Tema 3

Congruencias. Ideales y Cocientes

La construcción de cocientes aparece en la mayoría de los contextos algebraicos (conjuntos, anillos, grupos, monoides, etc.). Para hacer un cociente en estos contextos, necesitamos una congruencia, esto es, una relación de equivalencia que sea compatible con la estructura algebraica que estemos considerando. Esta compatibilidad permitirá trasladar la estructura al conjunto de clases de equivalencias, haciendo que la proyección canónica sea morfismo.

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, lo que significa:*

- Compatible con la suma*:*

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

- Compatible con el producto*:*

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

- Compatible con los opuestos*:*

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

Claramente la compatibilidad de los opuestos se deduce de la compatibilidad con el producto ya que

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

Si $\equiv$ es una congruencia en A, podemos trasladar la estructura de anillo de A al conjunto de clases de equivalencia $A/\equiv$ de manera que la proyección canónica $pr : A \twoheadrightarrow A/\equiv$ sea un morfismo de anillos, definiendo suma, producto y opuestos en el cociente como sigue:

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

- $\bar{a} \cdot \bar{b} := \overline{a \cdot b}$,
- $-\bar{a} := \overline{-a}$.

Para todo $\bar{a}, \bar{b} \in A/\equiv$.

Dejamos como ejercicio comprobar que esta suma, producto y opuestos están bien definidos y que cumplen la axiomática de anillo.

El anillo $A/\equiv$ es el *anillo cociente de A por la congruencia $\equiv$.*

Definición 3.0.2. *El núcleo de una congruencia $\equiv$ en un anillo A se define como:*

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

Destacamos las siguientes propiedades del núcleo de una congruencia:

- $0 \in Ker(\equiv)$
- 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 múlltiplos $a \in Ker(\equiv), \forall x \in A \Rightarrow x \cdot a \in Ker(\equiv)$.

Estas propiedades dan lugar a la siguiente

Definición 3.0.3. *Un ideal de un anillo A es un subconjunto $I \subseteq A$ que tiene las siguientes propiedades:*

- $0 \in I$
- *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 múlltiplos* $a \in I, \forall b \in A \Rightarrow a \cdot b \in I$.

Es fácil de comprobar la siguiente

Proposición 3.0.4. *Un subconjunto no vacío $I \subseteq A$ es un ideal si, y sólo si, es cerrado para combinaciones lineales, esto es:*

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

Si I es un ideal de un anillo A escribiremos $I \leq A$.

Está claro que el núcleo de una congruencia es un ideal, veamos ahora que todo ideal determina una congruencia que lo tiene a el por núcleo.

Proposición 3.0.5. *Si $I \leq A$ es un ideal, entonces la relación definida por*

$$a \equiv_I b \Leftrightarrow a - b \in I,$$

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

Demostración. Para ver que es congruencia tenemos que probar primero que es relación de equivalencia y después que es compatible con la estructura. Probamos solamente que es compatible con el producto, el resto de las propiedades las dejamos como ejercicio.

$$\left.\begin{array}{l} a \equiv b \Leftrightarrow a-b \in I \Rightarrow (a-b)c \in I \\ c \equiv d \Leftrightarrow c-d \in I \Rightarrow (c-d)b \in I \end{array}\right\} \overset{\text{sumando}}{\Rightarrow} (a-b)c+(c-d)b = ac-bd \in I \Rightarrow ac \equiv_I bd.$$

Si calculamos el núcleo

$$Ker(\equiv_I) = \{a \in A;\, a \equiv_I 0\} = \{a \in A;\, a-0 = a \in I\} = I.$$

■

Notemos ahora que dada una congruencia $\equiv$ en A, la relación $\equiv_{Ker(\equiv)}$ es la propia $\equiv$. De manera que tenemos:

Teorema 3.0.6. *Dar una congruencia en un anillo A es equivalente a dar un ideal de A.*

Observación 3.0.1. Dado un idea $I \leq A$ si $a \equiv_I b$ diremos que a es congruente con b módulo I y a veces también lo denotaremos $a \equiv b \mod I$.

Observación 3.0.2. Después del Teorema 3.0.6 tenemos que toda congruencia en A es de la forma $\equiv_I$ para $I \leq A$ un ideal. Al conjunto cociente $A/\equiv_I$ lo denotaremos simplemente por A/I y sus elementos serán clases de equivalencia módulo I. Veamos ahora como es la clase de equivalencia de un elemento $a \in A$ 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 $y \in I$. Así,

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

y la suma, el producto y los opuestos están definidos como:

- $(a+I)+(b+I) := (a+b)+I$,
- $(a+I)\cdot(b+I) := (a\cdot b)+I$,
- $-(a+I) := (-a)+I$.

Además la proyección canónica $pr : A \twoheadrightarrow A/I$ lleva un elemento $a \in A$ en $pr(a) = a+I \in A/I$.

Ejemplo 3.0.1. Todo anillo A tiene dos ideales *improòios*, el ideal cero $0 = \{0\} \leq A$ y el ideal *total* $A \leq A$.

Ejemplo 3.0.2. Si A es un anillo y $a \in A$ es un elemento, los múltiplos de a, que denotamos aA es un ideal de A. Está claro que los ideales impropios son los múltiplos de cero y de uno respectivamente. $0 = 0A$ y $A = 1A$.

Definición 3.0.7. *Un ideal $I \leq A$ se dirá principal si existe un elemento $a \in A$ tal que $I = aA$.*

El Teorema 2.1.1 de Euclides nos permite demostrar:

Teorema 3.0.8. *En el anillo $\mathbb{Z}$ todo ideal es principal.*

Demostración. El ideal trivial es claramente principal, supongamos entonces un ideal no trivial $I \leq \mathbb{Z}$, denotemos $I^+ = \{a \in I;\ 0 < a\} \subseteq \mathbb{N}$.

Puesto que si $a \in I$ entonces $-1 \cdot a = -a \in I$ e I es no trivail, tenemos que $I^+ \neq \emptyset$ y por tanto podemos tomar $a = min(I^+)$. Puesto que $a \in I^+ \subseteq I$ tenemos que $aA \subseteq I$. Recíprocamente, sea $b \in I$ un elemento cualquiera, ya que $a \neq 0$, podemos dividir b por a y tenemos que existen $q, r \in \mathbb{Z}$ tales que $b = aq + r$ y $0 \leq r < |a| = a$. Veamos que $r = 0$. Si no fuese cero, tendríamos que $r = b - aq \in I^+$ y $r < a$, que contradice que $a = min(I^+)$. Por tanto $r = 0$ y $b = aq \in aA$. Así $I \subseteq aA$ y tenemos la igualdad. ■

Observación 3.0.3. Por el Teorema 3.0.8 todo ideal de $\mathbb{Z}$ será de la forma $n\mathbb{Z}$ y sus elementos serán los múltiplos de $n \in Z$. Notemos que $n\mathbb{Z} = -n\mathbb{Z}$ y por tanto todo ideal de $\mathbb{Z}$ es de la forma $n\mathbb{Z}$ con $n \geq 0$. Además en lugar de escribir $a \equiv_{n\mathbb{Z}} b$ o $a \equiv b \mod n\mathbb{Z}$ escribiremos $a \equiv_n b$ o $a \equiv b \mod n$ y diremos que a es congruente con b módulo n, para $a, b, n \in \mathbb{Z}$ y $n \geq 0$.

3.1 El primer teorema de Isomorfía

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

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

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

Observación 3.1.1. Si $\equiv$ es una congruencia en A, entonces

$$\ker \equiv = \ker pr$$

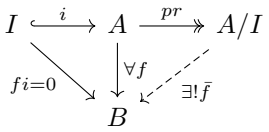
con $pr :: A \twoheadrightarrow A/\equiv$ la proyección canónica.

En particular, si $I \leq A$ es un ideal, $\ker \equiv_I = I$.

La proyección canónica $pr : A \twoheadrightarrow A/I$ tienen la siguiente propiedad universal:

Proposición 3.1.1 (Propiedad universal de la proyección canónica)**.**

Dado un ideal $I \leq A$ dar un morfismo $\bar{f} : A/I \to B$ es equivalente a dar un morfismo $f : A \to B$ tal que $f^*(I) = 0$. Sintetizamos esta propiedad mediante el siguiente diagrama:



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

Demostración. La demostración de esta proposición consiste en ver que dado un morfismo $f : A \to B$ podemos definir $\bar{f} : A/I \to B$ por $\bar{f}(a + I) := f(a), \forall a \in A$, si, y sólo si, $f(y) = 0, \forall y \in I$. Pero, utilizando la proposición 1.3.2 podemos definir la aplicación $\bar{f}$ si, y sólo si, $\forall a, b \in A$ se tiene que $a \equiv_I b$ implique $f(a) = f(b)$. Basta entonces considerar:

$$a \equiv_I b \Leftrightarrow a - b \in I \Rightarrow f(a - b) = 0 \Rightarrow f(a) = f(b).$$

Así si todos los elementos de I van a 0 por f podemos definir $\bar{f}$ que claramente es un morfismo. El recíproco es claro. ■

Teorema 3.1.2 (Primer teorema de Isomorfía)**.**

Dado un morfimso de anillos $f : A \to B$ existe un isomorfismo de anillos $b : A/\ker f \xrightarrow{I} m(f)$ que hace comnmutar el diagrama

$$\begin{array}{ccc} A & \xrightarrow{pr} & A/\ker f \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle b\cong} \\ B & \longleftarrow & Im(f) \end{array} \tag{3.1}$$

Demostración. El morfismo b está definido como $b(a+\ker f) := f(a)$. Utilizando la propiedad universal de la proyección claramente b está bien definido. Es rutinario probar que es morfismo, que es una biyección y que hace conmutar el diagrama 3.1. ■

Ejemplo 3.1.1. Tomemos $n \geq 2$ un entero y consideremos la aplicación $R : \mathbb{Z} \to \mathbb{Z}_n$ que a cada entero $a \in \mathbb{Z}$ le hace corresponder el resto de dividir a entre n. Esta aplicación es n morfismo de anillos y claramente es sobreyectivo ya que si $0 < a$ entonces $R(a) = a$. Además el resto de dividir a por n es cero si, y sólo si, a es un múltipo de n, pro tanto $\ker R = n\mathbb{Z}$. El primer teorema de isomoría nos asegura que se tiene un isomorfismo

$$b : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}_n;\ a + n\mathbb{Z} \mapsto R(A).$$

3.2 Operaciones con ideales

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

- La intersección $I \cap J$ es un ideal.
- En general la unión $I \cup J$ no lo es.
- La suma $I + J = \{a + b;\ a \in I, b \in J\}$ es un ideal. Además este es el menor ideal que contiene a I y a J.
- El producto, definido como

$$IJ = \{\sum_{i=1}^{r} a_i b_i;\ a_i \in I, b_i \in J\},$$

  es un ideal, que además está contenido en la intersección $IJ \subseteq I \cap J$.

Dejamos como ejercicio probar las afirmaciones anteriores.

Observación 3.2.1. El producto de dos elementos ab con $a \in I$ y $b \in J$ es un elemento de IJ, pero la suma de dos de estos productos $a_1b_1 + a_2b_2, a_i \in I, b_j \in J, i = 1, 2$, no tiene porqué ser un producto de este tipo, es decir no tiene porqué existir $a_3 \in I$ y $b_3 \in J$ tal que $a_1b_1 + a_2b_2 = a_3b_3$. A esto se debe que el producto de dos ideales se defina del modo que se ha hecho.

Sin embargo si hay un caso en el que el producto de dos ideales tiene una forma sencilla, este es cuando los ideales son principales, en cuyo caso es fácil comprobar:

$$aAbA = (ab)A.$$