Álgebra Conmutativa
Tarea 2: Ejercicios 7-12 Tema 1

José Luis Cánovas Sánchez

26 de septiembre de 2016

Ejercicio 7

$\mathcal{P} = \{x_i \quad i = 1, 2, ... \quad primos\} \subseteq \mathbb{Z}$
$\mathbb{Z}_{(\mathcal{P})} = \{q \in \mathbb{Q} \quad | \quad q = \frac{a}{b} \quad a, b \in \mathbb{Z} \quad (b, x_i) = 1 \, \forall x_i \in \mathcal{P}\}$
¿$\mathbb{Z}_{(\mathcal{P})}$ subanillo de $\mathbb{Q}$?
¿$\mathbb{Z}_{(\emptyset)}$?, ¿$\mathbb{Z}_{(\overline{\mathcal{P}})}$?, donde $\overline{\mathcal{P}}$ es el conjunto de todos los primos.

Comprobemos la definición 1.5 de subanillo:
(ii) $1 \in \mathcal{P}$
Como el 1 es coprimo con todos los enteros, $(1, x_i) = 1 \quad \forall x_i \in \mathcal{P}$, tomamos en la representación del racional $q = \frac{a}{b}$ $a = 1$ y $b = 1$, $q = 1 \in \mathcal{P}$.

(i) $u, v \in \mathbb{Z}_{(\mathcal{P})} \Rightarrow u - v \in \mathbb{Z}_{(\mathcal{P})}, \quad uv \in \mathbb{Z}_{(\mathcal{P})}$
Sean $u = \frac{n}{d}$ y $v = \frac{m}{e}$ con $(d, x) = 1$ y $(e, x) = 1$ $\forall x \in \mathcal{P}$.
$u - v = \frac{n}{d} - \frac{m}{e} = \frac{ne - md}{de}$
$uv = \frac{n}{d}\frac{m}{e} = \frac{nm}{de}$
Y como $(de, x) = 1 \quad \forall x \in \mathcal{P}$, $u, v \in \mathbb{Z}_{(\mathcal{P})}$.

En el caso $\mathbb{Z}_{(\emptyset)}$, como no hay elementos en el conjunto $\mathcal{P}$ no hay denominadores posibles que sean coprimos con ellos, ni siquiera el 1, por tanto $\mathbb{Z}_{(\emptyset)} = \emptyset$.

Sin embargo, $\mathbb{Z}_{(\overline{\mathcal{P}})}$ tiene la propiedad que un denomidador d entero, como se puede factorizar de manera única en producto de primos ($\mathbb{Z}$ es DFU), siempre será múltiplo de alguno, incluso si d es primo, ocurrirá $(d, d) = d$ por $d \in \overline{\mathcal{P}}$. Por tanto el único denominador coprimo con todos los elementos de $\overline{\mathcal{P}}$ es el 1, y por tanto $\mathbb{Z}_{(\overline{\mathcal{P}})} = \mathbb{Z}$.

Ejercicio 8

Describir $\mathbb{Z}_{(\mathcal{P})}$ cuando $\mathcal{P}$ está formado por un solo número primo p; y encontrar todos sus ideales.

Los elementos de $\mathbb{Q}$ cuyo denomidador no es múltiplo de p. Además tenemos en cuenta que $\mathbb{Z} \subset \mathbb{Z}_{(\mathcal{P})}$:
$\mathbb{Z} \bigcup \left(\mathbb{Q} \setminus \left(\frac{1}{p}\right)\right)$

Los ideales serán el nulo (0), el trivial $\mathbb{Z}_{(\mathcal{P})}$ y un ideal propio sólo podrá estar generado por elementos no unidades (por ejercicio3.ii). El primo p es el único elemento sin inverso, y por tanto el único ideal propio es el (p).

Ejercicio 9

¿Existe algún anillo que tenga exactamente tres ideales?

El del ejercicio 8.

Otro ejemplo lo sacamos pensando en que no puede ser un cuerpo (ejercicio 3.a) y que por simplicidad sea finito, acabamos pensando en los anillos de enteros módulo un número **no** primo.

Por ejemplo, el anillo de los enteros $\mathbb{Z}_4 = \{0,\ 1,\ 2,\ 3\}$ (siendo 0, 1, 2, 3 los representantes de las clases módulo 4).

Los ideales posibles son:
$(0) = \{0\}$
$(1) = \mathbb{Z}_4$
$(2) = \{0,\ 2\}$

Cualquier otro ideal da lugar a uno de los anteriores:
$(3) = \{0,\ 3,\ 2,\ 1\} = (1)$
$(\{0,\ 2\}) = (2)$
$(\{1,\ 2\}) = (1)$
$(\{2,\ 3\}) = (1)$
...

Ejercicio 10

Demostrar que todo subanillo de $\mathbb{Q}$ es igual a algún $\mathbb{Z}_{(\mathcal{P})}$.

Sea $\mathcal{Z}$ el conjunto de todos los $\mathbb{Z}_{(\mathcal{P})}$.
Sea $\mathcal{S}$ el conjunto de todos los subanillos de $\mathbb{Q}$.

$\mathcal{S} \supseteq \mathcal{Z}$
Por el ejercicio 7, todo $\mathbb{Z}_{(\mathcal{P})}$ es subanillo.

$\mathcal{S} \subseteq \mathcal{Z}$
Sea $S \in \mathcal{S}$ un subanillo de $\mathbb{Q}$.

Sean $q, t \in S \subset \mathbb{Q}$, con representantes en $\mathbb{Q}$ $q = \frac{a}{b}$ y $t = \frac{c}{d}$, que cumplen $(a, b) = 1$ y $(c, d) = 1$.

Por S subanillo, $q - t \in S$ y $qt \in S$, y aplicando ambas operaciones hemos visto en Ej.7 que los denominadores son en ambos casos $b \cdot d$.

Si descomponemos todos los denominadores que no son 1 de los elementos de S en producto de primos ($\mathbb{Z}$ DFU), y tomamos su intersección, tenemos un conjunto $\mathcal{P}$ de primos donde todos los denominadores de S son coprimos con todos los elementos de $\mathcal{P}$.

Ejercicio 11

Demostrar que el conjunto de los ideales no nulos de un dominio tiene una estructura de monoide con el producto de ideales. Probar que si el anillo es un DIP, entonces el monoide es cancelativo.

Veamos que cumple la asociatividad y tiene elemento neutro (propiedades de ser un monoide):

Sea $\mathcal{I}$ el conjunto de los ideales no nulos I del anillo A. No vacío porque el ideal $(1) = A$ siempre existe.

El producto se define como $IJ = (\{xy | x \in I\, y \in J\})$.

Veamos que el ideal $(1) = A$ es el neutro: ¿ $IA = AI = I$?

$IA = (\{xa | x \in I\, a \in A\}) \Rightarrow$ por I ideal, y A conmutativa por la suposición del inicio del capítulo, $ax = xa \in I \Rightarrow IA = (\{x | x \in I\}) \Rightarrow IA = AI = I$.

Sean I, J y K tres ideales de A.

¿$(IJ)K = I(JK)$?

$(IJ) = (\{xy | x \in I\, y \in J\}) =$ [Prop. 2.11] $= \{\sum_j a_j x_j y_j | a_j \in A,\ x_j \in I,\ y_j \in J\}$

$(IJ)K = (\{hz | h \in IJ\, z \in K\}) = \{\sum_j a_j x_j y_j z_j | a_j \in A,\ x_j \in I,\ y_j \in J,\ z_j \in K\}$

Con la misma construcción para $I(JK)$ tenemos:

$I(JK) = (\{xu | x \in I\, u \in JK\}) = \{\sum_j a_j x_j y_j z_j | a_j \in A,\ x_j \in I,\ y_j \in J,\ z_j \in K\}$

$\Rightarrow (IJ)K = I(JK)$.

Ahora el caso de que sea A un DIP.

Tomemos $I = (a)$, $J = (b)$, $K = (c)$ ideales principales de A, por hipótesis no nulos.

¿$IJ = IK \Rightarrow J = K$?

Sea $a_i \in A$:

$IJ = (a)(b) = \langle \sum_i a_i \cdot ab \rangle = \langle \sum_i ai \cdot ac \rangle = IK$

Como los $a_i \cdot a \in A$, podemos considerar los mismos conjuntos generados pero en vez de por ab y ac, por b y c, lo que nos da que los ideales son los mismos y $J = K$, que es la condición de ser cancelativo.

Ejercicio 12

Aplicar la Proposición 2.22 al anillo de los enteros.

Como $\mathbb{Z}$ es un DIP, podemos expresar los I_i de la proposición como (r_i) con cada $r_i\ \in \mathbb{Z}$

La aplicación quedaría:

$\phi\colon \mathbb{Z} \to \frac{\mathbb{Z}}{(r_1)} \times \cdots \times \frac{\mathbb{Z}}{(r_n)}$

donde $\phi\,(x) = (x + (r_1),\, x + (r_2), \ldots,\, x + (r_n))$

Llamando x_i a los valores tal que $x \equiv x_i\, mod\, r_i$, nos queda:

$\phi\,(x) = (x_1, \ldots, x_n)$

Si los ideales son primos dos a dos, veamos que siendo principales implica que los r_i también son primos dos a dos:

Si (r_i) y (r_j) son primos, $(1) = (r_i) + (r_j)$, por lo que existen $u, v \in \mathbb{Z}$ tal que $ur_i + vr_j = 1$.

Esta es la Identidad de Bezout e implica que r_i y r_j son coprimos: $(r_i, r_j) = 1$.

Además, el producto $\prod(r_i) = (r_1 \cdots r_n) = (N)$ con $N = r_1 \cdots r_n$

Tenemos por la proposición 2.22 que existe un isomorfismo

$\frac{\mathbb{Z}}{N} \cong \frac{\mathbb{Z}}{(r_1)} \times \cdots \times \frac{\mathbb{Z}}{(r_n)}$

En resumen, tenemos el Teorema Chino de los restos:

Supongamos que n_1, $n_2, \ldots, n_k$ son enteros positivos coprimos dos a dos. Entonces, para enteros dados a_1, $a_2, \ldots, a_k$, existe un entero x que resuelve el sistema de congruencias simultáneas

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

Más aún, todas las soluciones x de este sistema son congruentes módulo el producto $N = n_1 n_2 ... n_k$.

En lenguaje algebraico es que para cada entero positivo con factorización en números primos:

$n = p_1^{r_1} \cdots p_k^{r_k}$

se tiene un isomorfismo entre un anillo y la suma directa de sus potencias primas:

$\mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}/p_1^{r_1}\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/p_k^{r_k}\mathbf{Z}$