algunos casos **cuerpos** (este último caso es él que nos interesa).

Definición 1. *Sea* $(\mathbb{A}, +, \times)$ *un anillo.*

- **A:** *Un subconjunto* $S \subseteq \mathbb{A}$ *se llama* ***subanillo*** *si* S *con las operaciones del anillo,* $(S, +, \times)$*, es de nuevo un anillo.*
- **B:** *Un subconjunto* $I \subseteq \mathbb{A}$ *es un* ***ideal*** *si* $(I, +, \times)$*, es un subanillo de* $\mathbb{A}$ *y además para todo* $s \in I$ *y para todo* $a \in \mathbb{A}$ *se tiene que*

$$as \in I \qquad y \qquad sa \in I.$$

Observación 2. **A:** $S \subseteq (\mathbb{A}, +, \times)$ *es un subanillo si y solo si para todo* $s, s' \in S$ *se tiene que*

$$s - s' \in S \qquad y \qquad s \times s' \in S.$$

B: $I \subseteq (\mathbb{A}, +, \times)$ *es un ideal si y solo si para todo* $s, s' \in I$ *y para todo* $a \in \mathbb{A}$ *se tiene que*

$$s - s' \in I \qquad y \qquad sa, as \in I.$$

Demostración:

Claro, la condición $s - s' \in S$ (o $s - s' \in I$) nos dice que $(S, +)$ (o (I,+)) es un subgrupo de $\mathbb{A}$. La segunda condición nos dice que el producto es una operación cerrada en S. En **B:** además se verifica la condición adicional para ser ideal $\square$

A diferencia del caso de los Grupos, no nos van a interesar los subanillos, salvo para definir la estructura que nos interesa: la de **Ideal**.

Ejemplo 2. *Sea $I = \{0, 2, 4, 6, 8\} \subset \mathbb{Z}_{10}$. Vemos que I es un ideal.*

Para todo $s, s' \in I$, $s = 2k$ y $s' = 2k'$, se tiene que

$$s - s' = 2(k - k') \in I$$

(entendiendo que las operaciones las hacemos en congruencias). Además si $a \in \mathbb{Z}_{10}$, se tiene que $as = a2k \in I$. Por tanto $(I, +, \times)$ es un subanillo conmutativo (sin unidad, pero integro, ver tabla).

$\times$	0	2	4	6	8
0	0	0	0	0	0
2	0	4	8	2	6
4	0	8	6	4	2
6	0	2	4	6	8
8	0	6	4	8	4

Aún más, $(I, +, \times)$ es un Ideal $\square$

Ejemplos 1.
1. *$n\mathbb{Z} \subset \mathbb{Z}$ es un ideal (aunque como anillo no tiene unidad).*
2. *$\mathbb{Z} \subset \mathbb{Q}$ es un subanillo, pero claramente no es un ideal.*

Observación 3.
1. *Si $\mathbb{A}$ es un anillo e I es un ideal suyo de modo que $1 \in I$, entonces $I = \mathbb{A}$.*
2. *Los únicos ideales de un cuerpo son $\{0\}$ y el total.*
3. *La intersección de ideales es de nuevo un ideal.*

Esta última propiedad nos da pie, como en el caso de Grupos, a definir el ideal generado por un trozo del anillo $\mathbb{A}$.

Definición 2. *Sea $(\mathbb{A}, +, \times)$ un anillo y sea $A \subseteq \mathbb{A}$ un subconjunto.*

a: *Se llama ideal generado por A al ideal*

$$I = \bigcap_{A \subseteq I',\ I' \text{ ideal de } \mathbb{A}} I' =_{notación} (A)$$

b: *Sea $a \in \mathbb{A}$, al ideal generado por a, (a), se le llama **ideal principal**.*

c: *Un anillo $\mathbb{A}$, dominio de integridad, se llama* ***dominio de ideales principales*** *si todos sus ideales son principales.*

Observación 4. *Si $\mathbb{A}$ es un anillo* ***conmutativo****, entonces para $a \in \mathbb{A}$ se tiene que*

$$(a) = a\mathbb{A} = \{ar \ : \ r \in \mathbb{A} \ \}.$$

Ejemplos 2.

- *Sea $1 \in \mathbb{A}$, la unidad respecto a la multiplicación. Entonces $(1) = \mathbb{A}$.*
- *$n\mathbb{Z} = (n)$. Así $n\mathbb{Z}$ es un ideal principal de $\mathbb{Z}$.*
- *Otros ejemplos interesantes los veremos al estudiar polinomios.*

Proposición 1. **a:** *$\mathbb{Z}$ es un dominio de ideales principales.*

b: *Si $\mathbb{F}$ es un cuerpo, entonces el anillo de los polinomios con coeficientes en $\mathbb{F}$, $\mathbb{F}[x]$, es un anillo de ideales principales.*

Demostración:

b: Esta prueba es como la de la parte **a)**, a falta de ver todas las semejanzas que hay entre los enteros y los conjuntos de polinomios en lo que a divisibilidad se refiere. (La veremos más adelante).

a: Sea $I \subset \mathbb{Z}$ un ideal. Para todo $r, s \in I$, por el Lema de Bezout, existen $u, v \in \mathbb{Z}$, de modo que

$$d = m.c.d.(n, m) = ur + vs \in I \qquad \Rightarrow \qquad d\mathbb{Z} \subseteq I.$$

Como I es numerable, podemos escribir la parte positiva del ideal como una sucesión,

$$I^+ = \{ \ a_1, a_2, ..., a_k, ...\}$$

y así iniciar el proceso

$$\begin{array}{rcccl} d_2 & = & m.c.d.\{a_1, a_2\} & \geq & 1 \\ d_3 & = & m.c.d.\{a_1, a_2, a_3\} & \geq & 1 \\ \vdots & & & & \\ d_k & = & m.c.d.\{a_1, a_2, ..., a_k\} & \geq & 1 \\ \vdots & & & & \end{array}$$

La sucesión $(d_k)_k$ es decreciente y a partir de un k constante. Sea $d = \text{mín}\{d_k \ : \ k \geq 2 \ \}$. Claramente $d\mathbb{Z} \subseteq I$. Realmente tenemos una igualdad, ya que si $r \in I$, $r > 0$, entonces $d|r$ y así $r \in d\mathbb{Z}$. Por tanto

$$(d) = d\mathbb{Z} = I$$

y así I es un ideal principal $\square$

Entre los ideales de un anillo hay unos más apreciados que otros, como los primos entre los enteros.

Definición 3. *Un ideal I de un anillo $\mathbb{A}$ se llama* ***maximal*** *si $I \neq \mathbb{A}$ y si para cualquier otro ideal I' con $I \subsetneq I'$ necesariamente se tiene que $I' = \mathbb{A}$.*

Ejemplos 3.

a: *$n\mathbb{Z}$ es un ideal maximal de $\mathbb{Z}$ si y solo si n es primo.*

b: *Sea $p \in \mathbb{F}[x]$. El ideal generado por el polinomio p, (p), es maximal si y solo si p es irreducible (es decir que no es divisible por un polinimio de grado menor).*

La prueba usa que tanto $\mathbb{Z}$ como $\mathbb{F}[x]$ son dominios de ideales principales. La parte **b)** la dejaremos para cuando estudiemos polinomios.

Ahora si n no es primo, existe un primo p que divide a n, $p|n$. De aquí

$$n\mathbb{Z} \subsetneq p\mathbb{Z} \subsetneq \mathbb{Z}.$$

Por otro lado si p es primo, no existe ideal en $\mathbb{Z}$, $I' = n\mathbb{Z}$ de modo que $p\mathbb{Z} \subsetneq n\mathbb{Z}$, ya que ésto último nos diría que $n|p$ $\square$

Referencias

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

Email address: `Cesar_Ruiz@mat.ucm.es`