Universidad
Europea de Madrid

LAUREATE INTERNATIONAL UNIVERSITIES

LEYES, ESTRUCTURAS BÁSICAS Y COCIENTES

ANILLOS Y CUERPOS

Índice

Presentación 4

Definición de anillo 5

Axioma 1 5

Axioma 2 5

Axioma 3 5

Veamos un ejemplo 6

Comprobemos si es un anillo 6

Axioma 1. Grupo abeliano 7

Axiomas 2 y 3 8

Los "apellidos" de un anillo 9

Anillos íntegros 10

Subanillo 11

Subanillo ideal. Característica 12

Característica de un anillo 12

Homomorfismos entre anillos 13

Grupo multiplicativo de un anillo 14

Pero, ¿qué es un cuerpo? 15

Axioma 1 15

Axioma 2 15

Axioma 3 15

Integridad de un cuerpo 16

Resumen 17

Presentación

El paso de conjunto a grupo es un cambio dramático dentro de la estructura del conjunto debido a la inclusión de una simple ley de composición interna. Si además de esa primera ley, añadimos una segunda, la estructura resultante es aún más compleja, si cabe, que el grupo, pero igual de sólida. Surge el anillo.

Los anillos son estructuras algebraicas fascinantes, que pueden volverse muy sofisticadas según el número de propiedades que cumple cada una de sus dos leyes. Cuando ese tope de propiedades llega a una determinada cota, surge una cuarta estructura: el cuerpo.

Los cuerpos son una estructura muy potente, tanto, que los utilizamos día a día en toda clase de matemáticas. Los números reales forman un cuerpo, y los complejos también.

Descubramos todo lo que hay que saber sobre anillos y cuerpos en este tema y muchas cosas más...

Definición de anillo

Un anillo (A; +,·), es una terna. Una estructura matemática formada por un conjunto distinto del vacío, A, y dos leyes de composición internas, "+" y "·". Eso sí, hay que advertir, que aunque las leyes se denotan así, no son una suma y una multiplicación, sino que simplemente es habitual usar dichos símbolos para representar la primera y la segunda ley del anillo por convenio.

La terna se denomina anillo cuando cumple los siguientes axiomas:

Axioma 1

(A,+) es grupo abeliano, es decir, que A, con su primera ley interna cumple **asociatividad, neutro, simétrico y conmutatividad**.

Axioma 2

(A,·) es semigrupo, es decir, que A, con su segunda ley interna cumple la **asociatividad**.

Axioma 3

Distributiva de · respecto a +:

$$\forall a,b,c,\in A \begin{cases} a\cdot(b+c)=(a\cdot b)+(a\cdot c) \\ (b+c)\cdot a=(b\cdot a)+(c\cdot a) \end{cases}$$

Hay que fijarse en que el segundo axioma afirma que con la segunda ley, A solo tiene que cumplir la asociatividad, no la conmutatividad. Esa es la razón por la que hay que calcular la distributiva por la derecha y también por la izquierda.

- Al neutro de la primera ley (+), se le denomina el cero del anillo, y suele denotarse 0A.
- El neutro de la segunda ley no tiene por qué existir.

Veamos un ejemplo

El conjunto de los números enteros, Z, se definen las leyes de composición $\oplus$ y $\otimes$ que funcionan del siguiente modo:

$$a \oplus b = a + b + 1$$
$$a \otimes b = a + b + a \cdot b$$

Comprobemos si $(Z; \oplus\otimes)$ es un anillo

Fíjate que las leyes no son ni una suma ni una multiplicación, sino dos leyes particulares. Aún así, habrán de cumplir tanto el ser internas como la axiomática completa si queremos afirmar que Z es un anillo.

Primero veamos si las **leyes** son efectivamente **internas**:

- $\forall a, b \in Z \quad a \oplus b = \underbrace{a}_{\in Z} + \underbrace{b}_{\in Z} + \underbrace{1}_{\in Z} \in Z \quad \rightarrow \quad \oplus \, es \, interna$

Observa que la suma de tres números enteros es un entero.

- $\forall a, b \in Z \quad a \otimes b = \underbrace{a}_{\in Z} + \underbrace{b}_{\in Z} + \underbrace{a}_{\in Z} \cdot \underbrace{b}_{\in Z} \in Z \quad \rightarrow \quad \otimes \, es \, interna$

Observa que la suma de tres números enteros es un entero y el producto de dos enteros también es un entero.

Axioma 1. Grupo abeliano

Ahora veamos el primer axioma $(Z, \oplus)$ que debe ser grupo abeliano.

- $\forall a,b,c \in Z \quad a \oplus (b \oplus c) = a \oplus (b+c+1) = a+b+c+1+1 = (a \oplus b)+c+1 = (a \oplus b) \oplus c$

Luego se cumple la **asociatividad** con la primera ley:

- $\exists! -1 \in Z \quad / \quad \forall a \in Z \quad a \oplus -1 = a+(-1)+1 = a \quad \rightarrow \quad -1 \; es \; el \; neutro \; de \oplus$

Fíjate en que el "cero del anillo" es el número entero "-1", es decir, que el cero del anillo se llama así porque es el neutro de la primera ley, y no porque tenga nada que ver con el número 0.

Luego existe un único elemento, el -1, que actúa como neutro de Z con su primera ley.

- $\forall a \in Z \quad \exists a' = -a-2 \quad a \oplus (-a-2) = a+(-a-2)+1 = -1 \quad \rightarrow \quad a' = -a-2$

Es decir, que la estructura de los simétricos a' de cada elemento $a \in Z$ es $a' = -a-2$. De esa forma, el simétrico del elemento 3 por ejemplo, sería el $3' = -3-2 = -5$ pues se comprueba que efectivamente: $3 \oplus (-5) = 3+(-5)+1 = -1$, que es el **neutro** con la ley $\oplus$.

Luego todo elemento tiene un **simétrico** con la primera ley.

- $\forall a,b \in Z \quad a \oplus b = a+b+1 = b+a+1 = b \oplus a$

Luego la primera ley es **conmutativa**.

> Como se cumple que $(Z, \oplus)$ tiene asociatividad, elemento neutro, simetría para todos sus elementos y conmutatividad, podemos afirmar que se trata, efectivamente de un grupo abeliano.

Axiomas 2 y 3

Ahora veamos el segundo axioma, $(Z, \otimes)$ debe ser semigrupo.

$\forall a,b,c \in Z \quad a \otimes (b \otimes c) = a \otimes (b+c+bc) = a+b+c+bc+ab+ac+abc =$
$= (a+b+ab) \otimes c = (a \otimes b) \otimes c$

Luego se cumple la **asociatividad** con la segunda ley.

Por último, debemos comprobar si se cumplen las dos distributivas, descritas en el tercer axioma:

$\forall a,b,c \in Z \quad a \otimes (b \oplus c) = a \otimes (b+c+1) = a+b+c+1+ab+ac+a = (a+b+ab)+$
$+(a+c+ac)+1 = (a \otimes b)+(a \otimes c)+1 = (a \otimes b) \oplus (a \otimes c)$

Luego se cumple la a **distributiva** de $\otimes$ respecto a $\oplus$ **por la izquierda**.

$\forall a,b,c \in Z \quad (b \oplus c) \otimes a = (b+c+1) \otimes a = b+c+1+a+ba+ca+a = (b+a+ba)+$
$+(c+a+ca)+1 = (b \otimes a)+(c \otimes a)+1 = (b \otimes a) \oplus (c \otimes a)$

Luego se cumple la a **distributiva** de $\otimes$ respecto a $\oplus$ **por la derecha**.

Por lo tanto **se cumplen los tres axiomas**, y, efectivamente, se puede afirmar que $(Z; \oplus\otimes)$ es un anillo.

Los "apellidos" de un anillo

Ya hemos visto que un anillo es una estructura algebraica compleja. Cumple muchas cosas con su primera ley, y muy pocas con la segunda. A medida que el anillo va cumpliendo más cosas con la segunda ley, se le van otorgando sufijos, "*apellidos*".

Un anillo se llama unitario cuando posee neutro con la segunda de sus leyes. A dicho elemento neutro se le denomina "uno del anillo", y se le suele denotar 1_A.

Luego (A; +,·) es anillo unitario si y solo si, $\exists! \, 1_A \in A \quad / \quad 1_A \cdot a = a \cdot 1_A = a \quad \forall a \in A$.

Un anillo se llama abeliano cuando es conmutativa su segunda ley. Recordando, claro está, que la primera ley lo es siempre.

Luego (A; +,·) es anillo abeliano si y solo si, $\forall a, b \in A \quad a \cdot b = b \cdot a$.

Veamos que en el ejemplo que llevamos desarrollando hasta ahora, Z, con las leyes de composición $\oplus$ y $\otimes$, tenemos un anillo abeliano y unitario:

$$\forall a, b \in Z \quad a \otimes b = a + b + a \cdot b = b + a + ba = b \otimes a$$

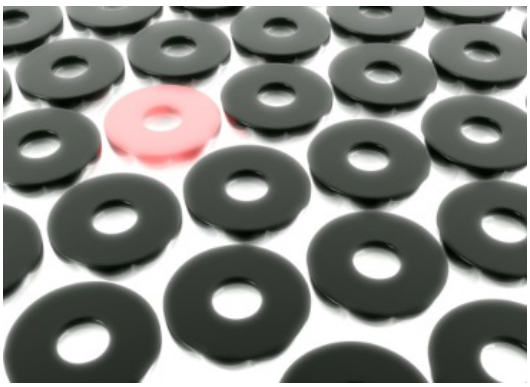
Luego se cumple la conmutatividad con la segunda ley y podemos afirmar que el anillo es abeliano.

$$\exists! 0 \in Z \quad / \quad 0 \otimes a = 0 + a + 0 \cdot a = a \quad \forall a \in Z$$

Luego existe un elemento neutro con la segunda ley por lo que podemos afirmar que el anillo es unitario.

Toma nota de lo curioso de este caso en particular, ya que es muy ilustrativo. El elemento neutro de la segunda ley de este anillo, elemento que habitualmente se denomina *"uno del anillo"*, es el número entero 0.

Anillos íntegros



Cuando un anillo se denomina íntegro o dominio de integridad, es porque cumple que para cualesquiera dos elementos del anillo distintos del neutro de la primera ley (cero del anillo), la operación de esos dos elementos con la segunda ley no da como resultado, jamás, el neutro de la primera ley.

Es decir, que no existen divisores de cero en dicho anillo.

- Si lo planteamos analíticamente, se denotaría así:

$$\forall \underbrace{a}_{a\neq 0_A}, \underbrace{b}_{b\neq 0_A} \in A \quad a \cdot b \neq 0_A$$

- Si tomamos un anillo conocido, como los números reales con la suma y multiplicación habitual, (R; +,·), es fácil de comprobar.

- Si tomamos dos números reales cualesquiera no nulos, el resultado de multiplicarlos (operarlos con la segunda ley), nunca puede ser el cero del anillo (el número real 0).

Tomemos dos reales cualesquiera, el 2 y el 5 por ejemplo:

$$\forall \underbrace{2}_{2\neq 0}, \underbrace{5}_{5\neq 0} \in \Re \quad 2 \cdot 5 = 10 \neq 0$$

Subanillo

Una parte no vacía S de un anillo es subanillo si y solo si cumple una de las siguientes condiciones:

- Cumple la axiomática completa de anillo.
- Cumple que:
  - $\forall a,b \in S \quad a+(-b) \in S \rightarrow$ Es decir, que forma un subgrupo con la primera ley.
  - $\forall a,b \in S \quad a \cdot b \in S \rightarrow$ Es decir que la segunda ley es interna dentro del subanillo.

Un subanillo hereda una serie de características del anillo del que proviene, de tal forma, podremos afirmar que:

- El neutro con la primera ley, 0_A, de un anillo coincide con el de todos sus subanillos.
- Si el anillo es unitario, el neutro con la segunda ley, 1_A, de un anillo coincide con el de todos sus subanillos.
- Si el anillo es abeliano, todos sus subanillos serán a su vez abelianos.
- Si el anillo es dominio de integridad, todos sus subanillos serán a su vez dominios de integridad.

Subanillo ideal. Característica

Un conjunto I perteneciente a un anillo (A; +,·) se denomina subanillo ideal suyo, cuando cumple lo siguiente:

1. I es subanillo.
2. $\forall a \in A; \forall i \in I \rightarrow = \begin{cases} a \cdot i \in I \\ i \cdot a \in I \end{cases}$

Mirando la segunda propiedad enunciada, se observa que un ideal hace que cualquier elemento del anillo operado por un elemento del ideal, se convierta en un elemento del ideal. Es decir, que el ideal es "sumidero" de elementos con la segunda ley.

Un ejemplo trivial, pero muy ilustrativo de ideales es el que forma el número 0 en el anillo de los reales con la suma y la multiplicación habituales, (R; +,·).

Si aceptamos que $I = \{0\}$ es un subanillo de R, formado exclusivamente por el 0, podemos observar que:

$$\forall a \in R\,;\, 0 \in I \quad \rightarrow \quad a \cdot 0 = 0 \in I$$

Conviene saber también que la intersección y suma de ideales, son ambos ideales.

Característica de un anillo

La característica de un anillo cuando existe es un número único p que cumple:

$$Caract(A) = p \quad \Leftrightarrow \quad \overbrace{a + a + a + \ldots + a}^{p\ veces} = 0_A$$

Homomorfismos entre anillos

Se denomina homomorfismo a una aplicación, f, entre dos anillos $(A_1;+,\cdot)$, que llamaremos inicial o de salida, y $(A_2;*,\Delta)$, que llamaremos final o de llegada, que cumple lo siguiente:

$$f: A_1 \to A_2$$
$$\forall a,b \in A_1 \quad f(a+b) = f(a) * f(b)$$
$$\forall a,b \in A_1 \quad f(a \cdot b) = f(a) \Delta f(b)$$

Es decir, que el transformado de la operación de dos elementos es la operación de los transformados de dichos elementos con ambas leyes internas.

Además de lo descrito, un homomorfismo también habrá de transformar, siempre, el cero del primer anillo (neutro con la 1ª ley), en el cero del segundo, de la forma:

$$f(0_1) = 0_2 \quad con\ 0_1 \in A_1 \ y\ 0_2 \in A_2$$

Los homomorfismos se clasifican del mismo modo que en el caso de los grupos, según la aplicación sea inyectiva, sobreyectiva o biyectiva, y según coincidan o no los anillos inicial y final: definamos ahora dos partes fundamentales de un homomorfismo, su núcleo y su imagen.

El núcleo de un homorfismo es el subanillo del anillo inicial que forman todos aquellos elementos que se transforman en el neutro con la primera ley, 0_2, del anillo final:

$$N(f) = \{x \in A_1 / f(x) = 0_2\}$$

Si f es inyectivo, el núcleo está formado únicamente por el elemento neutro con la 1ª ley del anillo inicial. La imagen de un homomorfismo es el subanillo del anillo final que forman todos aquellos elementos que son transformados de otro:

$$\mathrm{Im}(f) = \{y \in A_2 \ / \exists x \in A_1 \quad f(x) = y\}$$

Si f es sobreyectivo, la imagen está formada por todos los elementos del anillo final, A_2.

Grupo multiplicativo de un anillo

Antes de meternos con la descripción de un cuerpo, como estructura algebráica, conviene que demos una breve definición de una subestructura de los anillos que nos ayudará a definir correctamente al cuerpo: el grupo multiplicativo.

Se llama grupo multiplicativo de un anillo (A; +,·) a un conjunto U distinto del vacio que esta formado por todos aquellos elementos que tienen inverso con la segunda ley.

El conjunto U forma un grupo con la segunda ley del anillo, (U,·) y se cumple que:

$$\forall a \in A \quad 0_A \cdot a = 0_A \neq 1_A \quad \rightarrow \quad 0_A \notin U$$

Es decir, que el cero de un anillo nunca pertenece a su grupo multiplicativo.

Pero, ¿qué es un cuerpo?

Un cuerpo es un anillo. Hasta ahora a los anillos les habíamos dado apellidos según el número de cosas que cumpliesen con su segunda ley. Si resulta que su segunda ley se vuelve tan robusta en cuanto a propiedades como la primera, el anillo pasará a ser un cuerpo. Veámoslo de forma analítica:

Se dirá que un conjunto K dotado de dos leyes de composición internas, de la forma (K; +, ·) es cuerpo, si y sólo si se cumple:

Axioma 1

(K; +, ·) es un Anillo abeliano:

- (K,+) es grupo abeliano.
- (K,·) es semigrupo.
- Distributiva de · respecto a +: $\forall a,b,c \in K \quad = \begin{cases} a\cdot(b+c) = (a\cdot b)+(a\cdot c) \\ (b+c)\cdot a = (b\cdot a)+(c\cdot a) \end{cases}$
- (K; +,·) es abeliano: $\forall a,b \in K \quad a\cdot b = b\cdot a$

Axioma 2

Todos los elementos de K tienen inverso (simétrico con su segunda ley), salvo el neutro de la primera ley (el cero del cuerpo):

$$\forall \underbrace{a}_{\neq 0} \in K \quad \exists a^{-1} \in K$$

Este segundo axioma puede traducirse en que el grupo multiplicativo de K es todo K menos el "*Cero de K*":

$$U_K = K - \{0_K\}$$

Axioma 3

K es íntegro. Carece de divisores de cero: $\forall \underbrace{a}_{a\neq 0_K}, \underbrace{b}_{b\neq 0_K} \in K \quad a\cdot b \neq 0_K$

Integridad de un cuerpo

Ya sabemos qué es un cuerpo y cómo funciona, vamos a ver a continuación una serie de demostraciones referentes a su axiomática.

En primer lugar, sería interesante poder demostrar que un cuerpo no tiene divisores de cero.

Partiendo de que un cuerpo es un anillo unitario en el que todo elemento distinto del cero tiene inverso, se tiene que:

$$\text{Si } a \cdot b = 0 \rightarrow = \begin{cases} a = 0 \\ \quad \vee \\ a \neq 0 \rightarrow a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 \rightarrow (a^{-1} \cdot a) \cdot b = 0 \rightarrow 1 \cdot b = 0 \rightarrow b = 0 \end{cases}$$

Luego si el producto de dos elementos del cuerpo es cero, uno de ellos tiene que serlo y por tanto, todo el cuerpo es un anillo de integridad.

Resumen

Definición de anillo:

Axioma 1: (A,+) es grupo abeliano. Axioma 2: (A,·) es semigrupo.

Axioma 3: distributiva de · respecto a +: $\forall a,b,c \in A \quad \begin{cases} a\cdot(b+c)=(a\cdot b)+(a\cdot c) \\ (b+c)\cdot a=(b\cdot a)+(c\cdot a) \end{cases}$

Subanillo:

$\forall a,b \in S \quad a+(-b) \in S$. Es decir, que forma un subgrupo con la primera ley.

$\forall a,b \in S \quad a\cdot b \in S$. Es decir que la segunda ley es interna dentro del subanillo.

Subanillo ideal: un conjunto I perteneciente a un anillo (A; +,·) se denomina subanillo ideal suyo cuando cumple lo siguiente. I es subanillo: $\forall a \in A \; ; \forall i \in I \quad \rightarrow \quad \begin{cases} a\cdot i \in I \\ i\cdot a \in I \end{cases}$

- **Axioma 1.** (K; +, ·) es un Anillo abeliano:
  - (K,+) es grupo abeliano. (K,·) es semigrupo.
- **Axioma 2.** El grupo multiplicativo de K es todo K menos el "*Cero de K*": $U_K = K - \{0_K\}$.
- **Axioma 3.** K es íntegro. Carece de divisores de cero: $\forall \underbrace{a}_{a\neq 0_K}, \underbrace{b}_{b\neq 0_K} \in K \quad a\cdot b \neq 0_K$