Anillos Conmutativos

Conceptos básicos

Definición. *Una* **operación** *(binaria interna) en un conjunto X es una aplicación $f : X \times X \to X$. Dados $x, y \in X$, la imagen $f(x, y)$ se escribe utilizando una notación adecuada a cada caso, por ejemplo,*

$$x + y \quad ó \quad x.y \quad ó \quad xy \quad ó \quad x * y \quad \text{etc.}$$

- *Una operación $*$ en X es* **asociativa** *si $(x * y) * z = x * (y * z)$, para todo $x, y, z \in X$; y es* **conmutativa** *si $x * y = y * x$, para todo $x, y \in X$.*
- *Si $\circ$ es otra operación en X, se dice que $\circ$ es* **distributiva a izquierda** *respecto de $*$ si*

$$x \circ (y * z) = (x \circ y) * (x \circ z), \quad \text{para todo} \quad x, y, z \in X \ ;$$

$y \circ$ es **distributiva a derecha** *respecto de $*$ si*

$$(x * y) \circ z = (x \circ z) * (y \circ z), \quad \text{para todo} \quad x, y, z \in X.$$

Definición. *Un* **anillo** *es una terna $A = (A, +, .)$ donde A es un conjunto , y " $+$" y " $.$" son operaciones en A, denominadas* **adición** *y* **multiplicación**, *respectivamente, tales que:*

(A1) *la adición es asociativa:*

$$(a + b) + c = a + (b + c), \quad \text{para todo} \quad a, b, c \in A \ ;$$

(A2) *la adición es conmutativa:*

$$a + b = b + a, \quad \text{para todo } a, b \in A \ ;$$

(A3) *existe un elemento, denotado 0, en A tal que*

$$a + 0 = a = 0 + a, \quad \text{para todo } a \in A \ ;$$

(A4) *para cada $a \in A$ existe un elemento, denotado $-a$, en A tal que*

$$a + (-a) = 0 = (-a) + a \ ;$$

(A5) *la multiplicación es asociativa:*

$$(a.b).c = a.(b.c), \quad \text{para todo } a, b, c \in A \ ;$$

(A6) *existe un elemento, denotado 1, en A tal que*

$$a.1 = a = 1.a, \quad \text{para todo } a \in A \ ;$$

(A7) *la multiplicación es distributiva, a los dos lados, respecto de la adición:*

$$a.(b + c) = (a.b) + (a.c) \quad y \quad (a + b).c = (a.c) + (b.c), \quad \text{para todo } a, b, c \in A \ .$$

Nota. Por convenio la multiplicación precede a la adición; esto es, la expresión $x + y.z$, que en principio es ambigua, significa $x + (y.z)$; analogamente, $a.b + a.c$ significa $(a.b) + (a.c)$; etc.

Propiedades elementales. *En todo anillo A se cumplen las siguientes propiedades:*

PE1. *Sólo existe un elemento* 0 *en* A *que verifique* **A1***; se le denomina el* **cero** *del anillo* A.

Demostración. Si $z \in A$ cumple $a + z = a = z + a$, para todo $a \in A$, entonces $z = z + 0 = 0$.

PE2. *Para cada* $a \in A$ *sólo existe un elemento* $-a \in A$ *que cumpla* **A4***; se dice que* $-a$ *es el* **opuesto** *de* a.

Demostración. Dado $a \in A$, si $a' \in A$ cumple $a + a' = 0 = a' + a$, entonces

$$a' = a' + 0 = a' + (a + (-a)) = (a' + a) + (-a) = 0 + (-a) = -a$$

PE3. *Se tienen:*

$-0 = 0$*;*
$-(-a) = a$*, para todo* $a \in A$*;*
$-(a + b) = -a - b$*, para todo* $a, b \in A$.

Demostración. Son consecuencias de las siguientes identidades:

$$0 + 0 = 0, \quad a + (-a) = 0 \quad \text{y} \quad a + b + (-a - b) = 0 \ ,$$

respectivamente.
[*Nótese que* $-a - b$ *quiere decir* $(-a) + (-b)$.]

PE4. *Sólo existe un elemento* 1 *en* A *que verifique* **A6***; se le denomina el* **uno** *ó la* **unidad** *del anillo* A.

Demostración. Si $u \in A$ cumple $au = a = ua$, para todo $a \in A$, entonces $u = u1 = 1$.

PE5. *Para todo* $a \in A$, $a.0 = 0 = 0.a$.

Demostración. La primera igualdad se obtiene de $a.0 = a.(0+0) = a.0 + a.0$ sumando el opuesto de $a.0$ al primer y último miembro; analogamente se prueba la otra identidad: $0.a = (0 + 0).a = 0.a + 0.a$.

PE6. *Para todo* $a, b \in A$ *se cumplen las identidades:*

$a.(-b) = (-a).b = -a.b$,
$(-a).(-b) = a.b$.

Demostración. Se tiene $0 = a0 = a(b + (-b)) = ab + a(-b)$, de ahí que $a(-b) = -ab$; etc

El conjunto $\{0\}$ con las operaciones $0 + 0 = 0$ y $0.0 = 0$ (¡las únicas posibles!) es un anillo, llamado el **anillo cero**; en este anillo $0 = 1$. Reciprocamente, si A es un anillo en el que $0 = 1$, entonces para cualquier $a \in A$ se tiene $a = 1.a = 0.a = 0$; por tanto $A = \{0\}$, el anillo cero. Normalmente excluiremos el anillo cero en nuestra exposición.

Notación. Habitualmente se simplifica la notación (si no hay peligro de confusión) en el siguiente sentido: en un producto indicado $a.b$ de dos factores a, b en un anillo A se suele omitir el punto "." que denota a la operación de multiplicación; así ab querrá decir $a.b$. En general, un producto de dos o más factores se escribe mediante simple yustaposición de éstos. Por ejemplo, la expresión

$$a_1 a_2 a_3 a_4$$

quiere decir

$$a_1.a_2.a_3.a_4$$

Definición. *Un* **subanillo** *de un anillo $A = (A, +, .)$ es un subconjunto S de A tal que:*

S1. *El cero de A está en S ($0 \in S$); en particular $S \neq \emptyset$;*
S2. *la suma de dos elementos de S está en S (si $x, y \in S$, entonces $x + y \in S$);*
S3. *el opuesto de cualquier elemento de S pertenece a S (si $x \in S$, entonces $-x \in S$);*
S4. *el elemento unidad de A pertenece a S ($1 \in S$); y*
S5. *el producto de dos elementos de S está en S (si $x, y \in S$, entonces $xy \in S$).*

Proposición. *Un subconjunto S de un anillo A es un subanillo de A si, y sólo si, cumple las tres propiedades siguientes:*

1. *$a - b \in S$ para todo $a, b \in S$;*
2. *$ab \in S$ para todo $a, b \in S$; y*
3. *$1 \in S$.*

Demostración. Se deja como ejercicio simple.

Si S es un subanillo de un anillo A, entonces las operaciones binarias de adición ($+$) y multiplicación ($.$) definidas en A se restringen a S (por **S2** y **S6**):

$$\begin{array}{ll} S \times S \to S & S \times S \to S \\ (x, y) \mapsto x + y & (x, y) \mapsto xy \end{array}$$

y S con estas operaciones restringidas es un anillo (compruébese esta afirmación).

Definición. *Dos elementos a y b en un anillo A* **conmutan** *si $ab = ba$; y un anillo A es* **conmutativo** *si todo par de elementos de A conmutan.*

Los anillos que trataremos en este curso serán conmutativos; por tanto, y con el fin de abreviar, el término "anillo" querrá decir "anillo conmutativo" (salvo mención expresa en sentido contrario en algún ejemplo particular).

Notas, ejemplos y ejercicios

A fin de familiarizar al lector con el concepto de anillo y con los demás conceptos elementales relacionados, y otros que se tratarán posteriormente, se exponen a continuación unos cuantos ejemplos de anillos; deberá notarse que en casi todos ellos lo que se hace es construir un anillo (conjunto y operaciones) a partir de otro u otros anillos. El lector bisoño deberá esforzarse en entender cada uno de los detalles relevantes, por ejemplo:

- ¿cómo es el conjunto base?
- ¿cómo son las operaciones?
- ¿cuál es el cero?
- ¿cómo es el opuesto de cada elemento?
- ¿cuál es el elemento unidad?
- etc.

Para ello se recomienda que compruebe las afirmaciones hechas con lápiz y papel, si es necesario.

(a) Los conocidos anillos de números enteros $\mathbf{Z}$, racionales $\mathbf{Q}$, reales $\mathbf{R}$ y complejos $\mathbf{C}$ con las operaciones usuales de adición y multiplicación respectivas. Todos ellos son conmutativos. El anillo $\mathbf{Z}$ es un subanillo del anillo $\mathbf{Q}$; $\mathbf{Q}$ es un subanillo de $\mathbf{R}$; y $\mathbf{R}$ es un subanillo de $\mathbf{C}$.

(b) El conjunto $\mathbf{Z}_2 = \{0, 1\}$, con las operaciones de adición y multiplicación dadas por las tablas adjuntas,

$+$	0	1
0	0	1
1	1	1

$\times$	0	1
0	0	0
1	0	1

es un anillo.
Con mayor generalidad, sea m un entero, el conjunto $\mathbf{Z}_m$ de las clases de restos de enteros módulo m con las operaciones de adición y de multiplicación de clases es un anillo conmutativo: el **anillo de clases de restos módulo** m. Nótese que $\mathbf{Z}_1$ es el anillo cero: $\{0\}$ (¿por qué?).

(c) Sean A y B anillos, el conjunto $A \times B$ de los pares (a, b) con $a \in A$ y $b \in B$ con las operaciones de adición y multiplicación definidas "componente a componente":

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),\ (a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2),$$

es un anillo, llamado el **producto directo** de los anillos A y B. El anillo $A \times B$ es conmutativo si, y sólo si, A y B lo son.

(d) Sea n un entero positivo y, para cada $i = 1, \ldots, n$, sea A_i un anillo; el conjunto

$$\prod_{i=1}^{n} A_i = A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) \mid a_i \in A_i, i = 1, \ldots, n\}$$

con las operaciones de adición y multiplicación definidas "componente a componente":

$$(a_i)_{1 \le i \le n} + (b_i)_{1 \le i \le n} = (a_i + b_i)_{1 \le i \le n} \quad \text{y} \quad (a_i)_{1 \le i \le n}(b_i)_{1 \le i \le n} = (a_i b_i)_{1 \le i \le n}$$

es un anillo llamado el **producto directo** de los anillos $A_1, \ldots, A_n$. Como caso particular, si todos los anillos $A_1, \ldots, A_n$ son copias de (iguales a) un mismo anillo A, entonces el producto directo $A \times \ldots \times A$ (n factores A) se denota A^n.

(e) El conjunto $\mathbf{R}^X$ de las funciones reales definidas en un conjunto $X \neq \varnothing$ (con las operaciones usuales) es un anillo (conmutativo): si $f, g \in \mathbf{R}^X$, se definen $f + g$ y fg en la forma

$$(f + g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)g(x), \text{ para todo } x \in X.$$

(e1) Como caso particular, $X = \mathbf{R}$, considérese el conjunto $\mathcal{F}(\mathbf{R}, \mathbf{R}) = \mathbf{R}^{\mathbf{R}}$ de las funciones definidas en (todo) $\mathbf{R}$ y que toman valores en $\mathbf{R}$:

$$\mathcal{F}(\mathbf{R}, \mathbf{R}) = \mathbf{R}^{\mathbf{R}} = \{f \mid f : \mathbf{R} \to \mathbf{R}\}$$

Son ejemplos de elementos de este conjunto las funciones

$$f_1(x) = \operatorname{sen}(x),\ f_2(x) = \frac{x^2}{x^2 + 1},\ h(x) = \cos(x^2),\ g(x) \begin{cases} = 1, & \text{si } x \text{ es racional} \\ \\ = 0, & \text{si } x \text{ no es racional} \end{cases} \qquad (x \in \mathbf{R})$$

Sin embargo, funciones tales como

$$u(x) = \frac{x}{x - 1},\ v(x) = \tan(x),\ w(x) = \log(x)$$

no pertenecen al conjunto $\mathcal{F}(\mathbf{R}, \mathbf{R})$ (¿por qué?).
El conjunto $\mathcal{C}(\mathbf{R}, \mathbf{R})$ de las funciones continuas definidas en (todo) $\mathbf{R}$ y que toman valores en $\mathbf{R}$ es un subanillo del anillo $\mathcal{F}(\mathbf{R}, \mathbf{R})$.

(f) Para un entero positivo n dado, el conjunto $\mathrm{M}_n(\mathbf{Q})$ de las matrices cuadradas $n \times n$ con coeficientes racionales, junto con las operaciones de adición y multiplicación de matrices, es un anillo (no conmutativo si $n > 1$).

(g) El anillo $\mathbf{Q}[x]$ de los polinomios en una indeterminada x con coeficientes racionales (anillo conmutativo).

(h) El anillo $\mathbf{Z}[i]$ de los enteros de Gauss (anillo conmutativo).

$$\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\}$$

El anillo $\mathbf{Z}[i]$ es un subanillo del anillo $\mathbf{C}$ de los números complejos.

(i) El conjunto

$$\mathbf{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$$

con las operaciones

$$(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = a_1 + a_2 + (b_1 + b_2)\sqrt{2}$$
$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = a_1a_2 + 2b_1b_2 + (a_1b_2 + a_2b_1)\sqrt{2}$$

es un subanillo del anillo $\mathbf{R}$ de los números reales.

Sumas y productos. Múltiplos enteros y potencias

Sean n y m números naturales y sea

$$S = (a_i)_{n \le i \le m} = (a_n, a_{n+1}, a_{n+2}, \ldots, a_i, \ldots, a_{m-1}, a_m)$$

una sucesión (finita) de elementos de un anillo A. La **suma de la sucesión** S es

$$\sum_{i=n}^{m} a_i \begin{cases} = 0 \text{ (el cero del anillo } A), & \text{si } n \ge m \\ = a_n + \displaystyle\sum_{i=n+1}^{m} a_i, & \text{si } n \le m \end{cases}$$

El **producto de la sucesión** S es

$$\prod_{i=n}^{m} a_i \begin{cases} = 1 \text{ (el uno del anillo } A), & \text{si } n \ge m \\ = a_n \displaystyle\prod_{i=n+1}^{m} a_i, & \text{si } n \le m \end{cases}$$

Frecuentemente surgen sumas (respectivamente productos) en que se repite un mismo sumando (respectivamente factor) varias veces:

$$a + a + a + \ldots + a + \ldots + a$$
$$aaa \ldots a \ldots a$$

Conviene formalizar estas situaciones.

Definición. *Sean a un elemento de un anillo A y n un entero. Se pone:*

$$na \begin{cases} = 0, & \text{si } n = 0, \\ = a + (n-1)a, & \text{si } n > 0, \\ = (-n)(-a), & \text{si } n < 0. \end{cases}$$

Analogamente, para todo entero $n \ge 0$ se pone:

$$a^n \begin{cases} = 1, & \text{si } n = 0 \\ = aa^{n-1}, & \text{si } n > 0. \end{cases}$$

Nota. Deberán distinguirse los conceptos "múltiplo entero" (na donde $n \in \mathbf{Z}$ y $a \in A$) y "múltiplo en el anillo" (ba donde $b \in A$ y $a \in A$).

Proposición. *Sean a y b elementos de un anillo A, m y n enteros (resp. enteros no negativos para las potencias). Se tienen:*

(i)	$m(a+b) = ma + mb$;	**(i′)**	$(ab)^m = a^m b^m$, (si $ab = ba$);
(ii)	$(m+n)a = ma + na$;	**(ii′)**	$a^{m+n} = a^m a^n$;
(iii)	$m(na) = (mn)a$;	**(iii′)**	$(a^n)^m = a^{mn}$;
(iv)	$1a = a$;	**(iv′)**	$a^1 = a$;
(v)	$n(ab) = (na)b$ *[En particular,* $na = (n.1)a$*, aquí* 1 *es la unidad de* A*].*		

Nota. La propiedad **(i′)** se cumple siempre en anillos conmutativos ó si a y b conmutan, pero téngase en cuenta el siguiente contraejemplo: Considerar las matrices

$$a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

con coeficientes en cualquier anillo distinto del anillo cero; se tiene:

$$(ab)^2 = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix} \quad \text{y} \quad a^2b^2 = \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}.$$

Por tanto $(ab)^2 \neq a^2b^2$, ya que en todo anillo (distinto del anillo cero) $2 \neq 1$.

Proposición. *Sean a y b elementos de un anillo (conmutativo) A, y sea n un número natural. Se tiene:*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

Divisores de cero y unidades

Definición. *Un elemento $a \neq 0$ de un anillo A es un* **divisor de cero** *si $ab = 0$ para algún $b \neq 0$ de A. Un* **dominio de integridad** *es un anillo conmutativo distinto del anillo cero que no posea divisores de cero.*

Proposición. *Un anillo A es un dominio de integridad si, y sólo si,*

- $A \neq \{0\}$,
- *A es conmutativo y*
- *para todo $x, y \in A$, la relación $xy = 0$ implica $x = 0$ ó $y = 0$.*

Ejemplo 1. En el anillo $\mathbf{Z}_6$ de clases de restos de enteros módulo 6 se tienen las igualdades:

$$2 \times 3 = 0 \quad \text{y} \quad 4 \times 3 = 0$$

por tanto 2, 3 y 4 son divisores de cero en $\mathbf{Z}_6$; pero ni 1 ni 5 son divisores de cero. El anillo $\mathbf{Z}_6$ no es un dominio de integridad.

Ejemplo 2. El anillo $\mathbf{Z}_7$ es un dominio de integridad. ¿Por qué?

Ejemplo 3. El anillo $\mathcal{F}(\mathbf{R}, \mathbf{R})$, descrito previamente en el ejemplo **(e1)**, no es un dominio de integridad. Describir dos funciones $f_1, f_2 \in \mathcal{F}(\mathbf{R}, \mathbf{R})$, $f_1 \neq 0$, $f_2 \neq 0$, y tales que $f_1 f_2 = 0$.

Ejemplo 4. Sea A cualquier anillo conmutativo, $A \neq \{0\}$; por ejemplo $A = \mathbf{Z}$ ó $A = \mathbf{Z}_m$ para cualquier entero $m \geq 2$. En el anillo $M_2(A)$ de las matrices 2×2 con coeficientes en A pongamos

$$a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{y} \quad b = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix};$$

se tiene

$$ab = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ mientras que } ba = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ (el cero del anillo).}$$

Ejemplo 5. El anillo $\mathbf{Z}$ de los números enteros es un dominio de integridad.

Definición. *Un elemento u de un anillo A es una* **unidad** *si existe u' en A tal que $uu' = 1 = u'u$.*

Proposición. *Si u es una unidad de un anillo A, sólo hay un elemento $u' \in A$ que cumpla $uu' = 1 = u'u$.*

Definición. *Si u es una unidad de un anillo A, el elemento u' tal que $uu' = 1 = u'u$ es el* **inverso** *de u y se escribe $u' = u^{-1}$. Se denota $\mathrm{U}(A)$ al conjunto de las unidades de un anillo A.*

Proposición. *Sea A un anillo.*
(1) Si $u \in \mathrm{U}(A)$, entonces $u^{-1} \in \mathrm{U}(A)$; y se tiene $(u^{-1})^{-1} = u$.
(2) $1 \in \mathrm{U}(A)$; y se tiene $1^{-1} = 1$.
(3) Si $u, v \in \mathrm{U}(A)$, entonces el producto $u.v \in \mathrm{U}(A)$; y se tiene $(u.v)^{-1} = v^{-1}.u^{-1}$.
(4) El conjunto $\mathrm{U}(A)$, con la multiplicación de A restringida a él, es por tanto un grupo llamado el **grupo de las unidades** *del anillo A.*

Ejemplos:
(a) $\mathrm{U}(\mathbf{Z}) = \{1, -1\}$.
(b) $\mathrm{U}(\mathbf{Q}) = \mathbf{Q}^* = \{q \in \mathbf{Q} \mid q \neq 0\}$.
(c) $\mathrm{U}(M_n(\mathbf{Q})) = \mathrm{GL}(n, \mathbf{Q})$.

Definición. *Un* **cuerpo** *es un anillo distinto del anillo cero ($0 \neq 1$) y en el que todo elemento $\neq 0$ es una unidad. Por tanto un anillo $K = (K, +, .)$ es un cuerpo si y sólo si $K \neq \{0\}$ y $\mathrm{U}(K) = K \setminus \{0\}$.*

Ejemplos:
(a) $\mathbf{Z}_2$ es un cuerpo.
(b) Los cuerpos $\mathbf{Q}$, $\mathbf{R}$ y $\mathbf{C}$.
(c) El anillo $\mathbf{Q} \times \mathbf{Q}$ no es un cuerpo; ¿por qué?.

Proposición. *Todo subanillo de un cuerpo es un dominio de integridad; en particular, todo cuerpo es un dominio de integridad.*

Ideales. Anillos cociente. Teoremas de isomorfismo

Definición. *Una* **congruencia** *en un anillo (conmutativo) $A = (A, +, .)$ es una relación de equivalencia R en el conjunto A (soporte de la estructura de anillo) que sea compatible con las operaciones del anillo, en el sentido: Para todo $a, a', b, b' \in A$, si*

$$a \ R \ a' \quad y \quad b \ R \ b',$$

entonces

$$(a + b) \ R \ (a' + b') \quad y \quad (ab) \ R \ (a'b')$$

Ejemplo. Para cualquier entero m, la congruencia módulo m en $\mathbf{Z}$ es una congruencia en el anillo de los enteros.

Sea R una congruencia en un anillo A. Denotemos, como es habitual, $[a]_R$ o bien $[a]$, a la clase de equivalencia de un elemento cualquiera a de A con respecto a la relación de equivalencia R. Sea

$$A/R = \{[a] \mid a \in A\}$$

el correspondiente conjunto cociente. Dados $[a]$ y $[b]$ en A/R, las relaciones

$$[a] + [b] = [a + b] \quad \text{y} \quad [a][b] = [ab], \quad \text{con} \quad a \in [a], \ b \in [b],$$

definen dos operaciones binarias internas en el conjunto cociente A/R: En efecto, por ser R una congruencia en A, se tiene si $a, a' \in [a]$, y $b, b' \in [b]$, entonces $(a+b)\ R\ (a'+b')$ y $(ab)\ R\ (a'b')$, por tanto $[a+b] = [a'+b']$ y $[ab] = [a'b']$; esto garantiza la buena definición de las operaciones mediante la elección de representantes arbitrarios de las clases de equivalencia respectivas.

Quedan así definidas dos operaciones binarias internas en el conjunto cociente A/R, heredadas de las respectivas operaciones del anillo A:

$$\begin{array}{ll} A/R \times A/R \to A/R & A/R \times A/R \to A/R \\ ([a]\ ,\ [b]) \ \mapsto [a+b] & ([a]\ ,\ [b]) \ \mapsto [a.b] \end{array}$$

El conjunto cociente A/R con estas operaciones pasa a ser un anillo (conmutativo): Es una simple comprobación rutinaria.

Definición. *El anillo construido anteriormente sobre el conjunto A/R a partir de una congruencia R en un anillo A se denomina el* **anillo cociente de A por la congruencia R.**

Ejemplo. El anillo de clases de restos módulo m: $\mathbf{Z}/\equiv_m$ ó $\mathbf{Z}/(m)$, es el anillo cociente del anillo $\mathbf{Z}$ por la congruencia módulo m.

Nuestro próximo objetivo es tratar de dar respuesta a la siguiente pregunta ¿Cómo se pueden describir todas las congruencias en un anillo A?.

Proposición. *Sea R una congruencia en un anillo A. El conjunto $I = [0]$ verifica las siguientes propiedades:*
(1) *I es un subgrupo del grupo aditivo $(A, +)$ del anillo A.*
(2) *Para todo $a \in A$ y todo $m \in I$, se tiene $ma \in I$ y $am \in I$.*
(3) *Para todo $a, a' \in A$, aRa' si y sólo si $a - a' \in I$.*

Demostración. Téngase en cuenta que $I = \{x \in A \mid xR0\}$
(1) Como $0R0$ por reflexividad de R, se tiene $0 \in [0]$. Si $x, y \in [0]$, entonces $xR0$ e $yR0$, de donde $(x+y)R0$, con lo que $x + y \in [0]$. Si $x \in [0]$, entonces $xR0$, por otra parte $(-x)R(-x)$, por reflexividad de R, por tanto se tiene que $0R(-x)$; esto es, $(-x) \in [0]$.
(2) De las relaciones aRa y $mR0$ se deduce $(am)R0$ y $(ma)R0$; esto es, $am \in [0]$ y $ma \in [0]$.
(3) Si aRa', teniendo en cuenta que $(-a')R(-a')$, se obtiene $(a-a')R0$; esto es, $a-a' \in [0]$. Reciprocamente, si $a - a' \in [0]$, teniendo en cuenta que $a'Ra'$, se obtiene aRa'.

Definición. *Un* **ideal** *de un anillo A es un subconjunto M de A tal que*
(a) *M es un subgrupo del grupo aditivo $(A, +)$ del anillo A; y*
(b) *para todo $a \in A$ y todo $m \in M$, $am \in M$ y $ma \in M$.*

Corolario. *Si R es una congruencia en un anillo A, el conjunto $I = [0]$ es un ideal de A que representa a la congruencia R en el sentido:*

$$\text{para todo } a, a' \in A: \ aRa' \text{ si y sólo si } a - a' \in I.$$

Sea R una congruencia en un anillo A y sea $I = [0]$. Para un $a \in A$ se tiene: $x \in [a]$ si y sólo si xRa si y sólo si $x = a + m$ para algún $m \in I$. De ahí que

$$[a] = \{a + m \mid m \in I\};$$

es costumbre representar este conjunto mediante la notación $a + I$ (abuso de notación), y el anillo cociente A/R se denota A/I; las operaciones definidas en el anillo cociente se expresan ahora

$$(a + I) + (b + I) = a + b + I \text{ y } (a + I)(b + I) = ab + I,$$

el cero del anillo cociente A/I es $[0] = 0+I = I$, la clase opuesta de una clase $[a] = a+I$ es $-[a] = -(a+I) = -a + I$, y el elemento unidad es $[1] = 1 + I$.

Reciprocamente, un ideal I de un anillo A proporciona una congruencia R en A de forma que I es precisamente el ideal asociado a la congruencia R en el sentido de la construcción anterior, basta definir, para elementos $a, a' \in A$,

$$aRa' \text{ si y sólo si } a - a' \in I.$$

Ejercicio. Comprobar que la relación R así definida en A es una congruencia en el anillo A y que la clase de cero ($[0]$) respecto de R es el ideal I.

Queda así establecida una biyección entre el conjunto de las congruencias en un anillo A y el conjunto de los ideales de A.

Proposición. *Sea $(I_h)_{h\in H}$ una familia de ideales de un anillo A. La intersección $\bigcap_{h\in H} I_h$ es un ideal de A.*

Demostración. Ejercicio.

En particular, la interseción $I \cap J$ de dos ideales I y J de A es un ideal de A; además, $I \cap J \subseteq I$ e $I \cap J \subseteq J$; y si K es un ideal de A tal que $K \subseteq I$ y $K \subseteq J$, entonces $K \subseteq I \cap J$. Por tanto, la intersección $I \cap J$ de dos ideales I y J de un anillo A es el mayor ideal (respecto de la relación de inclusión) de A contenido en I y en J.

Dualmente, ¿existe el menor ideal $M(I, J)$ de A que contenga a dos ideales dados I y J? La proposición anterior proporciona directamente una respuesta afirmativa: basta considerar la intersección de todos los ideales de A que contienen a I y a J. Veamos una descripción explícita de los elementos de este ideal; evidentemente, todo elemento de I y todo elemento de J debe estar en $M(I, J)$, por tanto deben estar en $M(I, J)$ todas las sumas $u + v$ con $u \in I$ y $v \in J$. Pongamos

$$I + J = \{u + v \mid u \in I \text{ y } v \in J\};$$

es fácil comprobar que $I + J$ es un ideal de A que contiene a I y a J; además, si L es un ideal de A que contiene a I y a J entonces L contiene a $I + J$. Así $M(I, J) = I + J$. Se dice que el ideal $I + J$ es la **suma** de los ideales I y J.

Resulta de la discusión anterior que en el conjunto ordenado (por inclusión) $\mathcal{I}(A)$ de los ideales de un anillo A cada par de elementos I y J posee un supremo: $I + J$ y un ínfimo: $I \cap J$. De este modo $\mathcal{I}(A)$ es un retículo: el **retículo de los ideales** del anillo A.

Hay cierto tipo de anillos (los que más adelante denominaremos "dominios de ideales principales") en los que todos sus ideales poseen una estructura particularmente simple. El anillo $\mathbf{Z}$ de los enteros es uno de estos según se prueba en el siguiente resultado.

Teorema. (Estructura de los ideales del anillo $\mathbf{Z}$ de los enteros). *Sea m un entero; el conjunto*

$$(m) = \{mz \mid z \in \mathbf{Z}\}$$

es un ideal del anillo $\mathbf{Z}$. Reciprocamente, si I es un ideal de $\mathbf{Z}$, existe un único entero $m \geq 0$ tal que $I = (m)$.

Demostración. La comprobación de la primera afirmación es sencilla; pasemos a la segunda. Sea I un ideal de $\mathbf{Z}$; si $I = \{0\}$, tomar $m = 0$; si $I \neq \{0\}$, existe al menos un enteros no nulo u en I. Por ser I un ideal, $-u \in I$; por tanto hay al menos un entero positivo en I. Sea m el menor entero positivo en I. Como $m \in I$ e I es un ideal, resulta que $mz \in I$ para todo entero z; de ahí que $(m) \subseteq I$. Por otra parte, sea $x \in I$, pongamos $x = mq + r$ con $0 \leq r < m$; entonces $r = x - mq \in I$ y, por elección de m, debe ser $r = 0$; esto es, $x = mq \in (m)$. Con lo que $I \subseteq (m)$. Finalmente, si m y n son enteros positivos y $(m) = (n)$, entonces $m = na$ y $n = mb$ para algún entero a y algún entero b positivos; de ahí que $n = nab$, con lo que $ab = 1$, lo cual implica $a = b = 1$, y $m = n$.

Definición. *Sea m un entero, el ideal (m) de $\mathbf{Z}$ se denomina* **principal** *o* **monógeno**, *y m es un* **generador** *del ideal (m).*

Corolario. *El anillo $\mathbf{Z}$ de los enteros es un dominio de integridad en el que todo ideal es principal.*

Hay una estrecha conexión entre la relación de inclusión "$\subseteq$" en el retículo $\mathcal{I}(\mathbf{Z})$ y la relación de divisivilidad "$|$" en $\mathbf{Z}$:

Proposición. *Sean m y n enteros positivos, $(m) \subseteq (n)$ si y sólo si $n \mid m$.*

Demostrción. Inmediata.

Ejercicio. Sean m y n enteros. Encontrar enteros a y b que cumplan:

$$(a) = (m) + (n);\ (b) = (m) \cap (n).$$

Para un ideal cualquiera I de un anillo A, la aplicación natural $\pi : A \to A/I$ tal que

$$\pi(a) = a + I,\ (a \in A)$$

verifica las propiedades:
$\pi(a+b) = \pi(a) + \pi(b),\ (a, b \in A)$;
$\pi(ab) = \pi(a)\pi(b),\ (a, b \in A)$; y
$\pi(1) = 1 + I$ (el elemento unidad del anillo cociente A/I).

Definición. *Un* **homomorfismo** *de un anillo A en un anillo B es una aplicación*

$$f : A \to B$$

tal que
$f(a+b) = f(a) + f(b)$ *para todo* $a, b \in A$;
$f(ab) = f(a)f(b)$ *para todo* $a, b \in A$; *y*
$f(1) = 1$.

Ejemplos.

(1.) Sea m un número entero. La aplicación p_m del anillo $\mathbf{Z}$ de los enteros en el anillo $\mathbf{Z}_m$ de las clases de restos módulo m tal que

$$p_m(a) = [a]_m, (a \in \mathbf{Z}),$$

es un homomorfismo de anillos.

(2.) Sean m y n enteros. La aplicación $p : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n$, $p(a) = \big([a]_m, [a]_n\big),\ (a \in \mathbf{Z})$, es un homomorfismo del anillo $\mathbf{Z}$ de los enteros en el anillo $\mathbf{Z}_m \times \mathbf{Z}_n$ producto cartesiano de los anillos $\mathbf{Z}_m$ y $\mathbf{Z}_n$.

(3.) La inclusión canónica $j : \mathbf{Z} \to \mathbf{Q}$, $j(a) = \frac{a}{1}$, $(a \in \mathbf{Z})$, es un homomorfismo de anillos.

(4.) ¿Es un homomorfismo de anillos la aplicación $f : \mathbf{C} \to \mathbf{R}$ tal que $f(x + yi) = x$?.

(5.) Sean A y B anillos. La aplicación $p_A : A \times B \to A$, $p_A(a, b) = a$, $(a \in A)$ es un homomorfismo del anillo producto cartesiano $A \times B$ en el anillo A.

Ejercicio. Sean S un conjunto y A un anillo. Probar:
(1) El conjunto $F(S, A)$ de todas las aplicaciones de S en A con las operaciones de adición y multiplicación definidas "punto a punto" es un anillo;
(2) Si s es un elemento fijo de S, la aplicación

$$e_s : F(S, A) \to A,\ e_s(f) = f(s),\ (f \in F(S, A))$$

es un homomorfismo de anillos.

Propiedades inmediatas. *Sea f un homomorfismo de un anillo A en un anillo B. Entonces*
(1) $f(0) = 0$;
(2) $f(-a) = -f(a)$, para todo $a \in A$;
(3) $f(a-b) = f(a) - f(b)$, para todo $a, b \in A$;
(4) Si un elemento u de A es una unidad, entonces $f(u)$ es una unidad de B y se tiene $f(u^{-1}) = f(u)^{-1}$.

Demostración.
(1) $f(0) = f(0+0) = f(0) + f(0)$;
(2) $0 = f(0) = f(a-a) = f(a+(-a)) = f(a) + f(-a)$;
(3) $f(a-b) = f(a+(-b)) = f(a) + f(-b) = f(a) - f(b)$;
(4) Si u es una unidad en el anillo A, existe su inverso u^{-1} en A de modo que $1 = uu^{-1} = u^{-1}u$; por tanto

$$1 = f(1) = f(uu^{-1}) = f(u)f(u)^{-1} \text{ y } 1 = f(1) = f(u^{-}1u) = f(u)^{-1}f(u).$$

Definición. *Un* **isomorfismo** *de anillos es un homomorfismo biyectivo de anillos. Con mayor precisión, un isomorfismo de un anillo A en un anillo B es una aplicación $f : A \to B$ biyectiva y que sea homomorfismo. Dos anillos A y B son* **isomorfos** *si hay un isomorfismo de uno en otro; la relación "el anillo A es isomorfo al anillo B" se abrevia $A \cong B$.*

Proposición.
(1) Para un anillo cualquiera A, la aplicación identidad $1_A : A \to A$, $1_A(a) = a$, es un isomorfismo de anillos.
(2) Sean A y B anillos, si $f : A \to B$ es un isomorfismo de anillos, entonces la aplicación inversa $f^{-1} : B \to A$ es también un isomorfismo de anillos.
(3) Sean A, B y C anillos, si $f : A \to B$ y $g : B \to C$ son isomorfismos de anillos, entonces la aplicación compuesta $g \circ f : A \to C$ es también un isomorfismo de anillos.

Demostración. Es una simple comprobación rutinaria que se deja como ejercicio.

En consecuencia, la relación "es isomorfo a" es una relación de equivalencia entre anillos; una clase de equivalencia está formada por un anillo y todos los isomorfos a él. Desde un punto de vista algebraico, dos anillos isomorfos son considerados iguales o identificables; un isomorfismo explícito entre ellos permite realizar la identificación.

Ejemplo. Fijada una base $B = (b_1, b_2, \ldots, b_n)$ en un espacio vectorial V de dimensión finita n sobre un cuerpo conmutativo k, considerar la aplicación

$$M : \mathrm{End}_k(V) \to \mathrm{M}_n(k)$$

que a cada k-endomorfismo φ de V asocia su matriz $M(\varphi, B)$ con respecto a la base escogida B de V. Como es bien conocido, la aplicación M es un isomorfismo de anillos. Es este un ejemplo de isomorfismo no canónico o no natural por depender la definición del isomorfismo M de la elección arbitraria de un objeto: una base B de V; más adelante se verán ejemplos de isomorfismos naturales.

Definición. *El* **núcleo** *de un homomorfismo de anillos $f : A \to B$ es el conjunto*

$$Ker(f) = \{x \in A \mid f(x) = 0\},$$

y la imagen de f es el conjunto

$$Im(f) = \{f(x) \mid x \in A\}.$$

Teorema (fundamental de homomorfismos de anillos)**.** *Sea $f : A \to B$ un homomorfismo de anillos. Se cumplen:*
(1) $Ker(f)$ es un ideal del anillo A;
(2) $Im(f)$ es un subanillo del anillo B;

(3) la aplicación $\overline{f} : A/Ker(f) \to Im(f)$, $\overline{f}(a + Ker(f)) = f(a)$, $(a + Ker(f) \in A/Ker(f))$, *es un isomorfirmo de anillos. En particular,*

$$A/Ker(f) \cong Im(f).$$

Demostracion.

Nótese que la congruencia R en el anillo A asociada al ideal $Ker(f)$ coincide con la relación de equivalencia R_f en A asociada a la aplicación f; esto es, si $a, a' \in A$, son equivalentes aRa' y $f(a) = f(a')$. De ahí que, para un elemento $a \in A$, la clase de congruencia $a + Ker(f)$ está constituida por a y todos los elementos $x \in A$ cuya imagen por f coincide con la imagen de a:

$$a + Ker(f) = \{x \in A \mid f(x) = f(a)\}.$$

El efecto de la aplicación $\overline{f} : A/Ker(f) \to Im(f)$ es entonces enviar cada clase $a + Ker(f)$ en la imagen por f, $f(a)$, común a todos los los elementos $x \in a + Ker(f)$.

Teorema (de la correspondencia)**.** *Sea $f : A \to B$ un homomorfismo suprayectivo de un anillo A sobre un anillo B. Pongamos $K = Ker(f)$. Hay una biyección entre el conjunto de los ideales I de A que contienen a K (resp., subanillos S de A que contienen a K) y el conjunto de los ideales de B (resp., subanillos de B):*

$$\{I \mid I \text{ ideal de } A, K \subseteq I\} \longrightarrow \{H \mid H \text{ ideal de } B\}$$

$$I \mapsto f(I)$$

$$\{S \mid S \text{ subanillo de } A, K \subseteq S\} \longrightarrow \{R \mid R \text{ subanillo de } B\}$$

$$S \mapsto f(S)$$

Además, si I es un ideal de A que contiene a K, entonces la aplicación

$$A/I \longrightarrow B/f(I)$$

$$a + I \mapsto f(a) + f(I)$$

es un isomorfismo de anillos (segundo teorema de isomorfismo de anillos).

Demostración.

Teorema (primer teorema de isomorfismo de anillos)**.** *Sean A un anillo, S un subanillo de A e I un ideal de A. Entonces:*
(1) El conjunto $S + I = \{s + i \mid s \in S, i \in I\}$ es un subanillo de A;
(2) I es un ideal de $S + I$;
(3) El conjunto $S \cap I$ es un ideal de S;
(4) La aplicación

$$(S + I)/I \longrightarrow S/(S \cap I)$$

$$s + I \mapsto s + (S \cap I)$$

es un isomorfismo de anillos.

Demostración.

Sea A un anillo; la aplicación $j : \mathbf{Z} \to A$ tal que $j(n) = n.1, (n \in \mathbf{Z})$ es claramente un homomorfismo de anillos (recuérdense las propiedades de los múltiplos enteros de los elementos de un anillo, en el tema 4). El conjunto

$$j(\mathbf{Z}) = \{n.1 \mid n \in \mathbf{Z}\} = \mathbf{Z}.1$$

es un subanillo de A; y cualquier subanillo de A contiene a $\mathbf{Z}.1$ (¿por qué?); de modo que $\mathbf{Z}.1$ es el menor subanillo de A. Se dice que $\mathbf{Z}.1$ es el **anillo primo** del anillo A. Es fácil describir la estructura del anillo primo de cualquier anillo: Por el teorema fundamental de homomorfismos y por el teorema de estructura de los ideales de $\mathbf{Z}$, existe un entero $c \geq 0$ tal que $\mathbf{Z}/(c) \cong Z.1$. En consecuencia si $c = 0$, el anillo A contiene una copia del anillo $\mathbf{Z}$ de los enteros como anillo primo; esto ocurre exactamente cuando $n.1 \neq 0$ para todo entero $n > 0$; por el contrario, si $c \neq 0$, entonces el anillo A contiene una copia del anillo de clases de restos $\mathbf{Z}/(c)$ con $c > 0$ y donde c es precisamente el menor entero positivo que cumple $c.1 = 0$. El número entero c se denomina la **característica** del anillo A : $c = car(A)$.

BIBLIOGRAFIA.

Jacobson N. Basic Algebra I. Páginas 98 a 108.

EJERCICIOS

1. Sean a y b elementos de un anillo A no necesariamente conmutativo. Si $ab = ba$, entonces

1.1 se cumple la fórmula del **binomio de Newton**:

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

para todo entero $n \geq 0$.

1.2 se cumple

$$a^n - b^n = (a-b) \sum_{i=1}^{n} a^{n-i} b^{i-1}$$

para todo entero $n \geq 1$.

2. Sea A un anillo (conmutativo). Se denota por $A^{\mathbf{N}}$ el conjunto de todas las aplicaciones de $\mathbf{N}$ en A; esto es, el conjunto de todas las sucesiones de elementos de A. Se definen dos operaciones en $A^{\mathbf{N}}$: Si $a, b \in A^{\mathbf{N}}$,

$$(a+b)(i) = a(i) + b(i), (i \in N)$$

y

$$(a.b)(i) = \sum_{j=0}^{i} a(j)b(i-j)), (i \in \mathbf{N}).$$

Empleando otra notación: pongamos

$$a = (a_0, a_1, a_2, \ldots, a_i, \ldots) \text{ y } b = (b_0, b_1, b_2, \ldots, b_i, \ldots),$$

entonces

$$a + b = (s_0, s_1, s_2, \ldots, s_i, \ldots)$$

donde $s_i = a_i + b_i$, para $i = 0, 1, 2, \ldots,$
y

$$a.b = (p_0, p_1, p_2, \ldots, p_i, \ldots)$$

donde $p_i = a_0 b_i + a_1 b_{i-1} + a_2 b_{i-2} + \cdots + a_j b_{i-j} + \cdots + a_i b_0$, para $i = 0, 1, 2, \ldots$.
Probar que el conjunto $A^{\mathbf{N}}$ dotado de estas operaciones es un anillo conmutativo.

3. Sea A un anillo (conmutativo). Se denota por $A^{(\mathbf{N})}$ el conjunto de los elementos a de $A^{\mathbf{N}}$ tales que $a(i) = 0$ para todo $i \in \mathbf{N}$ salvo una cantidad finita; esto es, un elemento a de $A^{\mathbf{N}}$ está en $A^{(\mathbf{N})}$ si y sólo si existe un $m \in \mathbf{N}$ tal que $a(i) = 0$ para todo $i \in \mathbf{N}, i \geq m$. Probar que $A^{(\mathbf{N})}$ es un subanillo de $A^{\mathbf{N}}$.

4. Probar que en la definición de anillo la conmutatividad de la adición es consecuencia de los restantes postulados, por tanto es redundante.

5. Sea

$$S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbf{R} \right\}.$$

Probar que S es un anillo (subanillo del anillo $\mathrm{M}_2(\mathbf{R})$ de las matrices 2×2 con coeficientes reales). ¿Es S conmutativo? ¿Es S un cuerpo?

6. Definición. Un elemento a de un anillo A (no necesariamente conmutativo) es **nilpotente** si $a^n = 0$ para algún entero $n \geq 1$. Y un elemento u de A es **unipotente** si $1 - u$ es nilpotente.

6.1 Probar que en $\mathrm{M}_n(K)$, n un entero positivo y K un cuerpo conmutativo, las matrices de la forma

$$\begin{pmatrix} 0 & * & * & \cdots & * & * \\ 0 & 0 & * & \cdots & * & * \\ 0 & 0 & 0 & \cdots & * & * \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 & * \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

son nilpotentes. (Aquí se supone que las entradas $*$ se rellenan arbitrariamente con elementos del cuerpo K.

6.2 Sean a y b elementos nilpotentes de un anillo A, tales que $ab = ba$. Probar que $a + b$ y ab son nilpotentes.

6.3 Si u, v son elementos unipotentes de A y $uv = vu$, entonces uv es también unipotente.

6.4 Si u es un elemento unipotente de A, entonces u es una unidad, y su inverso u^{-1} es también unipotente.

6.5 Sea $X \in \mathrm{M}_n(K)$ una matriz cuadrada nilpotente. Entonces la matriz $I - X$ posee inversa y se tiene

$$(I - X)^{-1} = I + X + X^2 + X^3 + \cdots .$$

6.6 Calcular la inversa de cada una de las matrices siguientes

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$