Propiedades de un anillo

Principales propiedades

Marcos Daniel Calderón Calderón

Centro de Investigación en Matemáticas
marcos.calderon@cimat.mx

Resumen En este documento se hace un pequeño análisis de la estructura conocida como "anillo". Se incluyen las definiciones principales, los teoremas más importantes.

1. Fundamentos

DEFINICIÓN 1 (ANILLO) Sea $\mathbf{R}$ un conjunto no vacio en el cual tenemos dos operaciones cerradas binarias, denotadas por $+$ y $\cdot$ (dichas operaciones pueden ser diferentes a la multiplicación y suma ordinarias). Entonces ($\mathbf{R}$, $+$, $\cdot$) es un *anillo* si para todo a, b, $c \in \mathbf{R}$, las siguientes condiciones se cumplen:

a)	$a + b = b + a$.	Ley Conmutativa de $+$
b)	$a + (b + c) = (a + b) + c$.	Ley asociativa de $+$
c)	Existe $z \in \mathbf{R}$ tal que $a + z = z + a = a$ para cada $a \in \mathbf{R}$.	Existencia de una identitad para $+$
d)	Para cada $a \in \mathbf{R}$ hay un elemento $b \in \mathbf{R}$ donde $a + b = b + a = z$.	Existencia de inversos bajo $+$
e)	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$	Ley asociativa de $\cdot$
f)	$a \cdot (b + c) = a \cdot b + a \cdot c$ $(b + c) \cdot a = b \cdot a + c \cdot a$	Leyes distributivas de $\cdot$ sobre $+$

Como las operaciones binarias cerradas de $+$ (suma del anillo) y $\cdot$ (multiplicación del anillo) son ambas asociativas, no hay confusión si escribimos $a+b+c$ por la expresión $(a + b) + c$ o $a + (b + c)$, o $a \cdot b \cdot c$ por $(a \cdot b) \cdot c$ o $a \cdot (b \cdot c)$. COn frecuencia se escribe ab para representar $a \cdot b$. Las leyes asociativas pueden ser extendidas a mas de dos términos.

EJEMPLO 1 Bajo las operaciones binarias cerradas de la suma y multiplicación ordinaria, podemos concluir que $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ son anillos. En todos estos casos, la identidad aditiva z es el entero 0, y el inverso aditivo de cada número x es $-x$.

DEFINICIÓN 2 Sea ($\mathbf{R}$, $+$, $\cdot$) un anillo.

a) Si $ab = ba$ para todo $a, b \in \mathbf{R}$, entonces $\mathbf{R}$ es llamado un anillo *conmutativo.*

b) Se dice que el anillo $\mathbf{R}$ *no tiene divisores propios de cero* si para todo $a, b \in R, \quad ab = z \Rightarrow a = z \quad o \quad b = z.$

c) Si un elemento $u \in \mathbf{R}$ es tal que $u \neq z$ Y $au = ua = a$ para todo $a \in \mathbf{R}$, podemos llamar a u una identidad multiplicativa de $\mathbf{R}$. Por lo tanto $\mathbf{R}$ es llamado un anillo con un elemento identidad para la multiplicación.

Se puede concluir de la parte **(c)** de la definición anterior, que siempre que nosotros tengamos un anillo $\mathbf{R}$ con un elemento identidad para la multiplicación. entonces, $\mathbf{R}$ contiene al menos dos elementos.

EJEMPLO 2 Loa anillos $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ son anillos conmutativos cuya identidad para la multiplicación es el entero 1. Ninguno de estos anillos tiene divisores propios de cero.

DEFINICIÓN 3 Sea $\mathbf{R}$ un anillo con identidad multiplicativa u. si $a \in \mathbf{R}$ y existe un $b \in \mathbf{R}$ tal que $ab = ba = u$, entonce b es llamado un *inverso multiplicativo* de a.

DEFINICIÓN 4 Sea $\mathbf{R}$ un anillo con identidad multiplicativa u. Entonces, podemos decir lo siguiente:

a) $\mathbf{R}$ es llamado un *dominio de integridad* si $\mathbf{R}$ no tiene divisores propios de cero.

b) $\mathbf{R}$ es llamado un *campo* si cada elemento no cero de $\mathbf{R}$ tiene un inverso multiplicativo.

El anillo ($\mathbf{Z}$,+ . $\cdot$) es un dominio de integridad pero no es un cambo, mientras que $\mathbf{Q}$, $\mathbf{R}$ y $\mathbf{C}$, bajo las operaciones ordinarias de suma y multiplicación son dominios de integridad y campos.

TEOREMA 1 En cualquier anillo ($\mathbf{R}$, +. $\cdot$),

a) el elemento *cero* es único, y

b) el inverso aditivo de cada elemento del anillo es único.

Demostración.

a) Supongamos que R tiene más de una identidad aditiva y z_1, z_2 denotan a estos elementos. Entonces

$$z_1 = z_1 + z_2 = z_2$$

b) Para un $a \in \mathbf{R}$, supongamos que hay dos elementos $b, c \in \mathbf{R}$ conde $a + b = b+a = z$ y $a+c = c+a = z$. Entonces, $b = b+z = b+(a+c) = (b+a)+c = z+c = c$

Como un resuldado de la unicidad de la parte **(b)**, podemos denotar el inverso aditivo de $a \in \mathbf{R}$ como $-a$

Teorema 2 (Las leyes de cancelación para la adición o suma) Para todo $a, b, c \in \mathbf{R}$,

a) $a + b = a + c \Rightarrow b = c$, y
b) $b + a = c + a \Rightarrow b = c$

Demostración.
a) Como $a \in \mathbf{R}$, podemos confirmar que $-a \in \mathbf{R}$ y podemos hacer lo siguiente:

$$\begin{aligned} a + b = a + c &\Rightarrow (-a) + a + b = (-a) + a + c \\ &\Rightarrow [(-a) + a] + b = [(-a) + a] + c \\ &\Rightarrow z + b = z + c \\ &\Rightarrow b = c \end{aligned}$$

b) La demostración es similar a la anterior.

Teorema 3 En cualquier anillo $(\mathbf{R}, +. \cdot)$, y paras cualquier $a \in \mathbf{R}$, se cumple que $az = za = z$.

Demostración. Si $a \in R$, entonces $az = a(z + z)$ ya que $z + z = z$. Por lo tanto $z + az = az = az + az$. Al usar la ley de cancelación para la adición, tenemos que $z = az$. La prueba de que $za = z$ se realiza de manera similar.

Teorema 4 En un anillo $(\mathbf{R}, +. \cdot)$, para cualquier $a, b \in \mathbf{R}$,
a) -(-a)=a,
b) a(-b)= (-a)b= -(ab) y
c) (-a)(-b)= ab.

Demostración.
a) Por la convención mencionada $-(-a)$ denota el inverso aditivo de $-a$. Como $(-a) + a = z$, a también es un inverso aditivo para $-a$. EN consecuencia, por la unicidad de los inversos $-(-a) = a$.
b) Debemos probar que $a(-b) = -(ab)$. Sabemos aque $-(ab)$ denota el inverso aditivo de ab. Por lo tanto, $ab + a(-b) = a[b + (-b)] = az = z$ por el teorema 3 y por la unicidad de inversos aditivos, conclumos que: $a(-b)$

c) De la parte (b), podemos concluir que $(-a)(-b) = -[a(-b)] = -[-(ab)]$, y por lo tanto el resultado se obtiene de la parte (a).

Teorema 5 Para un anillo dado $(\mathbf{R}, +. \cdot)$,
a) Si $\mathbf{R}$ tiene un una identidad para multiplicación, entonces esta es única, y
b) Si $\mathbf{R}$ tiene un una identidad para multiplicación, y $x \in \mathbf{R}$, etonces el inverso multiplicativo de x es unico.

Teorema 6 Sea $(\mathbf{R}, +. \cdot)$, un anillo conmutativo con elemento unidad. Entonces $\mathbf{R}$ es un dominio de integridad si, para todo $a, b, c \in \mathbf{R}$, donde $a \neq z$, $ab = ac \Rightarrow b = c$. Por lo tanto, un anillo conmutativo con elemento unidad satisface la ley de la cancelación para la multiplicación es un dominio de integridad.

Un dominio de integridad no necesariamente es un campo.

Referencias

[RE1] Author: Article/Book: Other info: (date) page numbers.