Tema 5.-. Teoría de anillos. Dominios, cuerpos y cuerpos de fracciones. Característica de un cuerpo.

5.1. Anillos y cuerpos

Definición 5.1.1.– Un *anillo* es una terna $(A, +, \cdot)$ formada por un conjunto A y dos operaciones binarias $+, \cdot$ verificando:

1. El par $(A, +)$ es un grupo abeliano, cuyo elemento neutro llamaremos normalmente "cero (0)".

2. La operación binaria $\cdot$ es asociativa y tiene elemento neutro, que llamaremos normalmente "uno (1)".

3. La operación $\cdot$ es *distributiva* a la derecha y a la izquierda respecto de la operación $+$, i.e. para todos $x, y, z \in A$, se tiene $(x+y)\cdot z = x\cdot z + y\cdot z$, $x\cdot(y+z) = x\cdot y + x\cdot z$.

Si además la operación $\cdot$ es conmutativa, diremos que el anillo es conmutativo.

Nota 5.1.2.–

1. En general se usará la expresión "sea A un anillo", sobreentendiendo las operaciones. La operación $\cdot$ se notará normalmente por simple yuxtaposición.

2. En un anillo A se tiene $0 \cdot x = x \cdot 0 = 0$ para todo $x \in A$.

3. Si en un anillo A se tiene $1 = 0$, entonces $A = \{0\}$.

4. Para todo $x, y \in A$, ese tiene $x(-y) = (-x)y = -(xy)$.

5. Si $A_1, \ldots, A_n$ son anillos, el producto cartesiano $A_1 \times \cdots \times A_n$ posee una estructura natural de anillo, donde las operaciones están definidas componente a componente.

Ejemplo 5.1.3.–

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ son anillos conmutativos. La estructura de anillo de $\mathbb{Z}$ viene determinada por la de grupo aditivo: el producto de dos enteros xy coincide con el múltiplo de y con coeficiente x. Así pues, la estructura de anillo de $\mathbb{Z}$ no añade nada nuevo a la de grupo. Esto es falso para $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ en los que, obviamente, la estructura multiplicativa no viene determinada por la aditiva.

2. El conjunto $\mathcal{M}(n)$ de las matrices $n \times n$ sobre $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$ es un anillo, con respecto a la adición y la multiplicación ordinaria de matrices. No es conmutativo.

Definición 5.1.4.– Sea A un anillo. Una *unidad* es un elemento que posee un simétrico multiplicativo (a la izquierda y a la derecha), que llamaremos *inverso*. El conjunto de las unidades de A es un grupo para el producto y se notará A^*.

Un *cuerpo* es un anillo conmutativo tal que todo elemento distinto de cero es una unidad, i.e. $A^* = A - \{0\}$. (En algunos textos también se llaman cuerpos aquellos anillos no necesariamente conmutativos tales que todos sus elementos no nulos son unidades. En otros textos a estos anillos se les llama *anillos de división*).

Ejemplo 5.1.5.–

1. Las unidades de $\mathbb{Z}$ son $1, -1$. Los anillos $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ son cuerpos.

2. El grupo de las unidades del anillo $\mathcal{M}(n, k)$ con $k = \mathbb{Q}$, $\mathbb{R}$ ó $\mathbb{C}$ es $GL(n, k)$.

Definición 5.1.6.– Sea A un anillo. Un *subanillo* de A es un subconjunto $B \subset A$ que es un subgrupo de $(A, +)$, que es estable para la operación $\cdot$ y tal que $1 \in B$.

Si A es un cuerpo, diremos que B es un *subcuerpo* de A si es un subanillo y además $x^{-1} \in B$ para todo $x \in B - \{0\}$.

A partir de ahora sólo trabajaremos con anillos conmutativos. Así pues, la palabra '*anillo*' significará siempre anillo conmutativo.

Definición 5.1.7.– Sea A un anillo. Un elemento $x \in A$ se llamará un *divisor de cero* si y sólo si es distinto de cero y existe $y \in A$, $y \neq 0$, tal que $xy = 0$. Un anillo sin divisores de cero se llama un *dominio de integridad*. Un elemento $x \in A$ se llamará *nilpotente* si es distinto de cero y existe un entero $n > 0$ tal que $x^n = 0$. En un dominio de integridad se da la propiedad cancelativa por el producto de elementos no nulos:

$$a \neq 0, ab = ac \Rightarrow b = c.$$

Ejemplo 5.1.8.–

1. Las unidades no son divisores de cero. Así, todo cuerpo es un dominio de integridad.

2. $\mathbb{Z}$ es un dominio de integridad.

3. El anillo $\mathbb{Z}/\mathbb{Z}4$ no es un dominio de integridad. El anillo $\mathbb{Z}/\mathbb{Z}3$ es un cuerpo.

4. El elemento 2 es nilpotente en $\mathbb{Z}/\mathbb{Z}4$.

Definición 5.1.9.– Sea A un anillo. Un *ideal* de A es un subconjunto I de A que verifica:

1. I es un subgrupo del grupo aditivo de A.

2. Para todo $a \in I$, $x \in A$ se tiene $xa \in I$.

NOTA 5.1.10.– Sea $I \subset A$ un ideal de A. Se tiene:

1. Si I contiene una unidad, entonces $I = A$.
2. Si A es un cuerpo, sus únicos ideales son $\{0\}$ y A.
3. El grupo cociente A/I admite una estructura canónica de anillo. En efecto, basta ver que la fórmula
$$(a + I)(b + I) = ab + I$$
define una operación en A/I. Si $a + I = a' + I$ y $b + I = b' + I$ es $a - a' \in I$, y $b - b' \in I$. Así
$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b' \in I,$$
lo que prueba nuestro aserto.
4. Los ideales de $\mathbb{Z}$ y los subgrupos son la misma cosa, pues la estructura multiplicativa viene determinada por la aditiva.

EJEMPLO 5.1.11.– En el grupo $(\mathbb{Z}/\mathbb{Z}n, +)$ podemos definir un producto de la siguiente manera:

$$(a, b) \in \mathbb{Z}/\mathbb{Z}n \times \mathbb{Z}/\mathbb{Z}n \mapsto a \cdot b := \text{resto de la división de } ab \text{ entre } n.$$

De esta forma $\mathbb{Z}/\mathbb{Z}n$ es un anillo.

LEMA 5.1.12.– Sea $\{I_k\}$ una familia de ideales. Entonces $\bigcap_k I_k$ es un ideal.

DEFINICIÓN 5.1.13.– Si A es un anillo y $S \subset A$ no vacío. El ideal generado o engendrado por S es el menor ideal en A que contiene a S, o bien la intersección de todos los ideales que contienen a S. Lo notaremos por (S) o bien $\langle S \rangle$.

DEFINICIÓN 5.1.14.– Sean I_1, I_2 ideales. Definimos $I_1 + I_2 = \langle I_1 \cup I_2 \rangle$.

NOTA 5.1.15.– Es fácil ver que

$$\langle S \rangle = \{x_1a_1 + \cdots + x_na_n \mid x_1, \ldots, x_n \in A, a_1, \ldots, a_n \in S\}.$$

Si $S = \{a\}$ el ideal de llama *principal*. Todo ideal de $\mathbb{Z}$ es principal.

LEMA 5.1.16.– $I_1 + I_2 = \{a_1 + a_2 : a_i \in I_i\}$.

DEFINICIÓN 5.1.17.– Sean A, B anillos, $f : A \to B$ una aplicación. Se dirá que f es un *homomorfismo* de anillos si verifica:

1. Para todos $x, y \in A$, es $f(x + y) = f(x) + f(y)$.
2. Para todos $x, y \in A$, es $f(xy) = f(x)f(y)$.
3. $f(1) = 1$.

Un homomorfismo biyectivo se llama un *isomorfismo*.

PROPOSICIÓN 5.1.18.– Sea $f : A \to B$ un homomorfismo de anillos. Se tienen las siguientes propiedades:

1. $\ker(f) := \{a \in A \mid f(a) = 0\}$ es un ideal de A, y f es inyectivo si y sólo si $\ker(f) = \{0\}$.

2. Si $u \in A$ es una unidad, entonces $f(u)$ es una unidad en B. En particular cualquier homomorfismo (de anillos) entre cuerpos es inyectivo.

3. $\mathrm{im}(f) = \{b \in B \mid \exists a \in A, f(a) = b\}$ es un subanillo de B.

PROPOSICIÓN 5.1.19.– Primer teorema de isomorfía. Sea $f : A \to B$ un morfismo de anillos. Entonces $A/\ker(f)$ es isomorfo a $\mathrm{im}(f)$.

PROPOSICIÓN 5.1.20.– Segundo teorema de isomorfía. Sea A un anillo, $I \subset A$ un ideal, y $B \subset A$ un subanillo. Entonces $B + I = \{b + a : b \in B, a \in I\}$ es un subanillo de A, I es un ideal de $B + I$, $B \cap I$ es un ideal de B, y existe un isomorfismo de anillos

$$(B + I)/I \cong B/(B \cap I).$$

PROPOSICIÓN 5.1.21.– Tercer teorema de isomorfía. Sea A un anillo y sean I, J ideales de A con $I \subset J$. Entonces J/I es un ideal de A/I y

$$A/J \cong (A/I)/(J/I).$$

5.2. Cuerpo de fracciones.

Sea A un dominio y llamemos $A' = A - \{0\}$. Consideremos la relación binaria $\sim$ definida en $A \times A'$ por

$$(a, b) \sim (a', b') \Leftrightarrow ab' = a'b.$$

Es fácil verificar que $\sim$ es una relación de equivalencia. Llamamos $Q(A)$ al conjunto cociente $A \times A'/\sim$, y los elementos de $Q(A)$ los escribiremos como $\frac{a}{b}$. Se tienen las siguientes operaciones definidas en $Q(A)$:

- Suma $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$.
- Producto $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

LEMA 5.2.1.– Las operaciones están bien definidas, esto es, si $ab' = a'b$ y $cd' = c'd$, entonces

$$\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}, \frac{ac}{bd} = \frac{a'c'}{b'd'}.$$

PROPOSICIÓN 5.2.2.– $Q(A)$ es un cuerpo, denominado cuerpo de cocientes o fracciones de A.

PROPOSICIÓN 5.2.3.– Sea A un dominio de integridad y $Q(A)$ su cuerpo de fracciones. Se verifica:

1. La aplicación $\varphi : A \to Q(A)$ definida por $\varphi(a) = \frac{a}{1}$ es un homomorfismo inyectivo de anillos.

2. (*Propiedad universal de* $Q(A)$) Si K es un cuerpo cualquiera, todo homomorfismo inyectivo de anillos $\psi : A \to K$ factoriza por φ, es decir, existe un único homomorfismo de anillos $\Phi : Q(A) \to K$ que hace conmutativo el siguiente diagrama:

$$\begin{array}{ccc} A & \overset{\psi}{\to} & K \\ \varphi \searrow & & \nearrow \Phi \\ & Q(A) & \end{array}$$

3. Si L es un cuerpo que verifica la propiedad anterior de $Q(A)$, entonces L es isomorfo a $Q(A)$.

Se tiene, por tanto, que $Q(A)$ es el menor cuerpo que contiene a un dominio isomorfo a A, salvo isomorfismo. Dicho de otro modo, todo cuerpo que contiene a un dominio isomorfo a A, contiene también a un cuerpo isomorfo a $Q(A)$.

Demostración. El primer apartado es trivial. Para el segundo, definimos Φ mediante la expresión $\Phi(\frac{a}{b}) = \psi(a)\psi(b)^{-1}$. Hay que verificar que Φ está bien definida:

$$\frac{a}{b} = \frac{a'}{b'} \Rightarrow ab' = a'b \Rightarrow \psi(a)\psi(b') = \psi(a')\psi(b) \Rightarrow \psi(a)\psi(b)^{-1} = \psi(a')\psi(b')^{-1},$$

y que es un homomorfismo de anillos:

$$\begin{aligned} \Phi(\frac{a}{b} + \frac{a'}{b'}) &= \Phi(\frac{ab'+a'b}{bb'}) = \psi(ab'+a'b)\psi(bb')^{-1} = \\ &= \psi(a)\psi(b)^{-1} + \psi(a')\psi(b')^{-1} = \Phi(\frac{a}{b}) + \Phi(\frac{a'}{b'}), \end{aligned}$$

y análogamente conserva el producto y el elemento unidad. Se comprueba fácilmente que Φ hace conmutativo el diagrama, y de hecho es la única definición posible para que esto se cumpla, puesto que:

$$\Phi(\frac{a}{b}) = \Phi(\frac{a}{1} \cdot \frac{1}{b})) = \Phi(\frac{a}{1}) \cdot \Phi(\frac{1}{b}) = \Phi\varphi(a)\Phi\varphi(b)^{-1} = \psi(a)\psi(b)^{-1}.$$

Para la unicidad procedemos igual que con la propiedad universal de los grupos libres. Sea L un cuerpo verificando la propiedad universal, con $\varphi' : A \to L$. Tomando $K = Q(A)$, existe $\phi' : L \to Q(A)$ tal que $\varphi = \phi'\varphi'$. Aplicando 2) a $K = L$ y φ', se tiene que $\varphi' = \Phi\varphi$. De ambas, se tiene $\varphi = \Phi'\Phi\varphi$. Pero aplicando 2) a $K = Q(A)$ y φ, se tiene que $\Phi'\Phi$ y la identidad hacen conmutativo el correspondiente diagrama; por la unicidad se tiene que $\Phi'\Phi = \mathrm{i}d$. Análogamente se tiene que $\Phi\Phi' = \mathrm{i}d$, luego Φ es el isomorfismo buscado. □

5.3. Característica de un cuerpo.

NOTA 5.3.1.– Sea K un cuerpo. Todo homomorfismo de anillos φ de $\mathbb{Z}$ en K, lleva el elemento unidad de $\mathbb{Z}$ en el elemento unidad de K. Como vimos en el tema 4 (grupos libres) esto define unívocamente a φ. Por tanto existe un único homomorfismo de anillos φ de $\mathbb{Z}$ en K.

Caso inyectivo Si el homomorfismo φ de $\mathbb{Z}$ en K es inyectivo, hemos visto que entonces K contiene a su cuerpo de fracciones $\mathbb{Q}$. En ese caso diremos que K es un cuerpo de *característica cero*. Los cuerpos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son de característica cero, puesto que contienen a $\mathbb{Z}$. Además todo subcuerpo K de $\mathbb{C}$ es de característica cero. En otro caso el homomorfismo $\varphi : \mathbb{Z} \to K$ no inyectivo se extiende a $\mathbb{C}$, contradicción. Por tanto, todo subcuerpo de $\mathbb{C}$ contiene a $\mathbb{Q}$.

Caso no inyectivo En ese caso, $\ker(\varphi)$ es un ideal $\mathbb{Z}p$, con $p > 0$. Por el primer teorema de isomorfía $\mathbb{Z}/\mathbb{Z}p$ es isomorfo a un subanillo de K, luego no tiene divisores de cero. Así $\mathbb{Z}/\mathbb{Z}p$ es un dominio de integridad, o equivalentemente un cuerpo, y además, p es un número primo. Diremos entonces que K es un cuerpo de *característica* p. En ese caso se verifica que $px = 0$, para cada $x \in K$.