Capítulo

7

Anillos

7.1 Definiciones Básicas

El concepto de Anillo se obtiene como una generalización de los números enteros, en donde están definidas un par de operaciones, la suma y el producto, relacionadas entre si por una ley de distributividad.

Los anillos pues son estructuras algebraicas más completas que los grupos, pero sin embargo en el estudio de sus propiedades más importantes, nos apoyamos a lo largo de toda la exposición en nuestra experiencia con los grupos. La razon para esto es muy simple, pues todo anillo es un grupo en si mismo.!

Definición 7.1.1 *Un* **anillo** R *es un conjunto no vacío en donde están definidas un par de operaciones llamadas suma y producto, las cuales denotamos por* $+$ *y* $\cdot$ *respectivamente.*

Estas operaciones satisfacen cada una de las propiedades siguientes:

1) Para todo a, $b \in R$, *se tiene que* $a+b$ *y* $a \cdot b$ *están en* R.

2) Para todo a, $b, \in R$ *se tiene que*

$$a + (b + c) = (a + b) + c$$

3) Existe un elemento 0 *en* R, *el cual llamaremos* **cero**, *tal que*

$$a + 0 = 0 + a = a \quad \text{para todo } a \text{ en } R.$$

4) Para todo a *en* R, *existe otro elemento en* R, *denotado por* $-a$, *el cual llamamos el* **opuesto** *de* a *y que verifica*

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

5) Para todo a, b *en* R *se tiene*

$$a + b = b + a$$

6) Para todo a, b y c en R se satisface

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

7) Para todo a, b y c en R se satisface

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (a + b) \cdot c &= a \cdot c + b \cdot c \end{aligned}$$

Observación: De acuerdo a las propiedades 1-5 de la definición, se tiene que todo anillo es un grupo abeliano bajo la suma.

Definición 7.1.2 *Sea R un anillo y supongamos que existe un elemento* $1 \in R$ *tal que*

$$a \cdot 1 = 1 \cdot a = a \quad \textit{para todo } a \textit{ en } R.$$

Entonces el anillo R se dice **anillo unitario** *o* **anillo con unidad**.

Definición 7.1.3 *Sea R un anillo. Si para todos a y b en R se tiene*

$$ab = ba$$

entonces diremos que R es un **anillo conmutativo**.

Definición 7.1.4 *Sea R un anillo, un elemento* $a \in R$ *se dice* **invertible**, *si existe otro elemento* $a^{-1} \in R$ *tal que*

$$a \cdot a^{-1} = a^{-1} \cdot a = 1.$$

Definición 7.1.5 *Un* **anillo de división** *es un anillo con unidad, en donde todos los elementos distintos de cero son invertibles.*

Definición 7.1.6 *Un* **cuerpo** *es un anillo conmutativo con unidad, en donde todos los elementos distintos de cero son invertibles.*

Observación: Existen anillos de división no conmutativos y por ende no cuerpos. Ver problema 13.

Veamos a continuación una serie de ejemplos de anillos

Ejemplo 1: El conjunto $\mathbb{Z}$ de los números enteros, con las operaciones de suma y producto es un anillo conmutativo con unidad.

Ejemplo 2: El conjunto $\mathbb{Z}_m$ de enteros módulo m, con la suma y producto módulo m es un ejemplo de anillo conmutativo con unidad, el cual es finito. La suma y el producto módulo m se definen de la forma siguiente:

Para $[a]$, $[b]$ en $\mathbb{Z}_m$ se tiene

$$[a] + [b] = [a + b]$$

$$[a][b] = [ab]$$

Ejemplo 3: Si p es un número primo, entonces los enteros módulo p, denotado por $\mathbb{Z}_p$, es un cuerpo. Para verificar esto, basta observar que si $[a] \neq [0]$ en $\mathbb{Z}_p$, entonces $p \not| a$ y por lo tanto p y a son primos relativos.

Luego existen enteros x e y tales que

$$a \cdot x + p \cdot y = 1$$

Luego

$$a \cdot x \equiv 1 \ mod \ p.$$

Por lo tanto en $\mathbb{Z}_p$ se tiene que

$$[a] \cdot [x] = [1]$$

de esto se sigue que el elemento $[a]$ es invertible.

Ejemplo 4: Sea $I = [0, 1]$ el intervalo cerrado de números reales y sea R el conjunto de funciones de I en los números reales.

Si f y g son dos funciones, la suma y el producto de ellas se define por:

$$(f + g)(x) = f(x) + g(x)$$

$$(f \cdot g)(x) = f(x) \cdot g(x)$$

Entonces es fácil verificar que R es un anillo con este par de operaciones. Además R posee unidad y R es un anillo conmutativo.

Ejemplo 5: Sea R el conjunto de matrices cuadradas de orden 2×2 con coeficientes reales. Los elementos de R son de la forma:

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

donde $a_{ij} \in R$, $1 \leq i \leq 2,\ \ 1 \leq j \leq 2$.

Si A y B son dos elementos de R, entonces la suma y el producto están dadas por:

$$\begin{aligned} A + B &= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \\ &= \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix} \end{aligned}$$

$$\begin{aligned} A \cdot B &= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \\ &= \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \end{aligned}$$

donde

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} \text{ para todo } 1 \leq i \leq 2, \quad 1 \leq j \leq 2.$$

Se puede demostrar que R con estas dos operaciones así definidas es un anillo con unidad. Sin embargo R no es conmutativo. Para demostrar esto consideremos el siguiente ejemplo:

Sean

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

Entonces

$$AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

Mientras que

$$BA = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$$

Luego

$$AB \neq BA.$$

Definición 7.1.7 *Sea R un anillo y A un subconjunto de R, el cual es un anillo con las operaciones del anillo R, entonces A se llama un* **subanillo** *de R.*

Ejemplo: El conjunto de los enteros pares $2\mathbb{Z}$, es un subanillo del anillo $\mathbb{Z}$ de los números enteros.

Ejercicios

1) Demuestre que en cualquier anillo R, el conjunto de los elementos invertibles forma un grupo bajo el producto.

2) Pruebe que en un anillo conmutativo con identidad, el elemento unidad es único.

3) Probar que si R es un anillo conmutativo con identidad y a es invertible, entonces $a = (a^{-1})^{-1}$.

4) Sea R el conjunto de parejas ordenadas de números reales. Establecer cuales de las operaciones siguientes determinan una estructura de

a) Anillo.
b) Anillo conmutativo.
c) Anillo conmutativo con unidad.

i) $(a, b) + (c, d) = (a + c, b + d)$
$(a, b) \cdot (c, d) = (ac, bd)$

ii) $(a, b) + (c, d) = (a + c, b + d)$
$(a, b) \cdot (c, d) = (ac + bd, ad + bd)$

iii) $(a, b) + (c, d) = (a, c)$
$(a, b) \cdot (c, d) = (ac, bd)$

iv) $(a, b) + (c, d) = (a + c + 1, b + d)$
$(a, b) \cdot (c, d) = (ad + bc, ac + bd)$

5) Sea R un anillo y $a, b \in R$. Probar la fórmula

$$(a + b)^2 = a^2 + ab + ba + b^2$$

6) Sea R un anillo conmutativo con identidad y n un entero positivo y $a, b \in R$. Probar la fórmula

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

donde

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

7) **Números Complejos:** Sea R el conjuntos de símbolos de la forma $a + bi$, con a y b números reales, e i la raíz cuadrada de -1, esto es $i^2 = -1$. Convenimos en que dos símbolos $a + bi$ y $c + di$ son iguales si y sólo si $a = c$ y $b = d$. Definimos un par de operaciones en R, mediante

$$\begin{aligned}(a + bi) + (c + di) &= (a + c) + (b + d)i \\ (a + bi) \cdot (c + di) &= (ac - bd) + (ad + bc)i\end{aligned}$$

Probar que este conjunto R con las operaciones así definidas es un anillo conmutativo con unidad. Este anillo se llama **Anillo de los Complejos**, y lo denotamos por $\mathbb{C}$.

8) **Cuaternios Reales:** Sea R el conjunto de símbolos de la forma $a + bi + cj + dk$, con a, b, c y d números reales, y los símbolos i, j, k definidas por las relaciones:

i) $i^2 = j^2 = k^2 = -1$

ii) $ij = k,\ jk = i,\ ki = j.$

iii) $ji = -k,\ kj = -i,\ ik = -j.$

Convenimos en que dos elementos $a+bi+cj+dk$ y $a'+b'i+c'j+d'k$ son iguales si y sólo si

$$a = a', \quad b = b' \quad c = c', \quad \text{y} \quad d = d'.$$

Definimos la suma de elmentos en R componente por componente, esto es

$$(a+bi+cj+dk)+(a'+b'i+c'j+d'k) = (a+a')+(b+b')i+(c+c')k+(d+d')k$$

La multiplicación de elementos de R se define mediante las leyes de distributividad para expresiones polinómicas y las relaciones $1, 2, 3$. Por ejemplo

$$\begin{aligned}(5 + 3i)(2 + 4k) &= 2 \cdot 5 + 5 \cdot 4k + 3 \cdot 2i + 3 \cdot 4ik \\ &= 10 + 6i - 12j + 20k.\end{aligned}$$

Demostrar que en R, estas operaciones es un anillo de división. Este anillo se denomina anillo de cuaternios reales y se denotan por $\mathcal{Q}$.

9) Sea $(G, *)$ un grupo abeliano y consideremos el conjunto de homomorfismos de G sobre si mismo, denotado por $Hom(G)$. Definimos dos operaciones en este conjunto

$$\begin{aligned}(f+g)(a) &= f(a) * g(a),\\ (f \circ g)(a) &= g(f(a)),\end{aligned}$$

para todo $f, g \in Hom(G)$, y $a \in G$.

Demuestre que $(Hom(G), +, \circ))$ es un anillo.

7.2 Propiedades Elementales de los Anillos

Iniciamos con esta sección el estudio de las propiedades básicas de los anillos. En el transcurso de la misma se daran una serie de definiciones importantes, como lo son: divisor de cero, dominio de integridad y la característica de un anillo. Las mismas serán de utilidad para el resto de este capítulo.

Proposición 7.2.1 *Sea R un anillo, entonces para todos a, $b \in R$, se tiene*

i) $a \cdot 0 = 0 \cdot a = 0$

ii) $a(-b) = (-a)b = -(ab)$

Demostración:
i) Usando la propiedad distributiva (7 de la definición) para R, obtenemos

$$a \cdot 0 = a(0+0) = a \cdot 0 + a \cdot 0$$

Podemos usar a continuación la propiedad de cancelación en el grupo aditivo de R, para concluir

$$a \cdot 0 = 0$$

Similarmente se demuestra que

$$0 \cdot a = 0$$

ii) De acuerdo a *i*) se tiene

$$\begin{aligned} 0 &= a \cdot 0 \\ &= a(b-b) \\ &= ab + a(-b) \end{aligned}$$

Por lo tanto el inverso de ab bajo la adición en R (el cual es único) es igual a $a(-b)$ y luego se tiene

$$-(ab) = a(-b)$$

De la misma forma se demuestra que

$$-(ab) = (-a)b$$

y con esto termina la demostración.

♠

Corolario 7.2.1 *Sea R anillo con identidad. Entonces*

i) $(-1)a = -a$ *para todo* $a \in R$

ii) $(-1)(-1) = 1$.

Demostración:

i) Sea $a \in R$, luego podemos usar la proposición anterior para obtener

$$(-1)a = -(1a) = -a$$

ii) Aplicamos la proposición dos veces

$$\begin{aligned}(-1)(-1) &= -(1(-1)) \\ &= -(-(1 \cdot 1) \\ &= 1\end{aligned}$$

Nótese que se hizo uso de la fórmula

$$-(-a) = a, \quad a \in R$$

la cual es cierta en R, por ser un grupo bajo la adición.

♠

Observación: Un anillo R siempre contiene al elemento 0. Si este es el único elemento de R entonces R se llama el **anillo nulo** o el anillo cero.

Si R no es el anillo nulo, y además R contiene una unidad 1, entonces $1 \neq 0$.

En efecto, sea $a \in R$, $a \neq 0$ y supóngase que 1=0, luego

$$\begin{aligned}a &= a1 \\ &= a0 \\ &= 0\end{aligned}$$

lo cual es una contradicción.

Definición 7.2.1 *Sea R un anillo. Un elemento $a \in R$ distinto de cero, se dice* **divisor de cero** *si existe un b en R, distinto de cero, tal que*

$$ab = 0$$

Ejemplo 1: Sea $R = \mathbb{Z}_6$ el anillo de los enteros módulo 6. Luego

$$[2] \neq [0] \quad \text{y} \quad [3] \neq [0],$$

pero

$$\begin{aligned} [2][3] &= [2 \cdot 3] \\ &= [6] \\ &= [0] \end{aligned}$$

por lo tanto [2] y [3] son divisores de cero en este anillo.

Ejemplo 2: Sea $R = \mathbb{Z}$ el anillo de los enteros. Entonces se sabe de las propiedades que definen a los enteros, que $\mathbb{Z}$ no tiene divisores de cero. Para probar esta afirmación, basta usar la ley de cancelación para el producto en $\mathbb{Z}$.

Si $a \neq 0$ y $b \neq 0$ son enteros y además $ab = 0$, se tendrá entonces

$$a0 = 0 = ab$$

de donde

$$b = 0,$$

lo cual es una contradicción.

Definición 7.2.2 *Un anillo conmutativo con identidad que no posee divisores de cero se llama un* **Dominio de Integridad**.

Ejemplo: El anillo $\mathbb{Z}$ de los enteros es un dominio de integridad.

Proposición 7.2.2 *Un anillo conmutativo R, sin divisores de cero, finito es un cuerpo.*

Demostración: Al ser R un dominio de integridad, R es un anillo conmutativo con unidad. Sólo falta probar que todos los elementos de R diferentes de 0 son inversibles.

Consideremos $a \neq 0$ en R, y supongamos

$$R = \{a_1, \ldots, a_n\}$$

Entonces los elementos $aa_1, aa_2, \ldots, aa_n$ son n elementos distintos en R.

En efecto, si suponemos que

$$aa_i = aa_j$$

para algunos $i \neq j$, $1 \leq i \leq n$, $1 \leq j \leq n$, entonces se tendrá:

$$aa_i - aa_j = 0$$

$$a(a_i - a_j) = 0$$

Como R no admite divisores de cero, se debe tener

$$a_i - a_j = 0$$

lo cual implica que $a_i = a_j$, lo cual es una contradicción.

Una vez probado este hecho, el elemento a antes considerado, debe estar entre los aa_i, digamos $a = aa_k$, para algún $1 \leq k \leq n$.

Afirmamos que $a_k = 1$. En efecto, si $a_i \in R$, se tiene que existe un j, $1 \leq j \leq n$, tal que

$$a_i = aa_j$$

Luego

$$\begin{aligned} a_i a_k &= (aa_j)a_k \\ &= (aa_k)a_j \\ &= aa_j \\ &= a_i \end{aligned}$$

Por lo tanto hemos probado que a_k es el elemento unidad de R.

Para concluir, probaremos que el elemento a, elegido al principio es invertible. Siendo a un elemento cualquiera de R distinto de cero, se deduce entonces que todos los elementos de R no nulos son invertibles, y con esto se demuestra que R es un cuerpo.

En efecto, el elemento a_k debe estar entre los elementos $aa_1, \ldots, aa_n$, luego existe j, tal que

$$aa_j = a_k$$

Luego $a_j = a^{-1}$ y a es invertible.

♠

Corolario 7.2.2 *Un Dominio de Integridad finito es un cuerpo.*

Si R es un anillo cualquiera y n es un entero positivo, entonces na es igual a la suma de a $n-$veces. Por otro lado a^n indica el producto de a consigo mismo $n-$veces.

Definición 7.2.3 *Sea R un dominio de integridad. Entonces, el menor entero positivo n (si existe) tal que $na = 0$ para todo $a \in R$ se llama la* **característica** *del anillo. Si no existe dicho entero, entonces se dice que R es de característica 0.*

Ejemplo 1: El anillo $\mathcal{Q}$ de los números racionales con la suma y el producto habituales, es un anillo de característica 0.

Ejemplo 2: El anillo $\mathbb{Z}_7$ de los enteros módulo 7 es de característica 7, pues si $[a] \in \mathbb{Z}_7$, se tiene que

$$7[a] = [7a] = [0]$$

Además no existe un entero positivo menor con dicha propiedad (Verificarlo!).

Teorema 7.2.1 *Si el dominio R es de característica $p > 0$, entonces p debe ser un número primo.*

Demostración: Es claro que $p \cdot 1 = 0$, pues $pa = 0$ para todo a en R.

Por otro lado, si p no es primo, entonces $p = mn$ con $1 < m < p$, $1 < n < p$.

Luego

$$\begin{aligned} p1 &= (mn)1 \\ &= (m1)(n1) \\ &= 0 \end{aligned}$$

Como R es un dominio de integridad, se debe tener $m1 = 0$, o bien $n1 = 0$. Si suponemos $m1 = 0$, entonces para todo $a \in R$ se tendrá

$$\begin{aligned} ma &= m(1a) \\ &= (m1)a \\ &= 0a \\ &= 0 \end{aligned}$$

Luego la característica de R debe ser menor o igual m, lo cual es un absurdo pues $m < p$.

Ejercicios

6) Demuestre que el anillo de matrices cuadradas reales de orden 2×2 no es un dominio de integridad.

8) Si R es un dominio de característica p, probar

$$(a + b)^p = a^p + b^p \quad \text{para todo } a, b \in R.$$

9) Probar que el anillo de funciones $f : [0, 1] \longrightarrow R$ con la suma y producto definidas como en el ejemplo 4, no es un dominio de integridad.

10) Un elemento a en un anillo R se dice nilpotente si $a^n = 0$, para algún n entero positivo. Probar que en un dominio de integridad no hay elementos nilpotentes.

11) Demuestre que un anillo conmutativo D es un dominio de integridad si y sólo si para todos a, b y c en R con $a \neq 0$, la relación $ab = ac$, implica $b = c$.

7.3 Homomorfismos

Los homomorfismos de anillos son aplicaciones entre ellos que preservan las operaciones. Todo homorfismo de anillos es al mismo tiempo un homomorfismo de grupo y esto establece un paralelo entre la teoría de anillos y la teoría de grupos.

Muchas de las definiciones y resultados de esta sección ya han sido estudiadas en los grupos y por lo tanto omitimos algunas demostraciones.

En esta sección se introduce el concepto de ideal, el cual juega el mismo papel que los grupos normales dentro de la teoría de grupos. Mediente el uso de ideales es posible definir los anillos cocientes de forma similar como se hizo para los grupos.

Definición 7.3.1 *Sean R y S dos anillos, un* **homomorfismo de anillos** *entre R y S es una aplicación*

$$\phi : R \longrightarrow S$$

tal que

i) $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$

ii) $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$
para todo r_1, r_2 en R.

Observación 1: En primer lugar debe tenerse en cuenta que la suma $r_1 + r_2$ en $i)$ se efectua dentro de R, mientras que la suma $\phi(r_1) + \phi(r_2)$

tiene lugar dentro del anillo S. La misma observación es válida para el producto en $ii)$

Observación 2: Obsérvese que de acuerdo a la condición $i)$ todo homomorfismo de anillos es un homomorfismo de grupos y por lo tanto valen todos los resultados sobre homomorfismos, estudiados en el capítulo de grupo.

Ejemplo 1: Sea $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$, la aplicación dada por $\phi(x) = [x]$. Entonces ϕ es un homomorfismo de anillos, pues

$$\begin{aligned} \phi(n+m) &= [n+m] \\ &= [n] + [m] \\ &= \phi(n) + \phi(m) \end{aligned}$$

$$\begin{aligned} \phi(nm) &= [nm] \\ &= [n][m] \\ &= \phi(n)\phi(m) \end{aligned}$$

para todo m, n en $\mathbb{Z}$.

Ejemplo 2: Sea R cualquier anillo y definamos

$$\begin{aligned} \phi \ : \ & R \longrightarrow R \\ & \phi(x) = x \end{aligned}$$

Entonces es fácil verificar que ϕ es un homomorfismo, el cual se llama **homomorfismo identidad**.

Definición 7.3.2 *Sea R y R' dos anillos. Un homomorfismo*

$$\phi : R \longrightarrow R',$$

el cual es biyectivo, se dice que es un **isomorfismo de anillo**.

En tal caso diremos, que los anillos R y R' **son isomorfos** y lo simbolizamos por $R \approx R'$.

Al igual que en los homomorfismos de grupos, se tiene la siguiente propiedad para anillos.

Proposición 7.3.1 *Si $\phi : R \longrightarrow S$ es un homomorfismo de anillos, entonces*

i) $\phi(0) = 0$

ii) $\phi(-a) = -\phi(a)$ *para todo* $a \in R$

Demostración: (Ver el capítulo de grupos).

♠

También se define el **Kernel o núcleo** del homomorfismo, exactamente como se hizo en el caso de grupos.

Definición 7.3.3 *Sea $\phi : R \longrightarrow S$ un homomorfismo de anillos, entonces el* **Kernel** *del homomorfismo ϕ se define por*

$$\ker \phi = \{x \in R \mid \phi(x) = 0\}.$$

Observación: Si a y b son dos elementos en el $\ker \phi$, entonces será cierto, de acuerdo a la definición de homomorfismo, que $a + b$ y ab están en $\ker \phi$. Pero además de esta propiedad, el Kernel posee otra muy interesante y es que al multiplicar un elemento cualquiera del anillo por un elemento en el Kernel, entonces el producto de ambos esta de nuevo en el Kernel. Esta propiedad de "absorber" todos los elementos del anillo por multiplicación, motiva la siguiente:

Definición 7.3.4 *Sea R un anillo. Un subconjunto I de R se dice* **ideal a la derecha**, *si se tiene:*

i) $a + b \in I$ *, para todo* $a, b \in I$

ii) $\gamma a \in I$*, para todo* $\gamma \in R$ *y* $a \in I$*.*

Definición 7.3.5 *Sea R un anillo. Un subconjunto I de R se dice* **ideal a la izquierda**, *si satisface*

i) $a + b \in I$, *para todo* $a, b \in I$

ii) $a\gamma \in I$, *para todo* $\gamma \in R$ *y* $a \in I$.

Combinando ambas definiciones tenemos

Definición 7.3.6 *Sea R un anillo. Un subconjunto I de R se dice* **ideal de** *R, si I es un ideal a la derecha y a la izquierda.*

Observación: Cuando se estudian anillos conmutativos (como es el caso de la mayoría de los anillos), entonces todo ideal lateral, a la derecha o a la izquierda, es un ideal del anillo. Por lo tanto no se hace necesario verificar las dos condiciones simultáneamente.

Ejemplo 1: Sea $\mathbb{Z}$ el anillo de enteros y consideremos $I = 2\mathbb{Z}$, el conjunto de los enteros pares. Entonces se puede verificar que I es un ideal de $\mathbb{Z}$.

Ejemplo 2: Sea R el anillo de funciones de $[0, 1]$ en R y S el conjunto de funciones en R, tales que $f(\frac{1}{2}) = 0$. Luego se prueba fácilmente que S es un ideal del anillo R.

Ejemplo 3: Sea $\phi : R \longrightarrow R'$ un homomorfismo de anillos. Entonces el Kernel de ϕ es un ideal de R.

Si I es cualquier ideal en un anillo R, entonces I es un subgrupo normal del grupo aditivo de R. Luego se puede considerar el conjunto cociente R/I de clases laterales derechas. Este conjunto se le puede dotar de una estructura de anillo, con las operaciones de suma y producto de clases definidas de la forma siguiente

$$(a + I) + (b + I) = a + b + I \tag{7.1}$$
$$(a + I)(b + I) = ab + I \tag{7.2}$$

En estas condiciones se tiene:

Teorema 7.3.1 *Sea R un anillo e I un ideal de R. Entonces el conjunto cociente formado por las clases laterales*

$$R/I = \{a + I \mid a \in R\}$$

es un anillo

Este anillo se denomina **anillo cociente**.

Demostración: Debemos verificar en primer lugar que la suma y el producto de clases están bien definidas.

Sean a, b, a', c' elementos en R y supongamos que

$$a + I = a' + I \tag{7.3}$$
$$b + I = b' + I \tag{7.4}$$

Debemos verificar entonces que

1) $a + b + I = a' + b' + I$

2) $ab + I = a'b' + I$

En efecto, para la primera parte usamos las ecuaciones (**??**) y (**??**) para obtener

$$a - a' \in I \quad \text{y} \quad b - b' \in I.$$

Como I es un ideal, la suma de dos elementos cualesquiera en I estará de nuevo en I. Por lo tanto

$$(a - a') + (b - b') \in I,$$

luego

$$(a + b) - (a' + b') \in I,$$

de donde,

$$a + b + I = a' + b' + I.$$

Para la segunda parte, tomamos s_1 y s_2 en I, tales que

$$a = a' + s_1 \quad \text{y} \quad b = b' + s_2$$

Multiplicando estos dos elementos se obtiene

$$\begin{aligned} ab &= (a' + s_1)(b' + s_2) \\ &= a'b' + s_1b' + bs_2 + s_1s_2 \end{aligned}$$

Como I es un ideal, los elementos s_1b', bs_2 y s_1s_2 están todos en I. Luego

$$ab = a'b' + s$$

donde $s = s_1b' + bs_2 + s_1s_2 \in I$

Por lo tanto se concluye

$$ab + I = a'b' + I$$

La verificación de que R/I es un anillo con las dos operaciones dadas en (**??**) y (**??**), se deja como un ejercicio para el lector. Sin embargo haremos algunas acotaciones importantes es este sentido.

Por ejemplo, el elemento cero R/I, viene dado por

$$0 = 0 + I,$$

donde 0 es el cero en R.

Si R posee identidad 1, entonces el anillo cociente posee identidad, dada por

$$1 = 1 + I.$$

Si R es conmutativo, entonces el anillo cociente también es conmutativo.

Teorema 7.3.2 *Sea R un anillo e I un ideal de R. Entonces la aplicación*

$$\phi : R \longrightarrow R/I, \qquad \gamma \longrightarrow \gamma + I$$

es un homomorfismo de anillos sobreyectivo, con $\ker \phi = I$*, llamado la* **proyección de R sobre I.**

Demostración: La demostración de la condición de homomorfismo ϕ, se deriva de las ecuaciones (**??**) y (**??**). En efecto, si γ_1, γ_2 están en R, se tiene

$$\begin{aligned} \phi(\gamma_1 + \gamma_2) &= (\gamma_1 + \gamma_2) + I \\ &= (\gamma_1 + I) + (\gamma_2 + I) \\ &= \phi(\gamma_1) + \phi(\gamma_2) \end{aligned}$$

$$\begin{aligned} \phi(\gamma_1\gamma_2) &= \gamma_1\gamma_2 + I \\ &= (\gamma_1 + I)(\gamma_2 + I) \\ &= \phi(\gamma_1)\phi(\gamma_2) \end{aligned}$$

Evidentemente, el homomorfismo es sobreyectivo. Veamos a continuación la determinación del $\ker \phi$.

Sea $\gamma \in R$, tal que

$$\phi(\gamma) = \gamma + I = I$$

Luego $\gamma \in I$.

Por otro lado, si $\gamma \in I$ es claro que

$$\phi(\gamma) = I = 0 \quad \in R/I.$$

Luego

$$I = \ker \phi$$

♠

Basándonos en los teoremas de isomorfismos para los grupos, damos a continuación dos teoremas sobre homomorfismos de anillos. Las demostraciones se omiten pues son muy semejantes a las demostraciones dadas en el caso de los grupos.

Teorema 7.3.3 *Sea $\phi : R \longrightarrow S$ un homomorfismo de anillos sobreyectivo. Entonces*

i) Si I es un ideal de R que contiene a $\ker\phi$, entonces el conjunto

$$I' = \{\phi(x) \mid x \in I\}$$

es un ideal de S.

ii) Si L es un ideal de S, entonces el conjunto

$$\phi^{-1}(L) = \{x \in R \mid \phi(x) \in L\}$$

es un ideal de R que contiene a $\ker\phi$.

Teorema 7.3.4 *Sea $\phi : R \longrightarrow S$ un homomorfismo de anillos sobreyectivo con $K = \ker\phi$, y supongamos que I es un ideal de R que contiene a K. Sea L el ideal de S, dado por $L = \phi(I)$. Entonces*

$$R/K \approx S/L$$

Ejercicios

1) Sea U un ideal de anillo R y supongamos que el elemento unidad de R está en U. Probar entonces que $U = R$.

2) Probar que si R es un cuerpo, entonces los únicos ideales son (0) y R.

3) Probar que cualquier homomorfismo de anillos $\phi : R \longrightarrow S$, con R cuerpo, satisface $\phi = 0$ o $\phi =$identidad.

4) Sean I y J ideales de un anillo R. Entonces la suma de I con J se define

$$I + J = \{x + y \mid x \in I,\ y \in J\}$$

El producto de I con J se define por

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i \mid \text{ donde } x_i \in I,\ y_i \in J,\ 1 \leq i \leq n,\ n \geq 1 \right\}$$

Entonces probar que tanto $I + J$ como IJ son ideales de R.

5) Probar que si $\phi : R \longrightarrow S$ es un homomorfismo de anillos, sobre y $1 \in R$, entonces $\phi(1)$ es la identidad en S. Dar un ejemplo en donde esto no se cumple si se remueve la condición de sobreyectividad.

6) Sea $\phi : R \longrightarrow S$ un homomorfismo de anillos sobre. Probar que si I es un ideal de R, entonces $\phi(I)$ es un ideal de S.

7) Sea R un anillo, U un ideal de R y

$$\gamma(U) = \{x \in R \mid xu = 0,\ \forall u \in U\}$$

Probar que $\gamma(U)$ es un ideal de R. Este ideal se llama el **radical de** U.

8) Demuestre que si $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}$ es un homomorfismo de anillos sobreyectivo, entonces $\phi =$ identidad.

9) Sea R el anillo de matrices cuadradas reales 2×2 y consideremos el subconjunto S, de R de todas aquellas matrices de la forma

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

i) Probar que S es un sub-anillo de R.

ii) ¿Es S un ideal de R?.

10) Sea S el anillo de matrices definido arriba y $\mathbb{C}$ el anillo de los complejos. Probar que S es isomorfo a $\mathbb{C}$.

11) Sea $\mathbb{C}$ el anillo de los complejos, probar que la aplicación

$$\begin{array}{rccc} \phi & : & \mathbb{C} & \longrightarrow & \mathbb{C} \\ & & a+bi & \longrightarrow & a-bi \end{array}$$

es un homomorfismo de anillos.

12) Sea R un anillo conmutativo y $a \in R$. Definamos el conjunto

$$Ra = \{ra \mid r \in R\}$$

Probar que Ra es un ideal de R. Este ideal se denomina el **ideal generado por** a.

13) Sea R un anillo conmutativo con 1. Probar que $a \in R$ es invertible si y sólo si $Ra = R$.

14) Probar que si I y J son ideales de un anillo R, entonces $I \cap J$ es también un ideal.