UNIVERSIDAD NACIONAL DE EDUCACIÒN

Enrique Guzmán y Valle

Alma Máter del Magisterio Nacional

FACULTAD DE CIENCIAS

Escuela Profesional de Matemática e Informática

MONOGRAFÍA

ANILLO DE POLINOMIOS

Sucesiones en un anillo. Sucesión casi nula. Adición y multiplicación de sucesiones casi nulas. Construcción del anillo de Polinomios sobre un anillo o campo. Divisibilidad de Polinomios. Raíces de Polinomios Irreducibles.

Examen de Suficiencia Profesional Res. Nº1152-2018-D-FAC

Presentada por:

Rosa Isabel ALHUAY JUAREZ

Para optar al Título Profesional de Licenciado en Educación

Especialidad: Matemática e Informática

Lima, Perú

2018

MONOGRAFÍA

ANILLO DE POLINOMIOS

Sucesiones en un anillo. Sucesión casi nula. Adición y multiplicación de sucesiones casi nulas. Construcción del anillo de Polinomios sobre un anillo o campo. Divisibilidad de Polinomios. Raíces de Polinomios Irreducibles.

Designación de Jurado Resolución N°1152-2018-D-FAC

Mg. Aurelio Julián GÁMEZ TORRES
PRESIDENTE

Lic. Faustino Fortunato CUENCA CERVANTES
SECRETARIO

Lic. Vicente Carlos DAVILA HUAMAN
VOCAL

Línea de investigación: Curriculum y formación profesional en educación.

Dedicatoria:

A con aprecio a mis padres por incentivarme a perseverar en mis sueños.

Contenido

Introducción

La presente investigación monográfica titulada: *Anillo de polinomios*, tiene el propósito de mostrar la importancia que tienen los polinomios desde el punto de vista de su estructura algebraica, identificando las operaciones fundamentales que es posible realizar con ellos así como las propiedades que tienen.

Se sabe que los polinomios constituyen objetos matemáticos fundamentales en la enseñanza de la matemática en los diversos niveles educativos; asimismo son múltiples sus aplicaciones en las diversas disciplinas científicas, en el ejercicio de muchas profesiones, hasta en situaciones cotidianas. Así, usamos los polinomios para generalizar propiedades aritméticas, para representar relaciones entre diversas magnitudes, son la forma en la que se expresan la mayoría de las funciones y en la resolución de diferentes tipos de ecuaciones.

El presente investigación está estructura en 3 capítulos: El capítulo I, desarrolla conceptos preliminares sobre anillo de polinomios; el capítulo II, trata sobre sucesiones, sucesiones casi nulas, conjunto en el que se definen las operaciones de adición y multiplicación, así como la estructura algebraica que tienen; el capítulo III, presenta la aplicación didáctica a través de una sesión de aprendizaje; síntesis, conclusiones, apreciación crítica y sugerencias, y referencias.

De los distintos anillos que se conocen, los anillos de polinomios son tal vez uno de los más importantes. Por lo que es relevante construir los anillos de polinomios a partir de los conceptos de sucesiones, realizar operaciones y estudiar otras características de dicho anillo, que es fundamental en cualquier curso de álgebra y cálculo, quizá sea ésta la utilidad más importante de los polinomios que nos ayudará al desarrollo de las capacidades del razonamiento lógico algebraico. Finalmente, manifestamos que el presente estudio acerca del anillo de polinomios, nos ha permitido una mejor comprensión de estos objetos matemáticos, asimismo relacionar con otros objetos matemáticos que pese a ser de diferente naturaleza tienen la misma estructura algebraica. Del mismo modo, esperamos, que este trabajo sirva principalmente para motivar a que los estudiantes y los docentes de matemática en una actitud de aprendizaje permanente, para mejorar su desempeño profesional.

Capítulo I: Conceptos preliminares

1.1. Leyes de composición interna

Definición:

Sea $A \neq \Phi$, una ley de composición interna (LCI) es toda aplicación "$*$" de $A \times A$ en A.

Notaciones:

Si $*$ es una LCI en A, lo representamos por:

$$* : A \times A \to A$$

$(a;b) \to a*b$ y leemos "a compuesta con b"

Ejemplo 1:

Si A = N, Z, R,... y ; $* = +$ **la adición;** $* = \bullet$ **la multiplicación**

La adición es una ley de composición interna definida sobre A, pues:

$$+ : N \times N \to N$$

$$(a;b) \to a+b$$

$$(2;3) \to 2+3=5 \in N$$

La Multiplicación es una ley de composición interna definida sobre A, pues:

$$\bullet : Z \times Z \to Z$$

$$(a;b) \to a \bullet b$$

$$(2;3) \to 2 \bullet 3 = 6 \in Z$$

Ejemplo 2:

¿Será la sustracción una LCI en N?

$$-: N \times N \rightarrow N$$

$$(a;b) \rightarrow a-b$$

$$(3;2) \rightarrow 3-2=1 \in N$$

$$(2;3) \rightarrow 2-3=-1 \notin N$$

Por lo tanto, la sustracción no es una LCI sobre N

1.2. Estructura algebraica

Definición.-

Una estructura algebraica es un conjunto $A \neq \Phi$ provisto de una o más leyes de composición interna y/o externa o sus combinaciones.[1]

Notación:

Las estructura algebraicas se denotan como: (A,*, $, T, #, ...), donde A es el conjunto no vacío, y ,*, $, T, #, ..., son las leyes definidas en dicho conjunto.

1.3. Grupos y subgrupos

Definición.-

Sea $G \neq \Phi$, "$*$" una L.C.I.; decimos que el monoide $(G;*)$ tiene la estructura de ***grupo*** si verifica los siguientes axiomas:

1) Asociativa; "$*$" es asociativa $(x*y)*z = x*(y*z)$, $\forall x,y,z \in G$.

2) Existencia del elemento Neutro; $\exists e \in G / e*x = x*e = x$, $\forall x \in G$.

3) Existencia del elemento Simétrico; $\exists x' \in G$, $x'*x = x*x' = e$, $\forall x \in G$.

Si además se cumple:

---

[1] Algunos autores, a la estructura algebraica (A, *) le llaman ***monoide***.

4) Conmutativa; $x * y = y * x$, $\forall x, y \in G$, el grupo $(G,*)$ es un Grupo Abeliano

Ejemplo 1:

$(Z;+)$ es grupo Abeliano.

En efecto:

$+ : Z \times Z \to Z$

$(a;b) \to a + b$

Además cumple:

1) $\forall x, y, z \in Z$; $(x + y) + z = x + (y + z)$

2) Existe e = 0 $\in Z / 0 + x = x + 0 = x \ \forall x \in Z$

3) $\forall x \in Z$, $\exists - x \in Z /$ $(-x) + x = x + (-x) = 0$

4) $x + y = y + x$, $\forall x, y \in Z$

Ejemplo 2:

Sea G el conjunto de los números enteros, con la operación de la multiplicación "●", ¿Será $(Z;\bullet)$ un grupo?

Prueba:

La multiplicación es una LCI en los enteros

$\bullet : Z \times Z \to Z$

$(a;b) \to a \bullet b$

Además cumple:

1) Asociatividad $\forall x, y, z \in Z$; $(x \bullet y) \bullet z = x \bullet (y \bullet z)$
2) Existe e=1 $\in Z / 1 \bullet x = x \bullet 1 = x \ \forall x \in Z$
3) Existencia del Simétrico: se debe probar que: $\forall x \in Z, \exists x' \in Z / x' * x = x * x' = 1$, pero no existe en el conjunto de los enteros el inverso de cada número.

Por lo tanto $(Z;\bullet)$ no es un grupo.

Ejemplos 3:

En el conjunto de los números enteros Z se define la operación $*$ mediante $a * b = a + b + 3$. ¿Será el par $(Z, *)$ un grupo abeliano?

Prueba

a. **Asociativa**

$(a * b) * c = (a + b + 3) * c = a + b + 3 + c + 3 = a + b + c + 6$

y $a * (b * c) = a * (b + c + 3) = a + b + c + 3 + 3 = a + b + c + 6$

se verifica la igualdad.

b. **Elemento neutro**

$\forall a \in Z$ **,** $a * e = a$ **entonces** $a + e + 3 = a \Rightarrow e = -3$

y $e * a = a$ **entonces** $e + a + 3 = a \Rightarrow e = -3.$

Como el neutro a izquierda y el neutro a derecha son iguales, entonces existe el neutro $e = -3$.

c. **Inverso**

Supongamos que $\forall a \;,\; \exists a' \;/\; a * a' = e$, en nuestro caso

$a * a' = -3 \Rightarrow a + a' + 3 = -3$ luego $a' = -a - 6$ es inverso a derecha

$a' * a = -3 \Rightarrow a' + a + 3 = -3$ luego $a' = -a - 6$ es inverso a izquierda

d. **Conmutativa** $a * b = a + b + 3 = b + a + 3 = b * a$.

Por lo tanto de 1), 2), 3) y 4) se concluye que $(Z, *)$ un grupo Abeliano.

1.4. Anillos y subanillos

El concepto de anillo se obtiene como una generalización del conjunto de los números enteros con la adición, en donde ahora están definidas dos operaciones, la adición y la multiplicación, relacionadas entre sí por una ley de distributiva.

Los anillos son estructuras algebraicas más completas que los grupos, pero sin embargo en el estudio de sus propiedades más importantes, nos apoyamos en la Teoría de los grupos. La razón para esto es muy simple, pues todo anillo es un grupo en sí mismo.

1.4.1. Tipos de anillos

Definición.-

Sea el conjunto A diferente del vacío $(A \neq \emptyset)$ y las operaciones binarias " $+$ " y " $.$ "; la terna $(A, +, \ .)$ es un **Anillo**, si y sólo si cumple las condiciones siguientes:

1°) $(A; +)$ es un Grupo Abeliano

2°) $(A; .)$ es un Semigrupo

3°) La segunda operación $(+)$ es distributiva respecto a la primera operación $(.)$. Es decir:

La terna $(A, \ +, \ \cdot)$ es un **anillo** si y solo si, se cumplen los siguientes axiomas:

$A_1 : a + (b + c) = (a + b) + c \quad \forall \ a, b, c \in R$

Ley de Asociatividad respecto de " $+$ "

$A_2 : a + 0 = a, \quad 0 + a = a \qquad \forall \ a \in R$

Ley de la Identidad respecto de " $+$ "

$A_3 : a + (-a) = 0, \quad (-a) + a = 0$

Ley del opuesto aditivo.

$A_4 \ : a \ + b \ = \ b + a \ , \ \forall \ a, b \in R$

Ley conmutativa respecto de " $+$ "

$A_5 \ : \ a \, , \ b \ \in \ R \ \Rightarrow \ a \cdot b \ \in \ R$

Ley de clausura respecto de " $\cdot$ "

$A_6 \ : \ a \cdot (b \cdot c) = (\, a \cdot b) \cdot c \ ; \ \forall \ a, b, c \in R$

Ley de Asociatividad respecto de " $\cdot$ "

$$A_7 \ : \ \begin{matrix} a \cdot (b + c) = a \cdot b + a \cdot c \\ (b + c) \cdot a = b \cdot a + c \cdot a \end{matrix} \qquad \forall \ a, b, c \ \in \ R$$

Ley distributiva de la " $\cdot$ " respecto a la " $+$ "

Ejemplo 1:

$(\mathbb{Z}, +, \ \cdot)$, $(\mathbb{Q}, +, \ \cdot)$, $(\mathbb{R}, +, \ \cdot)$ y $(\mathbb{C}, +, \ \cdot)$ son anillos.

1.4.1.1. Anillo conmutativo

Definición:

Se llama anillo conmutativo a todo anillo $(R; *; \ \Delta)$ que cumple la propiedad:

$\forall \ a; \ b \ \in \ R \ \Rightarrow \ a \, \Delta \, b = b \, \Delta \, a$

Ejemplo 1:

En el conjunto de los números reales se definen las operaciones

$$x * y = x + y + 4, \quad x \circ y = xy + 4x + 4y + 12.$$

Probar si $(\mathbb{R}, \ *, \ \circ)$ es anillo conmutativo.

Prueba

a. Veamos que $(\mathbb{R},*)$ **es grupo Abeliano.**

i) La operación $*$ es cerrada.

ii) Asociativa

Si $x,\ y,\ z$ son números reales cualesquiera se verifica

$(x * y) * z = (x + y + 4) * z = x + y + 4\ + z\ + 4\ = x + y\ + z + 8.$

$x * (y * z) = x * (y + z + 4) = x\ + y + z + 4 + 4\ =\ x + y\ + z\ + 8.$

Es decir, la operación es asociativa.

iii) Conmutativa

Si $x,\ y$ son números reales cualesquiera se verifica que

$$x * y = x + y + 4 = y + x + 4 = y * x\ ,$$

Por tanto, $*$ es conmutativa.

iv) Elemento neutro

Supongamos que el número real e es neutro para la operación $*$ entonces debe cumplir que $e * x = x * e = x,\ \forall\ x \in R.$

Esto equivale a $e + x + 4 = x,$ es decir $e = -4$ es elemento neutro para la operación $*$. Similarmente el otro caso.

v) Elemento simétrico

Debido a la conmutatividad, un $x \in R$ tiene elemento simétrico $x' \in R$ si y solo si $x * x' = e$ o bien si $x + x' + 4 = -4.$

Existe por tanto x' para cada x siendo éste $x' = -8 - x.$

b. Veamos ahora que $(\mathbb{R}, \circ)$ **es semigrupo.**

i) Cerradura

La operación $\circ$ **es cerrada,** pues la suma y el producto de números reales es un número real.

ii) Asociativa

Se cumple pues:

$$(x \circ y) \circ z = (xy + 4x + 4y + 12) \circ z$$

$$= xyz + 4xz + 4yz + 12z + 4xy + 16x + 16y + 48 + 4z + 12$$

$$= xyz + 4(xy + xz + yz) + 16(x + y + z) + 60.$$

$$x \circ (y \circ z) = x \circ (yz + 4y + 4z + 12)$$

$$= xyz + 4xy + 4xz + 12x + 4x + 4yz + 16y + 16z + 48 + 12$$

$$= xyz + 4(xy + xz + yz) + 16(x + y + z) + 60.$$

iii) La operación $\circ$ es conmutativa.

iv) La operación $\circ$ es distributiva respecto a la operación $*$ si y solo si se verifica

$$x \circ (y * z) = (x \circ y) * (x \circ z).$$

Se cumple, pues:

$$x \circ (y * z) = x \circ (y + z + 4)$$

$$= xy + xz + 4x + 4x + 4y + 4z + 16 + 12$$

$$= xy + xz + 4(2x + y + z) + 28,$$

$$(x \circ y) * (x \circ z) = (xy + 4x + 4y + 12) * (xz + 4x + 4z + 12)$$

$$= xy + 4x + 4y + 12 + xz + 4x + 4z + 12 + 4$$

$$= xy + xz + 4(2x + y + z) + 28.$$

Por lo tanto, concluimos que $(\mathbb{R}, *, \circ)$ es un anillo conmutativo.

1.4.1.2. Anillo con identidad

Definición.-

Se llama anillo con identidad o con unidad a todo anillo $(R;*;\ \Delta)$ que cumple la propiedad:

$\forall\ a \in R,\ \exists\ 1 \in R\ /\ \ a\,\Delta\,1 = 1\,\Delta\,a = a.$

Observación:

Un anillo $(\mathrm{R},+,\cdot)$ siempre contiene al elemento 0. Si este es el único elemento de $(\mathrm{R},+,\cdot)$ entonces $(\mathrm{R},+,\cdot)$ se llama el **anillo nulo** o el anillo cero.

Definición.-

El anillo $(\mathrm{R},+,\cdot)$ no tiene divisores de cero, si y sólo si, elementos no nulos dan producto diferente de cero. Es decir:

$R\ carece\ de\ divisores\ de\ cero \Longleftrightarrow \forall\, x,y:\ \ x \neq 0 \wedge y \neq 0 \Rightarrow\ x.y \neq 0$

Análogamente

$R\ carece\ de\ divisores\ de\ cero \Longleftrightarrow \forall\, x,y:\ x.y = 0 \Rightarrow x = 0 \vee y = 0$

Definición: El anillo $(\mathrm{R},+,\cdot)$ tiene **divisores de cero**, si y sólo si elementos no nulos dan producto nulo. Es decir:

$R\ tiene\ divisores\ de\ cero \Longleftrightarrow \forall\, x,y:\ \ x \neq 0 \wedge y \neq 0 \Rightarrow\ x.y = 0$

Ejemplo 1:

Determinar los divisores de cero del anillo $\mathbb{Z}_6$:

Solución:

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

La tabla de Caylei del producto es:

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Luego:

$$[2] \neq [0] \quad y \quad [3] \neq [0],$$

pero,

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

De aquí, deducimos que los divisores de cero son 2, 3 y 4.

Ejemplo 2:

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

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.-

Un anillo $(R;\ *;\ \Delta)$ se dice que es un cuerpo o campo si:

1°) $(R;\ *)$ es un Grupo Abeliano

2°) $(R';\ \Delta)$ es un Grupo Abeliano, $R' = R - \{0\}$

Ejemplo:

$(\mathbb{Q}, +,\ \cdot)$, $(\mathbb{R}, +,\ \cdot)$ y $(\mathbb{C}, +,\ \cdot)$ son cuerpos.

1.5. Subanillos

Definición.-

Sea $(R, +, \cdot)$ un anillo; un subconjunto $A \subset R$ es un **Subanillo** de $(R, +, \cdot)$; si $(A, +, \cdot)$ es un anillo.

Observación:

Sea $(\mathbb{Z}, +, \cdot)$ el anillo de los enteros, como $2\mathbb{Z},\ 3\mathbb{Z},\ 5\mathbb{Z},\ 6\mathbb{Z}, ...$ están contenidos en $\mathbb{Z}$; entonces se tiene que $(2\mathbb{Z}, +, \cdot)$, $(3\mathbb{Z}, +, \cdot)$, $(5\mathbb{Z}, +,\ \cdot)$, …. Son subanillos de $(\mathbb{Z}, +,\ \cdot)$.

Es condición suficiente para probar que un subconjunto de un conjunto es un Subanillo del anillo:

$$i)\quad \forall\ a, b\ \in R\ ;\quad a - b \in R$$

$$ii)\quad \forall\ a, b\ \in R\ ;\quad a \cdot b \in R$$

Con esta definición probemos el siguiente ejemplo.

Ejemplo 1:

El conjunto de los enteros pares $(2\mathbb{Z}, +, \cdot)$ es un Subanillo del anillo $(\mathbb{Z}, +, \cdot)$ de los números enteros.

Prueba

En efecto:

i) Si $a \in 2\mathbb{Z}, \quad b \in 2\mathbb{Z} \;\Rightarrow\; a - b \in 2\mathbb{Z}$

Pero $si \;\; a \in 2\mathbb{Z}; \quad a = 2n, \quad n \in \mathbb{Z}$

$si \;\; b \in 2\mathbb{Z}; \quad b = 2m, \quad m \in \mathbb{Z}$

Entonces:

$$\begin{aligned} a - b &= 2n - 2m \\ &= 2(n - m) \\ &= 2t \quad \in \quad 2\mathbb{Z} \end{aligned}$$

ii) Si $a \in 2\mathbb{Z}, \quad b \in 2\mathbb{Z} \;\Rightarrow\; a \cdot b \in 2\mathbb{Z}$

Similarmente al caso anterior.

$$si \;\; a \in 2\mathbb{Z}; \quad a = 2n, \quad n \in \mathbb{Z}$$

$$si \;\; b \in 2\mathbb{Z}; \quad b = 2m, \quad m \in \mathbb{Z}$$

Entonces:

$$\begin{aligned} a - b &= (2n)(2m) \\ &= 2(2nm) \\ &= 2p \quad \in \quad 2\mathbb{Z} \end{aligned}$$

$\therefore \quad (2\mathbb{Z}, +, \cdot)$ es un Subanillo de $(\mathbb{Z}, +, \cdot)$

Observación:

En general, de esta manera se puede probar que:

$$(n\mathbb{Z}, +, \cdot) \text{ es un subanillo de } (\mathbb{Z}, +, \cdot), \quad \forall\ n \geq 1.$$

Proposición:

Sea $(R, +, \cdot)$ un anillo y sea B un subconjunto no vacío de R

$$B \text{ es Subanillo de } R \iff \begin{cases} \text{i)} \quad \forall\, a, b \in B \implies a - b \in B \\ \text{ii)} \quad \forall\, a, b \in B \implies a.b \in B \end{cases}$$

Demostración

$\Rightarrow)$

Si B es subanillo de R, entonces $B \neq \emptyset$ pues $0 \in B$. Además, B es subgrupo aditivo de R , luego se cumple (i). Como la operación producto es cerrada en B , se cumple (ii).

$\Leftarrow)$

De $B \neq \emptyset$ y (i), se deduce que $(B, +)$ es subgrupo de $(R, +)$ y además abeliano por serlo $(R, +)$, es decir, $(B, +)$ es grupo abeliano. De (ii) se deduce que la operación producto es cerrada en B, y además, es asociativa en B por serlo en R, lo cual implica que $(B, \cdot)$ es semigrupo.

Por último, se cumple la propiedad distributiva en B al cumplirse en R. Concluimos que $(B, +, \cdot)$ es anillo, y por tanto B es subanillo de R.

Ejemplo:

Verifique si el conjunto $B = \{\overline{0}, \overline{5}, \overline{10}\}$ es un subanillo del anillo $(\mathbb{Z}_{15}, +, \cdot)$.

Prueba

$B=\{\overline{0},\overline{5},\overline{10}\}\subset(\mathbb{Z}_{15},+,\cdot)$ es Subanillo si: $\begin{array}{l}\forall\, x,y\ \in B \;,\;\; x-y\in B\\ \forall\, x,y\ \in B \;,\;\; x\cdot y\in B\end{array}$

Cada elemento operado con su opuesto en $(\mathbb{Z}_{15},+,\cdot)$ se tiene:

$$\forall\, x,y\ \in B\,,\quad x-y\in B$$

$$\forall\, x,y\ \in B\,,\quad x\cdot y\in B$$

$$\begin{array}{ll}
0-0=0+0=\overline{0}\in B & 0\cdot 0=\overline{0}\in B\\
0-5=0+10=\overline{10}\in B & 0\cdot 5=\overline{0}\in B\\
0-10=0+5=\overline{5}\in B & 0\cdot 10=\overline{0}\in B
\end{array}$$

$$\begin{array}{ll}
5-0=5+0=\overline{5}\in B & 5\cdot 0=\overline{0}\in B\\
5-5=5+10=\overline{0}\in B & 5\cdot 5=\overline{10}\in B\\
5-10=5+5=\overline{10}\in B & 5\cdot 10=\overline{5}\in B
\end{array}$$

$$\begin{array}{ll}
10-0=10+0=\overline{10}\in B & 10\cdot 0=\overline{0}\in B\\
10-5=10+10=\overline{5}\in B & 10\cdot 5=\overline{5}\in B\\
10-10=10+5=\overline{0}\in B & 10\cdot 10=\overline{10}\in B
\end{array}$$

Luego $B=\{\overline{0},\overline{5},\overline{10}\}$ es un subanillo de $(\mathbb{Z}_{15},+,\ \cdot)$.

Observación:

Los subanillos pueden contener o no a la unidad; también puede ser que un subanillo de un anillo no conmutativo, sea conmutativo.

Definición:

Un subconjunto $A\subset R$ (Anillo) tal que $A\neq\emptyset$ se dice que es un subanillo de R si A con las operaciones de R posee estructura de anillo.

Ejemplo 2:

$(\mathbb{Z},+,\ \cdot)$ es subanillo de $(\mathbb{Q},+,\ \cdot)$, de $(\mathbb{R},+,\ \cdot)$ y de $(\mathbb{C},+,\ \cdot)$.

Observación:

- Si $1 \in R$ se dice que R es un subanillo con unidad.
- En todo anillo R, el conjunto R y el 0 son subanillos, llamados subanillos triviales.

  Los demás subanillos se llaman propios.
- La unión de subanillos no siempre es un subanillo.

  Veamos un ejemplo.

Sea $(\mathbb{Z},+,\ \cdot)$ un anillo y $(n\mathbb{Z},+,\ \cdot)\ \ \forall\ n \geq 1$ subanillos de $(\mathbb{Z},+,\ \cdot)$.

Tenemos que:

$2\mathbb{Z} \cup 8\mathbb{Z} = 2\mathbb{Z}$, es un subanillo de $(\mathbb{Z},+,\ \cdot)$

pero $2\mathbb{Z} \cup 3\mathbb{Z} \neq n\mathbb{Z}$, no es subanillo de $(\mathbb{Z},+,\ \cdot)$.

Capítulo II: Anillo de polinomios

Para realizar la construcción de un anillo de polinomios, debemos iniciar a partir de los conceptos de anillo, definir los conceptos de sucesiones en un anillo, caracterizar la sucesiones nulas y casi nulas; en el conjunto de sucesiones casi nulas definiremos las operaciones de adición (+) y multiplicación (.), y en las cuales dicho conjunto tendrá la estructura de un anillo, al que se le dominará, el anillo de polinomios y que cada sucesión casi nula constituirá un polinomio, con coeficientes los elementos del anillo

2.1. Sucesión

Una sucesión es una función cuyo dominio es el conjunto de los números naturales y cuya imagen es un anillo A; es decir:

$$S : N \to A$$

$$(i) \to S(i)$$

Donde N es el conjunto de números naturales sin el cero.

En la definición se supone que $i \in N.$ La imagen del número i se suele denotar por a_i, $i \in N$ Entonces la sucesión será S= $(a_0, a_1, a_2, a_3,......., a_i \ \ldots)$ donde los elementos de la sucesión pertenecen al anillo A.

Notación:

Si $S:N \rightarrow A$ es una sucesión:

$0 \rightarrow S(0) = a_0$

$1 \rightarrow S(1) = a_1$

$2 \rightarrow S(2) = a_2$

$3 \rightarrow S(3) = a_3$

$4 \rightarrow S(4) = a_4$

$5 \rightarrow S(5) = a_5$

$6 \rightarrow S(6) = a_6$

$7 \rightarrow S(7) = a_7$

....

$i \rightarrow S(i) = a_i$

Los elementos $a_0, a_1, a_2, a_3, ..., a_i$ pertenecen al anillo A

La sucesión S en A se puede expresar mediante:

$$S = (a_0, a_1, a_2, a_3, ..., a_i, a_{i+1} ....)$$

Si T es otra sucesión en A entonces se expresa como:

$$T : N \rightarrow A$$

$$(i) \rightarrow t(i) = b_i$$

Luego, $T = (b_0, b_1, b_2, b_3, ..., b_i, b_{i+1} ....)$

Donde $b_0, b_1, b_2, b_3, ..., b_i, b_{i+1}, ...$ son elementos de A

Ejemplos:

Sea (R,+, ●) el anillo de los números reales.

Definimos la sucesión $S:N \to R/\ S(i)=\frac{1}{i}$, es decir:

$$S:N \to R$$

$$1 \to S(1)=\frac{1}{1}=1$$

$$2 \to S(2)=\frac{1}{2}=\frac{1}{2}$$

$$3 \to S(3)=\frac{1}{3}=\frac{1}{3}$$

....

$$i \to S(i)=\frac{1}{i}=a_i$$

Entonces S= ($a_0, a_1, a_2, a_3, \ldots\ldots, a_i, a_{i+1} \ldots$)

Es decir S= (1,1/2,1/3,1/4…..1/i,…)

2.2. Sucesiones nulas y casi nulas

2.2.1 Sucesión nula

Se denomina sucesión nula a aquella sucesión cuyos elementos son todos ceros.

Si definimos:

Θ: N→ ℤ, $\theta(n)=0$, ∀n∈N

Θ: N→ ℤ

$0 \to \theta\ (0) = b_0=0$

$1 \to \theta\ (1) = b_1=0$

$2 \to \theta\ (2) = b_2=0$

$3 \to \theta\ (3) = b_3=0$

$4 \rightarrow \theta(4) = b_4 = 0$

$5 \rightarrow \theta(5) = b_5 = 0$

……………………………..

$n \rightarrow \theta(n) = b_n = 0$

…………………..

$\Theta = (b_0, b_1, b_2, b_3, \ldots b_n, \ldots) = (0, 0, 0, 0, 0, 0, 0, 0, 0, \ldots)$

Entonces, Θ se llama sucesión nula en A= $\mathbb{Z}$

2.2.2 Sucesión casi nula

Definición:

Se denomina sucesión casi nula, a aquella sucesión cuyos elementos son ceros excepto un número finito de ellos.

Una sucesión S = ($a_0, a_1, a_2, a_3, \ldots\ldots, a_i, a_{i+1} \ldots$) en un anillo se dice casi nula si existe algún natural i tal que para todo k >i, se tiene que $a_{k=0}$.

Se denota por: S= ($a_0, a_1, a_2, a_3, \ldots\ldots, a_i, 0,0,0\ldots$)

Ejemplo:

Sea A= $\mathbb{Z}$, el anillo de los números enteros con las operaciones de adición y multiplicación conocidas:

a) Sea S: N→ Z la sucesión definida como:

$0 \rightarrow S(0) = 0$

$1 \rightarrow S(1) = -3$

$2 \rightarrow S(2) = 4$

$3 \rightarrow S(3) = 8$

$4 \rightarrow S(4) = 0$

$5 \rightarrow S(5) = 0$

… ….

$n \rightarrow S(n) = 0$

… ….

S = (0, -3, 4, 8, 0,0,….)

Luego S es una sucesión casi nula.

b) Si definimos la sucesión q: $N \rightarrow \mathbb{Z}$, tal que:

$0 \rightarrow q(0) = 2$

$1 \rightarrow q(1) = 2$

$2 \rightarrow q(2) = -1$

$3 \rightarrow q(3) = 2$

$4 \rightarrow q(4) = 12$

$5 \rightarrow q(5) = 0$

$6 \rightarrow q(6) = 0$

… ….

q = (2, 2, -1, 2, 12, 0, 0,0)

Así, se tiene que q es una sucesión casi nula.

c) R = (0,0,0,0, ...) es una sucesión casi nula y se llama sucesión cero (0) o sucesión nula, se denota con $r = 0 = \theta$.

d) Son también sucesiones casi nulas

S_1= (1,0,0,0…..)

S_2= (0,1,0,0…..)

S_3= (0,0,1,0,0,0…..)

S_4= (0,0,0,1, 0, …..)

… ….

$S_n = (0,0,0,0,0,0……,0,0,1,0,0,0…..)$

2.3. Operaciones con sucesiones

2.3.1 Adición de sucesiones casi nulas

Sea (A,+,●) un anillo conmutativo con unidad. Denotamos por N(A) al conjunto formado por todas las sucesiones casi nulas; es decir:

N(A)= {S: N→A/ S es una sucesión casi nula}

Definición.-

Sean S_i y S_j dos sucesiones casi nulas.

S ∊N (A) → S= $(a_0, a_1, a_2, a_3,......., a_m.,0,0,0...)$

t ∊N (A) → t = $(b_0, b_1, b_2, b_3,.......,, b_n,0,0,0...…..)$

Definimos la **suma de sucesiones casi nulas** mediante:

S + t = $(a_0 + b_0, a_1 + b_1,......., a_n + b_n,..)$ ∈ A

Ejemplo 1:

Sean A el anillo de los enteros y sean R y S dos sucesiones casi nulas en ℤ:

R = (1,2,3,-4,0,0,0,….)

S = (0,2,5,6,7,9,0,0,0….)

R + S =(1,4,8,2,9,0,0,0,…)

Observación:

R + S también es una sucesión casi nula de ℤ, es decir, (R + S) ∊N(A), con A= ℤ

Ejemplo 2:

Sean las sucesiones:

$S = (0,0,1,7,0,0,0\ldots)$

$T = (-2,8,0,0,0,0,0\ldots)$

$S + T = (-2, 8, 1, 7, 0, 0,0,\ldots.)$

También $(S + T) \in N(A)$, es decir es una sucesión casi nula.

Ejemplo 3:

Sea el anillo $(Q,+,\bullet)$ donde Q es el conjunto de los números racionales; dados las sucesiones T y S, casi nulas:

$T = (\frac{1}{3}, \frac{-1}{8}, 0, \frac{3}{4}, 0,0,0\ldots)$

$S = (\frac{1}{3}, \frac{1}{8}, 1, \frac{-1}{4}, 2,0,0\ldots)$

$T + S = (2/3,0,1, \frac{1}{2}, 2,0,0,\ldots)$

$(T + S) \in N(A)$.

Nota:

Para sumar dos sucesiones casi nulas se suman los términos correspondientes de cada sucesión.

2.3.2 Multiplicación de sucesiones casi nulas

Definición.-

Sean las sucesiones S y T,

$S = (a_0, a_1, a_2. . . , a_n,\ldots\ldots,0,0,0,0,0\ldots..)$

$T = (b_0, b_1, b_2. . . , b_n,b_{n+1}\ldots..,b_m ,0,0,0,0,0\ldots..)$, definimos el producto de dichas sucesiones como:

$S.T = (c_0,c_1, c_2, c_3,\ldots\ldots,c_{r-1}, c_r,\ldots..0,0,0\ldots)$

donde: $c_k= \sum_{i+j=k} a_i b_j$

Para realizar el producto de dichas sucesiones, se debe tener en cuenta que, si m = n o si m > n (o para m < n) definimos el producto de sucesiones casi nulas, de la siguiente manera:

$c_0 = a_0 b_0$

$c_1 = a_1 b_0 + a_0 b_1$

$c_2 = a_2 b_0 + a_1 b_1 + a_0 b_2$

$c_3 = a_3 b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3$

$c_4 = a_4 b_0 + a_3 b_1 + a_2 b_2 + a_1 b_3 + a_0 b_4$

……… ………………………………..

$c_k = a_k b_0 + a_{k-1} b_1 + a_{k-2} b_{k-2} + \ldots\ldots\ldots + a_1 b_{k-1} + a_0 b_k$

Observamos que: $C_k \in (S.T)$

Observación:

1. $C_{n+m} = a_n b_m$
2. $C_{n+m+1} = 0$; puesto que

   $C_{n+m+1} = a_i b_j$ donde: $i + j = n+m+1$

   $= (n+1) + m$

   $= n + (m+1)$

   a) $C_{n+m+1} = a_{n+1} b_m = 0 b_m = 0$

   b) $C_{n+m+1} = a_n b_{m+1} = a_n 0 = 0$
3. $S.T \in N(A)$ el producto de dos sucesiones casi nulas es otra sucesión casi nula

Ejemplo1:

Sea A = Z el anillo de los números enteros y

S= (2, 3, 4, 0, 0,0,………)

T= (0, 5, 0,-2,0 0, 0,0…….)

S.T =(c_0,c_1, c_2, c_3,c_4,C_5, C_6,0,0,0,……)

Siendo:

S=(2, 3, 4, 0, 0,0…..)⇒ {a_0=2,a_1 =3, a_2 =-4,a_3 =0…………….

T=(0, 5, 0,-2,0 0, 0,0,0…..)⇒ {b_0=0,b_1 =5, b_2 =0 ,b_3 =-2……

Hallemos los valores de C_k donde: K = 0, 1, 2, 3, 4, 5, .. ¿A que será igual C_6?¿C_7? en efecto:

$c_0=a_0b_0=2(0) =0$

$c_1=a_1b_0 + a_0b_1=3(0)+2(5)=10$

$c_2=a_2b_0 + a_1b_1 + a_0b_2= 4(0) +3(5) +2(0) = 15$

$c_3=a_3 b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3 = 0(0) +4(5) +3(0) +2(-2) =16$

$c_4=a_4 b_0 + a_3 b_1 + a_2 b_2 + a_1 b_3 + a_0 b_4=0(0)+0(5)+4(0)+3(-2) +2(0)= -16$

$c_5=a_5 b_0 + a_4 b_1 + a_3 b_2 + a_2 b_3 + a_1 b_4+ a_0 b_5=0(0)+0(5)+0(0)+4(-2) +3(0)+ 2(0)= -8$

$c_6= a_6b_0 + a_5b_1 + a_4b_2 + a_3b_3 + a_2b_4+ a_1b_5+ a_0b_6=0(0)+0(5)+0(0)+0(-2) +4(0)+ 3(0)+ 0(0)= 0$

$c_7=0$

$c_8=0$

…………………………

Entonces el producto de S.T = (c_0, c_1, c_2, c_3, c_4, c_5, c_6…….) es

S.T = (0, 10, 15, 16,-6,-8, 0, 0,0……) ∊ N(Z)

Ejemplo 2:

Considerando A = Q el anillo de los números racionales se define:

T = (-1,6,3,0,0,0………)→m=2

$R = (2,1/2,1/3,0,0,0\ldots.) \rightarrow m=2$

$\Rightarrow m + n=4$

Siendo:

$t=(-1,6,3,0,0,0\ldots\ldots\ldots)$ y $r=(2,1/2,1/3,0,0,0,\ldots\ldots.)$ hallamos el producto t. r

$t.r = (c_0, c_1, c_2, c_3, c_4,0,0,0\ldots\ldots)$

Entonces hallamos los valores de C_k, K=0,1, 2, 3,4, en efecto

$c_0=a_0\, b_0=-1(2)=-2$

$c_1=a_1\, b_0 + a_0\, b_1=6(2)+(-1)(1/2)=23/2$

$c_2=a_2\, b_0 + a_1\, b_1 + a_0\, b_2=3(2) +6(1/2) +(-1)(1/3)=26/3$

$c_3=a_3\, b_0 + a_2\, b_1 + a_1\, b_2 + a_0\, b_3 = 0(2)+3(1/2)+6(1/3)+(-1)(0)=7/2$

$c_4=a_4\, b_0 + a_3\, b_1 + a_2\, b_2 + a_1\, b_3 + a_0\, b_4=0(2)+0(1/2)+3(1/3)+6(0) +(-1)(0)=1$

$c_5=0$

$c_6=0$

Luego: $T.R = (-2,23/2,26/3,7/2, 1, 0, 0,0\ldots.)$

Ejercicio 3:

De manera similar, Considerando A=Z el anillo de los números enteros se define

$R = (5, 6, 7, 0, 0,0\ldots\ldots\ldots)$

$M = (2, 3, 4, 5, 0, 0,0\ldots.)$

Hallar el producto R.M ejercicio!

2.4. Anillos de sucesiones casi nulas

Sea (A,+, ●) un anillo, afirmamos que el conjunto de todas las sucesiones casi nulas definidas sobre A, dotadas de las dos operaciones de adición y multiplicación de sucesiones casi nulas, es un anillo, es decir: (N(A),+, ●) es un anillo

Esto significa que:

I) (N(A),+) es un grupo Abeliano

a. cerradura o clausura:

$\forall$ s $\in$ N(A);$\forall$ t $\in$ N(A)$\rightarrow$ s + t $\in$ N(A)

b. conmutativa:

$\forall$ s $\in$ N(A);$\forall$ t $\in$ N(A)$\rightarrow$ s + t= t + s

c. asociativa:

$\forall$ s, t, r $\in$N(A) (s + t)+r=s+(t+r)

d. elemento neutro:

Existe la sucesión nula θ=(0,0,0,…) $\in$ N(A)/ $\forall$ s $\in$ N(A)$\rightarrow$ s + θ=θ + s=s

e. elemento opuesto:

$\forall$ s $\in$ N(A); existe –s $\in$ N(A)/s +(-s)=θ

Donde si:

S=(a_0, a_1, a_2. . . , a_n,……,0,0,0,0,0…..)

-S=($-a_0$, $-a_1$, $-a_2$. . . , $-a_n$,……,0,0,0,0,0…..)

II) (N(A),●) satisface:

a) Clausura o cerradura:

$\forall$ s $\in$ N(A); $\forall$ t $\in$ N(A)$\rightarrow$ s.t $\in$ N(A)

b) Asociativa:

$\forall$ s, t, r $\in$ N (A) $\rightarrow$ (s.t).r =s.(t.r)

III) Propiedad distributiva de ● respecto de +:

$\forall$ S, T, R $\in$ N(A) $\rightarrow$ S.(T+R) = S.T + S.R

(T+R).S = T.S + R.S

Prueba:

Se desea probar la conmutatividad

s+t = t+s, ∀s,t en N(A)

Si: $s \in N(A) \rightarrow s=(a_0, a_1, a_2. . . , a_n,\ldots\ldots,0,0,0,0,0\ldots..)$

$t \in N(A) \rightarrow t=(b_0, b_1, b_2. . . , b_n,b_{n+1}\ldots\ldots b_m,0,0,0,0,0\ldots..)$

Con n<m

$s+t= (a_0+b_0, a_1+ b_1,. . . , a_n+b_n,\ldots\ldots,0+b_m,0,0,0\ldots)$

$=(b_0+a_0, b_1+ a_1,. . . , b_n+a_n,\ldots\ldots,b_m+0,0,0\ldots)$

$=(b_0, b_1,b_2,. . . , b_n,\ldots\ldots,+b_m,0,0\ldots)+(a_0,a_1,a_2,a_3\ldots . . , a_n,\ldots\ldots,a_m,0,0\ldots)$

$=t+s$

Análogamente se cumple cuando n=m o m<n

Probemos que la multiplicación es asociativa:

Si $S =(a_0,a_1,a_2,\ldots . . , a_n,0,0\ldots)$ y $T =(b_0, b_1,b_2,\ldots , b_m,\ldots 0,0\ldots)$ y $r=(d_0, d_1,\ldots, b_l,0,0\ldots)$

Tenemos:

$$S.T =(c_0, c_1, \ldots, c_{m+n},0,0\ldots) \text{ con } c_K= \sum_{i+j=k} a_i b_j$$

$$T.R = (c_0, c_1, \ldots, c_{m+1},\ldots) \text{ con } c_{k1}= \sum_{j+u=k1} b_j d_u$$

Por lo tanto:

$S. (T.R)= (p_0,p_1,\ldots .p_{n+(m+1)},0,\ldots .)$

Con $P_k = \sum_{i+k1=k} a_i c_{k1} = \sum_{i+k1=k} a_i \left(\sum_{j+u=k1} b_j d_u \right) = \sum_{i+j+u=k} a_i (b_j d_u)$

Análogamente:

(S.T).R = (p0, p1,….$p_{(m+1)+1}$,0,….)

Con $P_K = \sum_{i+u=k} c_i d_u = \sum_{i+u=k} \left(\sum_{i+j=k} a_i b_j \right) d_u = \sum_{i+j+u=k} a_i (b_j d_u)$

En consecuencia:

S. (T.R)= (S.T).R

Además siendo A un anillo, se usó el hecho que

$(a_i.b_j).d_u = a_i.(b_j . d_u)\ \forall\ a_i, b_j, d_u$ en el anillo A

Prueba de la propiedad distributiva:

Sean:

S =(a_0, a_1, a_2. . . , a_n,……,0,0,0,…..)

T =(b_0, b_1, b_2. . . , b_m……b_m,0,0,0,…..)

R = (c_0, c_1, c_2…, c_p,0,0,0…)

si: m < p

T + R =(b_0+c_0, b_1+c_1,. . . , b_m+c_{m+1},……,c_p+0,0,…)

S.(T+R) = (d_0, d_1,d_2…, b_{n+p},0,0,0…)

Donde:

$d_0=a_0(b_0+c_0)= a_0 b_0 + a_0 c_0$

$d_1=a_1(b_0+c_0)+ a_0(b_1+c_1) =a_0b_1+ a_0c_1+ a_1b_0+ a_0c_1= a_0b_1+ a_1b_0+ a_0c_1+ a_1c_0$

$d_2=a_2(b_0+c_0)+ a_1(b_1+c_1) +a_0(b_1+c_2) =a_2b_0+ a_2c_0+ a_1b_1+ a_1c_1+ a_0b_2+ a_0c_2= a_2b_0 + a_1b_1 + a_0b_2 + a_2c_0 + a_1c_1 + a_0c_2$

………   ………

En general:

Con $d_K = \sum_{i+j=k} a_i(b_j + c_j) = \sum_{i+j=k} a_i.b_j + \sum_{i+j=k} a_i c_j$

S.(T+R) = S.T +S.R

Observación:

1) Todas las demostraciones son consecuencia inmediata de la definición de anillo
2) si(A,+,●) es un anillo conmutativo, entonces (N(A),+,●) es un anillo conmutativo

2.5. Anillo de polinomios

Al anillo (N(A),+,●) se le llama anillo de polinomios con coeficientes en el anillo (A,+,●) de una variable **a** y sus elementos de N(A) se llaman polinomios.

Es decir, si P∈N(A) entonces **una sucesión casi nula será un polinomio sobre el anillo A**.

Los polinomios serán simplemente elementos de ciertos anillos y lo que interesa será las propiedades algebraicas de ese anillo es decir:

Sea (A,+, ●) un anillo. Llamaremos anillos de polinomio sobre A en la indeterminada **x**, y le representaremos por A[X] al conjunto de todos los símbolos $a_0 + a_1x^1 + a_2X^2 + \ldots + a_nx^n$, donde, "n" puede ser cualquier entero no negativo y donde los coeficientes $a_0, a_1, a_2, \ldots\ldots a_n$, está en el anillo A.

Se dice que P es un polinomio sobre un anillo A, si y solo si existen $a_0, a_1, a_2, \ldots..,$ a_n en A , tal que $p=(a_0, a_1, a_2. . . , a_n, 0,0,0\ldots.)$ es una sucesión casi nula.

Si P∈N(A) los elementos $a_0, a_1, a_2. . . , a_n$ se llaman coeficientes del polinomio P

Notación:

sea S= N(A) el anillo de polinomio sobre A

$p \in S \Leftrightarrow p=(a_0, a_1, a_2, . . . , a_n, 0,0,0….)$

$p=(a_0,0,0,0,0…)+(0, a_1,0,0,0…)+ (0,0,a_2,0,0…)+…. + (0,0,0,0……a_n,….)$

$p=a_0(1,0,0,0,….)+ a_1(0,1,0,0,0…)+a_2(0,0,1,0,0,0..)+….+a_n(0,0,0……1)$

$p=a_0 + a_1x^1 +a_2x^2 +………..a_nx^n$

Por convenio los polinomios se le denotan:

$p=a_0 + a_1x^1 +a_2x^2 +………..a_nx^n$

Ejemplos de polinomios:

1) si $\theta=(0,0,0,0…….)$ en S=N(Z)

Θ se llama polinomio nulo sobre Z

2) Dado A=Z y S= N(Z)

$P_1 \in S \Rightarrow P_1 =(1,0,0,0,0,0,0,0………)$

$P_2 \in S \Rightarrow P_2 =(0,12,3,6,0,0,0,0,0………)$

$P_3 \in S \Rightarrow P_3 =(-2,4,1,4,,0,5,0,0………)$

P_3 Tiene como coeficiente a los números enteros:-2, 4, 1, 4, 0,5

2.5.1 Grado de un polinomio

Sea $p \in N(A)$ un polinomio no nulo $p= (a_0, a_1, a_2, . . ., a_n, 0, 0,0) \neq \emptyset$ entonces existe $a_i \neq 0$ para algún $n \in N$ (n finito). Al mayor número entero $n \geq 0$ se llama el grado del polinomio P y denotaremos Grad(p)=n

Ejemplo:

1) Sea A=Z (el anillo de los enteros) y dados P,Q,S en el anillo,

P =(1,0,5,0,0,0,0,0………)

Q = (1, 3, 0,-5, 9, 0, 0,0………)

S= (8, 0, 0, 0,0,………)

Tenemos:

Para P: Existen n=2 el mayor entero positivo tal que $a_2=5,a_2\neq 0$, entonces

Grad(P)=2

Para Q: Existen n=4, tal que $a_4=9\neq 0$, entonces: Grad(Q)=4

Para S: Existen n=0 en Z, tal que $a_0=8\neq 0$, entonces: Grad(S)=0

Ejemplo:

2) Dado A=Q (el anillo de los Racionales) y sean las sucesiones:

R =(9,8/7,0,0,0,…)

S =(1/2,0,1,0,1/3,0,0,0……)

T = (7, 0,0…) en dicho anillo; entonces:

Observamos que: Grad(R)=1, Grad(S)=4, Grad(T)=0

Nota:

1. Todo polinomio de la forma P=(a_1,0,0,0…) con $a_1\neq 0$ se llama un polinomio de grado cero

Así, son polinomios de grado cero

P_1 = (13, 0, 0, 0,0…) en N(Z) o N(Q)

P_2 = (1/9, 0, 0,0……) en N(Q)

P_3 = (-4, 0, 0,0…) en N(Z) o en N(Q)

2. El grado del polinomio nulo no se define

   Θ= (0, 0, 0, 0, 0,0……)

Definición:

Sea A[X]= el anillo de polinomio en x con coeficiente en A, Es conveniente denotar los elementos de A[X] con la notación p(x) ó a(x),…

$p(x)= a_0 + a_1x^1 + a_2x^2 + \ldots\ldots\ldots\ldots a_nx^n$

Un polinomio p(X) ∈ A[X] tiene grado cero si y solo si p(x)=a∈A, Los polinomios de grado 0 como el polinomio nulo constituyen los llamados polinomios constantes.

Así: Los polinomios considerados en la nota anterior son polinomio constante

Los polinomios de grado 1 tiene la expresión general ax +b, a, b ∈A, a≠0

Los polinomios de grado 2 tiene la expresión general ax^2+bx+c con a, b, c en A

Observación:

Sean s,p en N(A), donde:

$s=(a_0, a_1, a_2, \ldots, a_m, 0,0,0\ldots)$ de grado m

$p=(b_0, b_1, b_2, \ldots, b_m, 0,0,0\ldots)$ de grado n

Considerando n≥m

Grado de (s.p):

$$s.p=(a_0b_0, a_1b_1+ a_0b_1, \ldots, c_k \neq \sum_{i+j=k} a_ib_j , \ldots. c_{m+n}, 0, \ldots)$$

Pero puede ocurrir que: $c_{m+n}=a_m b_n=0$, entonces

- grad(s.p)≤m+n
- grad(s.p)=m+n. Cuando A es un dominio de integridad, es decir: si $a_mb_n\neq 0$

Ejemplo:

En el anillo de los polinomios P=N(Z), considere

s=(1,3,0,5,0,0,…)

$p=(-7,6,0,-4,0,0,\ldots)$

$q=(5,1,3,0,-2,0,0\ldots)$

Tenemos: Grados(s)=3, aquí m=3

Grados (p)=3, aquí n=3

Grados (q)=4, aquí r=4

a) $s+p=(-6,9,0,1,0\ldots)$

Como $m=n=3 \Rightarrow grad(s+p)=1 \leq 3$

b) $p+q=(-1,1,3,-4,-2,0,0,0,\ldots)$

$r>m \Rightarrow grad\ (p+q)= \max\ \{4,3\}=4$

Notación:

1) Si **N**(A) es el anillo de los polinomios con coeficientes en un anillo A, en adelante a este anillo lo denotaremos con A[x], es decir: N(A)=A[x]
2) Denotamos con P_0 al conjunto de los polinomios sobre A de la forma (a,0,0,0,0,0) para cada $a \in A$

Observación:

Si A=Z es el anillo de los números enteros, entonces afirmamos que

$Z \subset Z\ [X]$

Este hecho nos permite afirmar que todo número entero **a**, puede considerarse como un polinomio de la forma (a, 0, 0,0,….). Luego podemos hacer la siguiente identificación: a=(a, 0, 0, 0,0,….)

Consideraciones básicas

Si definimos la función f de A en P_0, todo elemento **a** del anillo A, se puede escribir: **a**=(a, 0, 0,0….)

Si llamamos 1 al polinomios 1= (1, 0, 0,0…..) y polinomio

X= (0, 1, 0, 0,0,….)

Entonces se deduce que:

X^2= (0, 0, 1, 0, 0,0….)

X^3= (0, 0, 0, 1, 0, 0,0….)

X^4= (0, 0, 0, 0, 1, 0, 0,0,….)

……………………………………..

X^n= (0, 0,0,…., 0, 1, 0,0….) (n ceros antes del 1)

Dados un polinomio P en el anillo de polinomios A[x], siendo

P=(a_0, a_1, a_2. . . , a_n,……,0,0,0,…..)

Teniendo en cuenta las consideraciones anteriores, se deduce que el polinomio P tiene la siguiente forma.

$P= a_0+a_1x+a_2x^2+a_3x^3+\ldots+a_nx^n$

Por convenio:

Al polinomio P en adelante se escribirá como $P(x)= a_0+a_1x+a_2x^2+a_3x^3+\ldots+a_nx^n$

Además:

Se afirma que P(x) es un polinomio en la indeterminada x. donde

grad(P)= grad(P(x))=n para $a_n \neq 0$

Ejemplo:

Dado el anillo de los enteros Z y sea Z[x] el anillo de los polinomios con coeficiente en Z, sean los polinomios P, Q y S en Z[x] donde:

P= (2,-9, 3, 0, 0,0……)

Q= (1, 8, 0, 9, 7, 0, 0,0…..)

S= (10,-1,5,-1,1,-1,0,0,0….)

En base a lo estudiado anteriormente, estos polinomios los representaremos como sigue:

$P= 2-9x+3x^2$

P es un polinomio de grado 2 y por convenio se acostumbra a escribir:

$P(x)=3x^2-9x+2$

$Q=1+8x +9x^3+7x^4$

$Q(x)= 7x^4+9x^3+0x^2+8x +1$

$S=10-x+5x^2-x^3+x^4-x^5$

$S(x)=- x^5+ x^4- x^3+5x^2- x+10$

Sumandos estos polinomios se deducen:

$P(x) + Q(x)=3-1x+3x^2+ 9x^3 +7x^4$

$Q(x)+S(x)= 11+7x+5x^2+8x^3+8x^4-x^5$

Ejemplo de suma y producto de polinomios

Ejemplo 1:

En anillo de los polinomios Z(x) sean:

$P(x)=8+2x-6x^2$; $Q(x)=4+2x^2$

Suma: $P(x) + Q(x)=(8+2x-6x^2) +(4+0x+2x^2)$

$=(8+4)+(2+0)x+(-6+2)x^2$

$=12+ 2x -4x^2$

Ejemplo 2:

Sea el anillo de los polinomios de los números enteros Z[X]

$P(x)= - 3x^4 + 2x^3 – x^2 + 2 x +0$

$Q(x) = 5x^4 + 3x^3 + 7x^2+ 2 x +1$

suma: P(x)+Q(x)

$=(-3x^4 + 2x^3 – x^2 + 2 x +0) +(5x^4 + 3x^3 + 7x^2+ 2 x +1)$

$=(-3+5)x^4 + (2+3)x^3 +(-1+7)x^2+(2+2)x +(0+1)$

$=2 x^4+5 x^3+6 x^2+4x+1$

Producto:

$S(x)P(x)=(3+2x^2)(0+4x+3x^2+ 3x^3)$

$S(x)P(x)=(3)(0)+ [(3)(4)+(0)(0)]x+ [(3)(3)+(0)(2)+(0)(1)^2]x^2 + [(3)(2)+(0)(-3) +$

$(2)(4) + (0)(0)]x^3 + [(3)(0)+(0)(2)+(2)(-3) +(0)(4)+(0)(0)] x^4+[(3)(0) +(0)(0)$

$+(2)(2) +(0)(-3) +(0)(4) +(0)(0)]x^5$

$S(x).P(x)=0 +12x -9x^2+14x^3-6x^4+4x^5$

Ejemplo 1:

$P (x)= 4x^3 - 5x^2 + 2x + 1$

$Q (x)= 3x – 6$

Se resuelve análogamente:

$P(x).Q(x) =$ $\mathbf{12x^4 - 39x^3 + 36x^2 - 9x - 6}$

2.5.2 Raíces de polinomio

Definición: sea $p(x)= a_0 + a_1x^1 + a_2x^2 + \ldots\ldots\ldots\ldots a_nx^n$ un polinomio en A[X] se llama el valor numérico del polinomio p(x) en β∈A, al número:

$a_0 + a_1\beta^1 + a_2\beta^2 + \ldots\ldots\ldots\ldots a_n\beta^n$.

El valor numérico del polinomio es el resultado que obtenemos al sustituir la variable **x** por un número cualquiera.

Ejemplos 1:

1.- P(x) es un polinomio Z[x], Donde $P(x)= 2+3x+x^2$

El valor numérico del polinomio en P en β=3 en Z es:

$P(3)=2+3(3)+(3)^2$

P(3)=20 por lo que 20 es el valor numérico de p(x) cuando x=3

Ejemplo 2:

El valor numérico del polinomio P en 0, en Z

$P(0)=2+3(0)+0^2$

P(0)=2

Ejemplo 3:

El valor numérico del polinomio P en 1, en Z

$P(x) = 2x^3 + 5x - 3; \qquad x = 1$

$P(1) = 2 \cdot 1^3 + 5 \cdot 1 - 3$

$P(1) = 2 + 5 - 3$

$P(1) = 4$

Observación:

Sea(A,+,●) es un anillo

Para P(x) y Q(x) en A[x], se cumple

a) Si P(x)=Q(x),entonces para x=a, es p(a)=Q(a)

b) Decir que P(x)=Q(x)significa que los polinomios P(x) y Q(x) tiene igual grado y los mismo coeficientes

Raíz de un polinomio

Definición: un elemento de β de A es una raíz o cero de un polinomio P(x) si y solo si: P(β)=0.

SI P(β) ≠0, entonces diremos que β de A no es raíz de polinomio p(x)

Ejemplo 1:

$P(x)=30+4x-2x^2$ en Z[x]

β=5∈Z es raíz de p(x) porque:

$P(x)=P(5)=30+4(5)-5(3)^2=0$

P(5)=0

Sin embargo para β=0; $p\ (0)= 30+4(0)-5(0)^2$

p (0)=30

Entonces β=0 no es raíz de p(x)

Ejemplo 2:

Calcular las raíces de los polinomios

$$P(x) = x^2 - 5x + 6$$

Para $x = 2$ y $x = 3 \in Z$ (el conjunto de los números enteros) remplazamos:

$P(2) = (2)^2 - 5 \cdot (2) + 6$

$P(2) = 4 - 10 + 6 = 0$

$P(3) = (3)^2 - 5 \cdot (3) + 6$

$P(3) = 9 - 15 + 6 = 0$

Entonces $x = 2$ y $x = 3$ son raíces o ceros del polinomio:

$P(x) = x^2 - 5x + 6$, porque $P(2) = 0$ y $P(3) = 0$.

Teorema 1:

Si p(x) es un polinomio en A[X]. y $\beta \in A$, entonces existe un polinomio s(x) en A[x], tal que $P(x)-Q(\beta)=(X-\beta)S(X)$

Corolario 1:

Sea P(x) un polinomio A[x] donde para β en A, existe s(x) en A[x] tal que $p(x)=(x-\beta)\, s(x)$, entonces β es raíz de P(x): Es decir: $\beta \in A$ es una raíz del polinomio P(x), si y solo si $(x-\beta)$ divide exactamente a P(x)

Corolario 2:

Si $\beta_1, \beta_2, \beta_3, \ldots, \beta_n$ son m elementos distintos del anillo A que son raíces del polinomio P(x) es decir $P(\beta_1)= P(\beta_2)=\ldots P(\beta_m)=0$ entonces existe un polinomio $s(x) \in A[x]$ tal que :

$P(x)=(x- \beta_1)(x- \beta_2)(x- \beta_3),\ldots(x- \beta_m)\, s(x)$

Corolario 3:

Si p(x) es un polinomio de grado n en A[x], entonces no puede existir n+1 elementos diferentes: $\beta_1, \beta_2, \beta_3, \ldots, \beta_n, \beta_{n+1}$ de A tal que:

$P(\beta_1)= P(\beta_2)=\ldots.P(\beta_n)= P(\beta_{n+1})=0$

Por el corolario 2, existe un polinomio $s(x)\in A[x]$ tal que :

$P(x)= (x- \beta_1)(x- \beta_2)(x- \beta_3),\ldots.(x- \beta_n)\ (x- \beta_{n+1})\ s(x)$

En cuyo caso:

Grado de $P(x)\geq n+1>n$, el cual contradice la hipótesis, si $s(x)\neq 0$

Si $s(x)=0$ entonces resultaría:

$P(x)= (x- \beta_1)(x- \beta_2)(x- \beta_3),\ldots.(x- \beta_n)\ (x- \beta_{n+1}) = 0$

$P(x)=0$

Se contradice con el grado de $P=n\neq 0$

Observaciones

Sea p(x) un polinomio en A[x]

El corolario 3 nos demuestra que un polinomio $P(x)\neq 0$ de grado n tiene a lo más n raíces .

Si $\beta_1, \beta_2, \beta_3, \ldots, \beta_n$ son raíces del polinomio P(x), entonces estos se descomponen en los factores: $P(x)= (x- \beta_1)(x- \beta_2)(x- \beta_3),\ldots.(x- \beta_n)\ (x- \beta_{n+1})\ s(x)$

Recíprocamente, si vale esta descomposición entonces $\beta_1, \beta_2, \beta_3, \ldots, \beta_n$ son raíces del polinomio P(x)

De estas observaciones se infiere que la teoría de ecuaciones o sea el problema de la determinación de las raíces de P(x), está vinculada a la teoría de divisibilidad de polinomio

2.5.3 Divisibilidad de un polinomio

Sea p(x) y Q(x) dos polinomios en el anillo A[x]

Definición: diremos que Q(x) $\neq 0$ es divisor de P(x) y escribimos Q(x)/P(x), si existe un polinomio S(x) en A[x] tal que: P(x)=Q(x) S(x)

En consecuencia, se debe cumplir: Q(x)/P(x) $\leftrightarrow$P(x) =Q(x) S(x)

Ejemplo1:

En el anillo Z[x] sean P(x)=x^2-3x+2 ; Q(x)=x-1

Tenemos:

Q(x)/P(x), Es decir

Q(x) = x-1, es divisor de P(x)=x^2-3x+2 pues, existe

S(x)=x-2 en Z[x] tal que P(x)=Q(x) s(x)

P(x)=(x-1).s(x) con s(x)=x-2

P(x) =(x-1)(x-2)

P(x) =x^2 -3x + 2 = (x-1)(x+2)

Ejemplo2:

En Z(x) sean p(x)= x^5+5x^3+2 x^2+10 Q(x)=x^3+2

Tenemos:

Q(x)=x^3+2, es divisor de p(x)= x^5+5x^3+2 x^2+10 pues, existe s(x)=x^2+5 en Z[x]

P(x)=Q(x)s(x)

P(x)=(x^3+2)s(x), con s(x)= x^2+5

P(x)=(x^3+2)(x^2+5)

p(x)= x^5+5x^3+2 x^2+10

Teorema:(Algoritmo de la división de los polinomios)

Sean P(x) y Q(x) dos polinomios en A [X], y Q(X) ≠0, entonces existen dos polinomios únicos C(x) y R(x) en A [X] tal que cumplen las siguientes propiedades:

1. P(x)=Q(x)C(x) + R(x) es decir R(x)=P(x)-Q(x).C(x)
2. R(x)=0 o bien grad(R(x))<grad(Q(x))

El polinomio C(x) se denomina cociente de dividir el polinomio P(x) por Q(x)

El polinomio R(x) se denomina resto de dividir el polinomio P(x) por Q(x)

La demostración tiene dos partes: existencia y unicidad

Demostración (existencia)

Sean $P(x)= a_0 + a_1x^1 +a_2x^2 +\ldots\ldots\ldots a_nx^n$

$Q(x)= b_0 + b_1x^1 +b_2x^2 +\ldots\ldots\ldots b_mx^m$; $b_m\neq 0$

Analicemos los siguientes casos:

1) P(x)=0, el resultado es inmediato
2) Si Grad P(x)< Grad Q(x) (n<m)

   Es suficiente tomar c(x)=0 y resulta

   P(x)= 0; Q(x) + P(x)

   Grad(P(x))= Grad(R(x))= n<m= Grad(Q(x))

   Grad(R(x))< Grad(Q(x))

3) Si Grad(P(x))= Grad(Q(x),n=m)

   Debe exitir c(x) y R(x) tal que

   P(x)=c(x)Q(x)+R(x)……………………………(α)

   En este caso será suficiente considerar el polinomio constante

   $c(x)= a_n b_n^{-1}$(m=n, $b_n\neq 0$), que satisface (α) es decir:

$P(x)= a_n\, b_n^{-1}(b_0 + b_1x^1 +\ldots\ldots+b_nx^n)+R(x)$

$a_0 + a_1x^1 +a_2x^2 +\ldots\ldots\ldots\ldots a_nx^n= a_n\, b_n^{-1}\, b_0+ a_n\, b_n^{-1}\, b_1x + a_n\, x^n+R(x)$

$R(x)= a_0 + a_1x^1 +a_2x^2 +\ldots\ldots+a_{n-1}x^{n-1}-(a_n\, b_n^{-1}\, b_0+ a_n\, b_n^{-1}\, b_1x +\ldots.+ a_n\, b_n^{-1}\, x^{n-1})$

Grad $R(x)\leq n-1\leq n=$Grad

Grad $R(x)<$Grad $Q(x)$

4) Si Grad$(P(x))>$Grad$(Q(x))(n>m)$

Sea $P_1(x)=P(x)- a_n\, b_m^{-n-m}(b_0 + b_1x^1 +\ldots\ldots+b_mx^m)$

$P_1(x)=P(x)- a_n\, b_m^{-1}\, x^{n-m}\, Q(x)$

$P_1(x)= a_0 + a_1x^1 +a_2x^2 +\ldots\ldots+a_nx^n- a_n\, b_n^{-1}\, x^{n-m}\, (b_0 + b_1x^1 +\ldots+b_mx^m)$

Grad$P_1(x)\leq n-1<n$

Razonando de acuerdo a un principio de inducción matemática para $P_1(x)$:

Existen $c_1(x)$ y $R_1(x)$ tal que:

$R_1(x)=P_1(x)-c_1(x)Q(x)$ tal que

$P_1(x)=c_1(x)Q(x)+R_1(x)$…………………………………(β)

Y Grad $R_1(x)<$ Grad$Q(X)$

De (α) y (β) se tiene :

$P(x)=a_n\, b_m\, x^{n-m}=c_1(x)Q(x)+R_1(x)$

$P(x)=a_n\, b_m\, x^{n-m}Q(x)+ c_1(x)\, Q(x)+ R_1(x)$

Llamando:

$c(x)= a_n\, b_m\, x^{n-m}Q(x)+ c_1(x)$ y $R_1(x)= R(x)$

Resulta

$P(x)= C(x)Q(x)+ R(x)$

$R(x)= P(x)- C(x)Q(x)$

Además grad$(R(x))<$grad$(Q(x))$

Unicidad

$c(x)$ y $R(x)$ son únicos

En efectos:

Supongamos que además existen $c'(x)$ y $R'(x)$ tal que

$P(x)= c'(x)\ Q(x) + R(x)$

$P(x)= c(x)\ Q(x) + R(x)$

Igualando:

$R(x)-R'(x)=(c(x)-c'(x))Q(x)$

Si $c(x)- c'(x)=0 \rightarrow c(x)=c'(x)$

Si $c(x)- c'(x)\neq 0$

Por cuestiones de grado tendríamos

$Grad(R(x)-R'(x))=Grad(c(x)-c'(x))+Grad\ Q(x)$

$R>0$

$Max(Grad(R(x)),Grad(R'(x)))$

$Grad(Q(x))\leq KGrad(R(x))$

$Grad(Q(x))\leq Grad(R(x))(\rightarrow\leftarrow)$

Contradicción con $grad(R(x))<Grad(Q(x))$

Entonces debemos aceptar que: $C(x)-C'(x)=0\rightarrow c(x)=C'(x)$

Por lo tanto

$R(x)-R'(x)=0\rightarrow R'(x)= R(x)$

Ejemplo 1:

En el anillo Z[X] Sean en cada caso

$P(x)=x^{4}-5x^{3}+11x^{2}-12x+6$ sea

$Q(x)= x^{2}-3x+3$

Existe $R(x) = P(x)-Q(x)C(x)$

$R(x)= x^4-5x^3+11x^2-12x+6 - (x^2-3x+3)C(x)$ siendo $C(x)=x^2-2x+2$

$R(x)= (x^4-5x^3+11x^2-12x+6)-(x^2-3x+3)(x^2-2x+2)$

$R(x)=0$

Ademas: $Grad(R(x))=0<Grad\ Q(x)=2$

$\rightarrow Grad\ (R(x))< Grad\ (Q(x))$

El algoritmo de la división se representa usualmente como:

$$\begin{array}{l|l} P(x) & Q(x) \\ \cline{2-2} R(x) & C(x) \end{array}$$

Dónde: $P(x)=Q(x).C(x) + R(x)$

$C(x)$= el cociente de dividir $P(x)$ entre el polinomio $Q(x)$, $Q(x)\neq 0$ y $R(x)$ es el resto

Ejemplo1:

En el anillo $Z[x]$ sean los polinomios:

$P(x)= X^4-2x^3 -11x^2+30x-20$ y $Q(x)= x^2+3x-2$Hallar el $C(x)$ y $R(x)$ únicos tales que $P(x)=Q(x)C(x) +R(x)$

Solución:

Usando el esquema anterior, tenemos:

$$\begin{array}{l|l} X^4-2x^3 -11x^2+30x-20 & x^2+3x-2 \\ \cline{2-2} \underline{-x^4-3x^3+2x^2} & x^2-5x+6 \longrightarrow C(x) \\ 0-5x^3-9x^2+30x & \\ \underline{-5x^3+15x^2-10x} & \\ 0+6x^2+20x-20 & \end{array}$$

$-6x^2-18x+12$

$2x - 8 \longrightarrow R(x)$

Luego $C(x)= x^2-5x+6$ y $R(x)= 2x - 8$

Se puede comprobar que $R(x)=P(x)-Q(x)C(x)$ Además vemos que:

$grad(R(x))<grad(Q(x))$

Ejemplo2:

En el anillo Z[x] sean los polinomios:

$P(x)= 6X^5+ X^4+0x^3 +4x^2 -7x+1$ y $Q(x)= 2x^2+x-3$ Hallar el C(x) y R(x) únicos tales que:

$P(x)=Q(x)C(x) +R(x)$

Solución:

Usando el esquema anterior, tenemos:

$6X^5+ X^4+0x^3 +4x^2 -7x+1 \,\lfloor\, 2x^2+x-3$

$-6X^5-3X^4+9x^3$ $\qquad 3x^3 -x^2 +5x-2$

$0- 2X^4+9x^3 +4x^2$

$+2X^4+x^3 -3x^2$

$0+10x^3 +x^2 -7x$

$-10x^3 -5x^2 +15x$

$-4x^2 +8x+1$

$4x^2 +2x-6$

$0 +10x-5 \longrightarrow R(x)$

Luego $C(x)= 3x^3 -x^2 +5x-2$ y $R(x)= 10x-5$

Se puede comprobar que R(x)=P(x)-Q(x)C(x) Además vemos que : grad(R(x))<grad(Q(x))

Polinomios asociados:

Definición.-

Los polinomios son tales que uno de ellos es igual al otro, multiplicado por una constante cualquiera no nula, y estos se llaman polinomios asociados.

Es decir,

P(x) y Q(x) son asociados P(x)=KQ(x) v Q(x)=KP(x)

Siendo K una constante de A

Ejemplo 1:

En el anillo Z[x] sean: P(x)= x^3-7x-2, Q(x)=5x^3-35x-10 entonces, P(x) y Q(x) son asociados pues, Q(x)=5P(x)

2.5.4 Máximo común divisor de polinomios

Definición: Dados dos polinomios P(x) y Q(x) en el anillo A[x], su máximo común divisor es el Polinomio D(x) si se verifica:

1. D(x)/P(x) $\wedge$ D(x)/Q(x)
2. Si d(x)/P(x) $\wedge$ d(x)/Q(x) $\longrightarrow$ **d(x)/D(x)**

Escribimos: D(x)= MCD (P(x), Q(x))

Ejemplo:

Dados P(x)=X^5+ x^4-2x^3 Q(x)= x^5+2x^4-x^3-2x^2

Entonces existe $D(x)=(x-1)(x+2)=x^2+x-2$, es tal verifica:

(1) $D(x)/P(x)$, pues $P(x)=D(x)(x^3)$

$D(x)/Q(x)$, pues $Q(x)=D(x)(x^2)$

(2) Si $d(x)=x-1$

$d(x)/P(x)$; pues; $P(x)=d(x)(x^3+2x)$

$d(x)/Q(x)$; pues; $Q(x)=d(x)(x^3+x^2)$

Entonces: $d(x)/D(x)$; puesto que.

$D(x)=d(x)c(x)$

$X^2+x-2=(x-1)c(x)$, $c(x)=x+2$

$MCD(P(x),Q(x))=x^2+x-2$

Nota: en la parte (2), d(x) puede tomarse también como $x+2=d(x)$

Definición:

Diremos que dos polinomios P(x) y Q(x) en A[(x)] son primos entre si, si su máximo Común Divisor es igual a 1 y se denota:

P(x) p si Q(x) $\longrightarrow$ $MCD(P(x),Q(x))=1$

Ejemplo 1:

Sean P(x) y Q(x) en Z[x], donde $P(x)=x+1$, $Q(x)=x-1$ se tiene MCD (P(x), Q(x))=1, entonces P(x) y Q(x) Son primos entre si

2.5.5 Polinomio irreducible

Definición.-

Un polinomio P(x) es irreducible en el anillo A [X], si y solo si, P(x) admite por divisores a 1, y a los asociados de estos.

De manera equivalente:

Un polinomio P(x) en A[x] es irreducible sobre A, si se tiene que P[x]=S[x]T[x] donde uno de los dos, S(x) o T(x), es de grado cero.

Ejemplo 1:

Sea el anillo de polinomio Z[x] y el polinomio P(x)= X^2+1, sus divisores son x^2+1 y 1 entonces, P(x)= $X^2+ 1$ es irreducibles.

Ejemplo 2:

Sea P(x)= $X^2- 4$, en $\mathbb{Z}$ [x], sus divisores son 1,x +2 y x-2 son divisores de P(x) diferentes de 1 y sí mismo.

Capítulo III

3.1. Sesión de aprendizaje

Título: Anillo de polinomios

I. OBJETIVOS:

1.1 Objetivo general:

- Define el anillo de polinomios y un polinomio a partir de sucesiones casi nulas en un anillo.
- Realiza operaciones con polinomios

1.2 Objetivos específicos:

- Define el anillo de polinomios.
- Realiza operaciones con polinomios
- Caracteriza los polinomios de acuerdo a sus propiedades
- Resuelve problemas de aplicación.

II. ORGANIZACIÓN DE LOS APRENDIZAJES:

Conceptos	Aprendizaje(S) esperados	Actitudes

▪ Ley de Composición Interna (LCI) ▪ Estructura Algebraica ▪ Grupos y Subgrupos ▪ Anillo y Subanillo ▪ Sucesiones y sucesiones casi nulas ▪ Suma y producto de sucesiones casi nulas ▪ Grado de un polinomio ▪ Raíces de un polinomio ▪ Divisibilidad de polinomios ▪ Teorema del algoritmo de la división de polinomios ▪ Máximo Común Divisor de Polinomios	**COMUNICACIÓN MATEMÁTICA:** ▪ Expresa verbalmente una ley de composición interna y algunas estructuras algebraicas. ▪ Infiere procedimientos ▪ Evalúa conceptos y definiciones sobre Anillos ▪ Analiza las operaciones de suma y producto de sucesiones casi nulas. ▪ Define un anillo de polinomios ▪ Define un polinomio. RAZONAMIENTO Y DEMOSTRACIÓN ▪ Identifica el concepto de ley de composición interna ▪ Prueba las propiedades de los anillos RESOLUCIÓN DE PROBLEMAS ▪ Resuelve problemas de suma de sucesiones casi nulas ▪ Resuelve problemas de producto de sucesiones casi nulas. ▪ Resuelve problemas de operaciones con polinomios.	• Muestra deseos de superación personal y profesional. • Muestra rigurosidad en el manejo conceptual. • Muestra perseverancia en la solución de la guía de práctica.

III. SECUENCIA DIDÁCTICA:

Situaciaciónes de aprendizaje	Estrategias	Recursos	Evaluación			Tiempo
			Criterio	Indica dores	Instrum entos	
INICIO	• Presentación. • Exploración de saberes previos. • Define leyes de composición interna en un conjunto dado. • Define un anillo.	• Exposición oral. • Equipo multimedia. • PPT • Pizarra, plumones y mota.	C.M.			10’
PROCESO	• Define sucesiones distinguiendo las sucesiones casi nulas • Define y calcula la suma y el producto de sucesiones casi nulas. • Define un anillo de polinomios, polinomio y grado de un polinomio. • Realiza operaciones con polinomios.	• Exposición oral. • Equipo multimedia. • PPT • Pizarra, plumones y mota.	C.M. R.P.			30’
SALIDA	• Resuelve la guía práctica.	• Guía práctica.	R.M. R.P.			10’

Guía de práctica

1. Se tienen las sucesiones:

S = (-8, 2,-3,-1, 2, 0, 0,0……)

T = (-10, 3, 0, 7,-5, 0, 0,0……)

   a. Identifica el tipo de sucesiones que representan.

   b. Hallar la suma de dichas sucesiones.

2. Dadas las sucesiones R = (1, 2,-5, 4, 0, 0, 0, 0,0……)

T = (-6, 3, 0, 0, 0, 0,0…………)

   a. Calcule el producto de estas sucesiones.

   b. Identifique los coeficientes del polinomio.

3. Proponga dos sucesiones casi nulas y halle la suma y el producto, identificando los coeficientes en cada caso.

4. Halle el grado en el anillo de sucesiones casi nulas que caracteriza a los polinomios en el anillo de polinomios.

   P= (8, 1,-1, 6, 2, 0, 0,0,………....)

   Q= (0,-27, 15, 0, 0,0…………….…)

   R= (1, 4, 0, 5, 0, 0,0…………...…)

   S= (3,-7, 4, 0, 0,0……..................)

   T= (4, 0,-1, 6, 0, 0, 0,0………….…)

   U= (0, 6, 5, 0, 0, 0, 0,0…………….)

   V= (6,-9, 15, 2, 7, 5, 1, 1, 0, 0,0….)

5. Represente a los polinomios a partir de las siguientes sucesiones casi nulas

P= (4, 0, 5, 8, 9, 0, 0, 0,0,…………)

Q = (0,19,-5,7,0,9,8,0,0,0,0…..)

R=(-4,1,0,6,7,3,0,0,0,0,……….)

6. Dados los polinomios A=6x+2x-7, B=-4x+3x-5 Calcular: A+B y A.B.

7. Dividir los siguientes polinomios

a. $(x^4 - 2x^3 - 11x^2 + 30x - 20) : (x^2 + 3x - 2)$

b. $(x^6 + 5x^4 + 3x^2 - 2x) : (x^2 - x + 3)$

c. $P(x) = x^5 + 2x^3 - x - 8$ $\quad Q(x) = x^2 - 2x + 1$

8. Calcula el valor de los polinomios cuando x=3 y x=2?

a. $P(x)= x2 + 3x - 2$

b. $R(x)= 2x4 + 3x3 + 3x2 - 2x+3$

c. $Q(x) = x2 - 2x + 1$

9. Calcule los productos que se indican:

a. $(x^4 - 2x^2 + 2) \cdot (x^2 - 2x + 3)$

b. $(3x^2 - 5x) \cdot (2x^3 + 4x^2 - x + 2)$

c. $(2x^2 - 5x + 6) \cdot (3x^4 - 5x^3 - 6x^2 + 4x - 3)$

Síntesis

Para comprender la construcción del anillo de polinomios, es necesario tener los siguientes conceptos fundamentales:

1. **Semigrupo**

   Sea un conjunto $A \neq \Phi$, y "$*$" una L.C.I. definida sobre *A*. *S*i "$*$" es asociativa, decimos que $(A;*)$ es un semigrupo.

   Es decir, $(A;*)$ es un semigrupo, sii, $(x*y)*z = x*(y*z), \forall x, y, z \in A$

2. **Grupo**

   Sea $G \neq \Phi$, "$*$" una L.C.I.; decimos que el monoide $(G;*)$ tiene la estructura de grupo si y solo si, verifica los siguientes axiomas:

   G1) Asociativa $(x*y)*z = x*(y*z)$, $\forall x, y, z \in G$.

   G2) Existencia del elemento Neutro; $\exists e \in G / e*x = x*e = x$, $\forall x \in G$.

   G3) Existencia del elemento Simétrico; $\exists x' \in G$, $x'*x = x*x' = e$, $\forall x \in G$.

   Si además se cumple:

   G4) Conmutativa; $x*y = y*x$, $\forall x, y \in G$, el grupo $(G,*)$ es un grupo abeliano

3. **Anillos**

   Sea el conjunto R diferente del vacío $(R \neq \emptyset)$ y las operaciones binarias "$*$" y "Δ"; la terna $(R;\ *;\ \Delta)$ es un **anillo**, si y solo si, se verifican las siguientes condiciones:

   1°) $(R;\ *)$ es un grupo abeliano

   2°) $(R;\ \Delta)$ es un semigrupo

   3°) La segunda operación (Δ) es distributiva respecto a la primera operación $(*)$.

Por simplicidad en las notaciones consideramos las operaciones anteriores como + y . ; entonces diremos, que la terna $(R, +, \cdot)$ es un **Anillo** si y solo si, se cumplen las siguientes propiedades:

A_1 : $a + (b + c) = (a + b) + c$

Ley de Asociatividad respecto de " + "

A_2 : $a + 0 = a, \quad 0 + a = a \quad \forall\ a \in R$

Ley de la identidad respecto a " + "

A_3 : $a + (-a) = 0, \quad (-a) + a = 0$

Ley del opuesto aditivo.

A_4 : $a + b = b + a$

Ley Conmutativa respecto de " + "

A_5 : $a, b \in R \Rightarrow a \cdot b \in R$

Ley de absorción respecto a " · "

A_6 : $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

Ley de Asociatividad respecto de " · "

A_7 : $\begin{array}{l} a \cdot (b + c) = a \cdot b + a \cdot c \\ (b + c) \cdot a = b \cdot a + c \cdot a \end{array} \quad \forall\ a, b, c \in R$

Ley Distributiva de la " · " respecto a la " + "

4. Subanillos

Sea $(R, +, \cdot)$ un anillo; un subconjunto $A \subset R$ es un **subanillo** de $(R, +, \cdot)$; si $(A, +, \cdot)$ es un anillo.

Ejemplo:

Sea $(\mathbb{Z}, +, \cdot)$ el anillo de los enteros, como $2\mathbb{Z}$, $3\mathbb{Z}$, $5\mathbb{Z}$, $6\mathbb{Z}, \ldots$ están contenidos en $\mathbb{Z}$; entonces se tiene que $(2\mathbb{Z}, +, \cdot)$, $(3\mathbb{Z}, +, \cdot)$, $(5\mathbb{Z}, +, \cdot)$, …. Son subanillos de $(\mathbb{Z}, +, \cdot)$.

Observación:

Para probar que un subconjunto de un conjunto es un subanillo, es suficiente probar:

$$i)\ \forall\ a,b\ \in R\ ;\quad a-b\in R$$

$$ii)\ \forall\ a,b\ \in R\ ;\quad a\cdot b\in R$$

5. Sucesión

Una sucesión es una función cuyo dominio es el conjunto de los números naturales y cuya imagen es un anillo A.

Es decir, $S:N\to A$

$$(i)\to S(i).$$

Donde N es el conjunto de números naturales sin cero.

6. Suma de sucesiones casi nulas

Sea (A,+,●) un anillo conmutativo con unidad

Denotamos por N(A) al conjunto formado por todas las sucesiones casi nulas es decir: N(A)= {S: N→A/s es una sucesión casi nula} .

Sean S_i y S_j dos sucesiones casi nulas.

S_i ∈N (A) → S= ($a_0,a_1,a_2,a_3,.......,a_m$.,0,0,0...)

S_j ∈N (A) → S= ($b_0,b_1,b_2,b_3,.......,,b_n$,0,0,0...…..)

Definimos la suma de sucesiones casi nulas mediante:

S_i + S_j = ($a_0+b_0,a_1+b_1,.......,a_n+b_n$,..) ∈A

7. Producto de sucesiones casi nulas

Sean las sucesiones S y T,

$S = (a_0, a_1, a_2. . . , a_n,\ldots\ldots,0,0,0,0,0\ldots..)$

$T = (b_0, b_1, b_2. . . , b_n,b_{n+1}\ldots..,b_m ,0,0,0,0,0\ldots..)$, definimos el producto de dichas sucesiones como: $s.t=(c_0,c_1, c_2, c_3,\ldots\ldots,c_{r-1}, c_r,\ldots..0,0,0\ldots)$ donde:

$$c_k= \sum_{i+j=k} a_i b_j$$

8. Anillo de polinomios

Sea (A,+, ●) un anillo. Llamaremos anillo de polinomios sobre A en la indeterminada **x**, y lo representaremos por A[x] al conjunto de todos los símbolos $a_0+ a_1x^1+ a_2x^2+ \ldots+a_nx^n$, donde, "n" es cualquier entero no negativo y los coeficientes $a_0, a_1, a_2,\ldots\ldots a_n$, están en el anillo A.

Es decir, se dice que P es un polinomio sobre un anillo A, si y solo si existen a_0, a_1, $a_2,\ldots.., a_n$ en A , tal que $p =(a_0, a_1, a_2. . . , a_n,0,0,0\ldots)$ es una sucesión casi nula.

Si P∈N(A) los elementos $a_0, a_1, a_2. . . , a_n$ se llaman coeficientes del polinomio P

9. Valor numérico de un polinomio

Sea $p(x)= a_0 + a_1x^1 +a_2x^2 +\ldots\ldots\ldots..a_nx^n$ un polinomio en A[X] se llama el valor numérico del polinomio p(x) en β∈A, al número:

$a_0 + a_1\beta^1 +a_2\beta^2 +\ldots\ldots\ldots..a_n\beta^n$.

El valor del polinomio es el resultado que obtenemos al sustituir la variable **x** por un número cualquiera.

10. Raíz de un polinomio

Un elemento de β de A es una raíz o cero de polinomio P(x) si y solo si P (β)=0

Si P (β) ≠0, entonces diremos que β de A no es raíz de polinomio p(x)

Apreciación crítica y sugerencias

Apreciación crítica

El presente trabajo se realiza con el interés de aportar a la reflexión y mejoramiento de la enseñanza de los polinomios frente a las dificultades que presenta su aprendizaje desde los niveles básicos, que afectan su adecuada comprensión y su posterior aplicación.

Es muy común que los estudiantes desde el nivel primario, pasando por el nivel de educación secundaria y superior, presenten dificultades en la comprensión de cuestiones algebraicas, posiblemente debido a su nivel de abstracción conceptual y su expresión eminentemente simbólica. Por lo que una manera efectiva de abordar la solución del problema es mejorando tanto la formación inicial y en servicio de los docentes de matemática principalmente en cuanto a su formación disciplinar.

Es importante entender que mejorar la enseñanza de los polinomios, significa también mejorar la comprensión de muchos otros conceptos que se encuentran directamente relacionados a los polinomios, como son las funciones, las ecuaciones y muchos otros conceptos matemáticos fundamentales.

El estudio de los polinomios no solo limitado a cuestiones operativas o de cálculo, sino fundamentalmente al estudio de sus propiedades que le dan la estructura de anillo, permite mejorar su comprensión, estableciendo analogías con otros objetos matemáticos de diferente naturaleza y sus posibilidades de aplicación en la interpretación y solución de situaciones diversas.

El uso de conceptos preliminares para entender la construcción de anillos de polinomios no está claramente comprendido por los estudiantes; es por ello que se vuelve dificultosa su comprensión. Se necesita conocer la estructura algebraica que es esencial para la construcción de los anillos de polinomios.

La importancia de conocer este tema de anillos de polinomios es que nos ayuda a comprender la construcción de los polinomios, bajo la comprensión del concepto de estructura algebraica, ley de composición interna, grupos subgrupos y las propiedades que caracterizan a los anillos.

Por lo que destacamos la realización del presente estudio, con miras a poner en primer plano la importancia de mejorar la comprensión de los polinomios para una mejora de su enseñanza en todos los niveles educativos.

Sugerencias

En el desarrollo de los sistemas numéricos, así como en el de los polinomios y otros objetos matemáticos, en el nivel de educación secundaria es posible introducir el concepto de estructuras algebraicas de manera progresiva, iniciando con el concepto de leyes de composición interna.

Enfatizar en la comprensión de las estructuras algebraicas en la formación de los estudiantes de educación en la especialidad de matemática, así como en aquéllos que ya se encuentran en ejercicio.

Introducir innovaciones en la enseñanza de las estructuras algebraicas a los futuros docentes de matemática, estableciendo vínculos con situaciones no matemáticas.

Replantear la enseñanza de los polinomios tanto en el nivel secundaria como en el nivel superior, para ir más allá del cálculo y profundizar en la comprensión de sus propiedades y su utilidad en el aprendizaje de otros objetos matemáticos.

En general, revisar el enfoque que se le da a la enseñanza del álgebra en la educación básica, para superar los principales obstáculos que se presentan en su aprendizaje desde los niveles básicos.

Referencias

Fraleigh, J. (1987). *Álgebra abstracta*. México: Addison-wesley.

Gentile, E. (1989). *Anillo de polinomios*. Buenos Aires: Editorial Docencia.

Herstein, I. (1985). *Álgebra Moderna*. México: Editorial Trillas.

Queysanne, M. (1989). *Álgebra básica*. Buenos Aires: Talleres gráficos.

Trejo, C. (1969). *Matemática elemental moderna*. Buenos Aires: Talleres gráficos.

Trujillo, F. & otros. (2014). *Introducción a las estructuras algebraicas*. Lima: UNE EGV.

http://www.mimosa.pntic.mec.es/jgomez53/matema/docums/taanillos.pdf (recuperado el 10-11-2018)

http://www.ugr.es/jesusgm/Curso/Matematica/Polinomios.pdf (recuperado el 10-11-2018).