Tema 3. Congruencias

Ideales y Cocientes

Definición 3.0.1

Dado un anillo A, una congruencia (de anillos) en A es una relación de equivalencia $\equiv$ en A compatible con la estructura de anillo:

Compatible con la suma

$$\left.\begin{array}{l} x \equiv y \\ z \equiv t \end{array}\right\} \Rightarrow x+z \equiv y+t$$

Compatible con el producto

$$\left.\begin{array}{l} x \equiv y \\ z \equiv t \end{array}\right\} \Rightarrow xz \equiv yt$$

Compatible con los opuestos

$$x \equiv y \Rightarrow -x \equiv -y$$

Se deduce de

$$\left.\begin{array}{l} -1 \equiv -1 \\ x \equiv y \end{array}\right\} \Rightarrow -x \equiv -y$$

Si $\equiv$ es una congruencia en A podemos trasladar la estructura de anillo de A al conjunto de clases de equivalencia $A/\equiv$ de tal forma que la proyección canónica sea un morfismo de anillos. $pr: A \twoheadrightarrow A/\equiv$

Con estas operaciones, $A/\equiv$ es un anillo

$\bar{a} + \bar{b} := \overline{a+b}$

$\bar{a} \cdot \bar{b} := \overline{a \cdot b}$ $\quad \forall\, \bar{a}, \bar{b} \in A/\equiv$ $\quad$ $A/\equiv$ es el anillo cociente de A por la congruencia $\equiv$

$-(\bar{a}) := -\bar{a}$

$\bar{0}\,,\ \bar{1}$

Definición 3.0.2

El núcleo de una congruencia $\equiv$ en un anillo A se define como:

$$\mathrm{Ker}(\equiv) := \{a \in A \,;\, a \equiv 0\}$$

$$:= \ker(pr) := pr^{*}(\{0\})$$

$$\mathrm{Ker}(\equiv) \subseteq A$$

Propiedades

- $0 \in \ker(\equiv) \Rightarrow \ker(\equiv) \neq \emptyset$
- Es cerrado para sumas: $a, b \in \ker(\equiv) \Rightarrow a+b \in \ker(\equiv)$
- Es cerrado para opuestos: $a \in \ker(\equiv) \Rightarrow -a \in \ker(\equiv)$
- Es cerrado para múltiplos: $a \in \ker(\equiv),\ \forall x \in A \Rightarrow x \cdot a \in \ker(\equiv)$

Definición 3.0.3

Un ideal de un anillo A es un subconjunto $I \subseteq A$ que tiene:

- $0 \in I$
- Es cerrado para sumas: $a, b \in I \Rightarrow a+b \in I$
- Es cerrado para opuestos: $a \in I \Rightarrow -a \in I$
- Es cerrado para múltiplos: $a \in I,\ \forall b \in A \Rightarrow a \cdot b \in I$

Proposición 3.0.4

Un subconjunto no vacío $I \subseteq A$ es un ideal si y sólo si, es cerrado para combinaciones lineales:

$$\forall a,b \in I, \ \forall x,y \in A, \ xa + yb \in I$$

Si I es ideal de $A \Rightarrow I \trianglelefteq A$

El núcleo de una congruencia es un ideal

$\forall \equiv$ congruencia de A

$Ker(\equiv) \trianglelefteq A$

$\forall f : A \to B$ morfismo

$$Ker(f) = f^*(\{0\}) = \{a \in A : f(a) = 0\} \trianglelefteq A$$

Proposición 3.0.5

Si $I \trianglelefteq A$ es un ideal, entonces la relación definida por $a \equiv_I b$

$$a \equiv_I b \overset{def}{\Longleftrightarrow} a - b \in I$$

es una congruencia con núcleo $Ker(\equiv_I) = I$

"a congruente con b módulo I"

Después de probar que $\equiv_I$ es congruencia, vemos que $\equiv_{Ker(\equiv)} = \equiv$

Teorema 3.0.6

Dar una congruencia en un anillo A es equivalente a dar un ideal en A.

Es decir, toda congruencia es la congruencia asociada a todo ideal y todo ideal es el núcleo de una congruencia.

Dado un ideal $I \leq A$ si $a \equiv_I b$ diremos que a es congruente con b módulo I ; $a \equiv b \mod I. \iff a-b \in I$

Toda congruencia en A es de la forma $\equiv_I$ para $I \leq A$ un ideal.
El conjunto cociente $A / \equiv_I$ lo denotaremos por A/I, sus elementos serán las clases de equivalencia módulo I:

$$\bar{a} = \{x \in A : x \equiv_I a\} = \{x \in A : x - a \in I\} = a + I$$

Donde $a+I$ es el conjunto de los elementos de A que se escriben de la forma $a+y$ con $y \in I$

$$A/I = \{a + I \; ; a \in A\}$$

Suma: $(a+I) + (b+I) := (a+b)+I$

Producto: $(a+I)(b+I) := (ab) + I$

Opuesto: $-(a+I) := (-a) + I$

La proy. canónica $\Rightarrow$ $pr : A \longrightarrow A/I$ $\quad pr(a) = a + I \in A/I$

Definición 3.0.7

Un ideal $I \leq A$ se dirá principal si existe un elemento $a \in A$ tq $I = aA$

Teorema 3.0.8.

En el anillo $\mathbb{Z}$ todo ideal es principal.

Por este teorema, todo ideal de $\mathbb{Z}$ será de la forma $n\mathbb{Z}$ y sus elementos serán múltiplos de $n \in \mathbb{Z}$.

$n\mathbb{Z} = -n\mathbb{Z}$; todo ideal de $\mathbb{Z} \Rightarrow n\mathbb{Z}$ con $n \geq 0$

$a \equiv_{n\mathbb{Z}} b \mod n\mathbb{Z} \Rightarrow a \equiv_n b$ ó $a \equiv b \mod n$ (a es congruente con b mod n)

El primer teorema de Isomorfía.

Dado un morfismo de anillos $f: A \to B$ su núcleo está definido como:

$$\ker f = \{a \in A : f(a) = 0\}$$

$0 \in \ker f$, $\ker f$ es cerrado para combinaciones lineales y por tanto, $\ker f$ es un ideal de A, $\ker f \leq A$

Si $\equiv$ es una congruencia en A, entonces $\ker \equiv = \ker pr$, $pr : A \twoheadrightarrow A/\equiv$ la proyección canónica.

Propiedad universal de la proyección canónica.

Dado un ideal $I \leq A$ dar un morfismo $\bar{f} : A/I \longrightarrow B$ es equivalente a dar un morfismo $f : A \to B$ tal que $f^*(I) = 0$.

$$\begin{tikzcd}
I \arrow[r, hook, "i"] \arrow[dr, "fi=0"'] & A \arrow[r, two heads, "pr"] \arrow[d, "\forall f"] & A/I \arrow[dl, dashed, "\exists ! \bar{f}"] \\
 & B &
\end{tikzcd}$$

$\bar{f}(a+I) = f(a)$

Demo

Dado $f: A \to B$ podemos def $\bar{f} : A/I \to B$; $\bar{f}(a+I) := f(a), \forall a \in A$ $\iff f(y) = 0 \ \forall y \in I$. Para podemos def $\bar{f} \iff \forall a,b \in A \Rightarrow a \equiv_I b \Rightarrow f(a) = f(a)$ | $a \equiv_I b \iff a-b \in I \Rightarrow f(a-b) = 0 \Rightarrow f(a) = f(b)$

Teorema 31.2

Dado un morfismo $f: A \to B$, existe un isomorfismo de anillos $b: A/\ker f \xrightarrow{\cong} Im(f)$ que hace conmutar el diagrama.

$$\begin{tikzcd} A \arrow[r, "\pi"] \arrow[d, "f"] & A/\ker f \arrow[d, "b"] \\ B & Img(f) \arrow[l, hook] \end{tikzcd}$$

Demo

El morfismo b está definido como $b(a+\ker f) := f(a)$. Utilizando la prop. universal de la pr. claramente b está bien def. Es rutinario probar que es morfismo, que es biyección y que hace conmutar el diagrama.

Operaciones con ideales

Sea A un anillo y sean $I, J \leq A$ dos ideales. Entonces:

- $I \cap J$ es ideal.
- En general $I \cup J$ no lo es.
- $I+J = \{a+b : a \in I, b \in J\}$ es un ideal. Es el menor ideal que contiene a I y a J.
- Producto $\Rightarrow$ $IJ = \{\sum_{i=1}^{r} a_i b_i ; a_i \in I, b_i \in J\}$ es un ideal

que además está contenido en $I \cap J$; $IJ \subseteq I \cap J$

Observación: $a_1 b_1 + a_2 b_2 = a_3 b_3$ no tiene por qué

Sin embargo $aA\, bA = (ab)A$ cuando los ideales son principales.