Tema 2 - Anillos Conmutativos

En primer lugar, una operación (binaria) o ley de composición interna en un conjunto A es cualquier aplicación $*: A \times A \longrightarrow A$, mediante la cual cada par ordenado (a,b) de elementos de A tiene asignado un elemento $*(a,b)$; $a*b$ al que nos referimos como el resultado de operar a con b, de acuerdo con $*$.

En los conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$ o $\mathbb{C}$ se definen una operación producto y una suma.

Concepto de anillo conmutativo (E. Noether)

Es un conjunto A en el que hay definidas dos operaciones, una denotada de forma aditiva ("+") y la otra de forma multiplicativa ("·"), tal que se cumplen estas propiedades:

1. $a+(b+c) = (a+b)+c$ Asociativa de +
2. $a+b = b+a$ Conmutativa de +
3. $\exists 0 \in A \;/\; a+0 = a$ Existencia de cero.
4. $\forall a \in A, \exists -a \in A \;/\; a+(-a) = 0$ Existencia de opuestos.
5. $a(bc) = (ab)c$ Asociativa del producto.
6. $ab = ba$ Conmutatividad del producto.
7. $\exists 1 \in A \mid a \cdot 1 = a$ Existencia de uno.
8. $a(b+c) = ab + ac$ Distributiva del producto respecto a la suma.

- Un anillo no es conmutativo si no cumple 6.

Los anillos $\mathbb{Z}_n$

Teorema de Euclides: Para cualesquiera enteros $a, b \in \mathbb{Z}$ con $b \neq 0$ existen dos únicos enteros $q, r \in \mathbb{Z}$ tales que:

1. $a = bq + r$
2. $0 \leq r < |b|$.

$q \equiv$ cociente de dividir a por b

$r =$ resto.

Si $a, b \geq 0$

Sea $\Sigma = \{a - bq \; ; \; q \in \mathbb{N}, a - bq \geq 0\}$

$\Sigma \subseteq \mathbb{N}$

$a \in \Sigma \Rightarrow \Sigma \neq \emptyset$

Sea r min Σ

$r = a - bq$ para cierto $q \in \mathbb{N} \Leftrightarrow a = bq + r \qquad 0 \leq r$

Tenemos que ver $r < \overset{\wedge b}{|b|}$

- Supongo $r \geq b \Rightarrow r = b + k$ con $k \in \mathbb{N}$ $\qquad k = r - b$

$r = a - bq \Rightarrow b + k = a - bq \Rightarrow k = a - b(q+1) \; ; k \in \mathbb{Z}$

$k < r$!! Contradicción $k < r = \min \Sigma$ con $k \in \Sigma$

Si $a \leq 0$ y $b > 0$

$$\left.\begin{array}{l} -a \geq 0 \\ b > 0 \end{array}\right\} \Rightarrow 0 \leq r < |b|$$

$$a = b(-q) - r$$

$$= b(-q) - b + b - r = b(-q-1) + b - r$$

$$a = b(-q-1) + b - r \quad , \quad 0 \leq b - r < b$$

Si $r = 0 \rightarrow a = b(-q)$

Si $a \geq 0$ y $b < 0$

$$a = (-b)q + r$$

$$\Downarrow$$

$$a = b(-q) + r$$

$$0 \leq r < \underset{|b|}{\underset{\parallel}{-b}}$$

Si $a \leq 0$ y $b < 0$

$$-a = (-b)q + r$$

Si $r \neq 0 \Rightarrow a = bq - r = bq + b - b - r = b(q+1) - b - r$

Si $r = 0 \Rightarrow a = b(q)$

Unicidad de q y r

Supongo:

$a = bq + r = bq' + r'$; $0 \leq r, r' < |b|$, $q \neq q'$ $\Rightarrow b(q - q') = r' - r \Rightarrow |b(q-q')| = |r' - r|$

$\Rightarrow b(q-q') > b; |q - q'| \geq 1 \Rightarrow |r' - r| \geq b \rightarrow$ No $\Rightarrow$ Necesariamente $r' = r$ y $q = q'$

$\forall\, n \geq 2$, sea $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ el conjunto de los restos posibles resultantes al dividir cualquier entero entre n.

Sea $R : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ la aplicación que asigna a cada entero a su resto al dividirlo por n.

Propiedades de la aplicación.

1. Si $0 \leq a < n$, entonces $R(a) = a$,

2. $R(a + a') = R(R(a) + R(a'))$

3. $R(aa') = R(R(a)R(a'))$

$\oplus \Rightarrow r \oplus s = R(r+s)$

$\otimes \Rightarrow r \otimes s = R(rs)$

Proposición 2.1.2

Con estas operaciones, $\mathbb{Z}_n$ es un anillo conmutativo. Es llamado el anillo de restos módulo n.

Son conmutativas y asociativas:

$$(r \oplus s) \oplus t = R(s+r) \oplus R(t) = R(R(s+r) + R(t)) = R((s+r)+t)$$

$$r \oplus (s \oplus t) = R(r) \oplus (R(s+t)) = R(R(r) + R(s+t)) = R(r+(s+t))$$

$$(r \otimes s) \otimes t = R(r \cdot s) \otimes R(t) = R(R(r \cdot s) \cdot R(t)) = R((rs)t)$$

$$r \otimes (s \otimes t) = R(r) \otimes R(st) = R(R(r) \cdot R(st)) = R(r(st))$$

• $(-a)b = -(a,b)$

$ab + (-a)b = (a-a)b = 0b = 0 \Rightarrow -(ab) = (-a)b$

• $(-a)(-b) = ab$

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

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

$(-1)a = -a$

• $(a-b)c = a\cancel{b} - bc$

$(a-b)c = (a+(-b))c = ac + (-b)c = ac - bc$

• El anillo con un solo elemento $A = \{0\}$ con las operaciones obvias $0+0=0$, $00=0$ se llama anillo trivial.

• A es no trivial $\Longleftrightarrow 1 \neq 0$

• Sumas y productos reiterados.

Si $(a_1, \dots, a_n) \in A^n$ es una lista de n elementos del anillo, definimos su suma y su producto

$$\sum_{i=1}^{n} a_i = \left(\sum_{i=1}^{n-1} a_i\right) + a_n \; ; \qquad \prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i\right) a_n$$

Proposición 2.2.1

Sean naturales $m, n \geq 1$, $(a_1, \dots, a_m, a_{m+1}, \dots, a_{m+n})$ una lista de $m+n$ elementos del anillo. Entonces,

$$\sum_{i=1}^{m+n} a_i = \left(\sum_{i=1}^{m} a_i + \sum_{i=m+1}^{m+n} a_i\right), \quad \prod_{i=1}^{m+n} a_i = \left(\prod_{i=1}^{m} a_i\right)\left(\prod_{i=m+1}^{m+n} a_i\right)$$

En $\mathbb{Z}_n$ hay cero $(0 \oplus r = R(0+r) = R(r) = r)$ y un uno $(1 \otimes r) = R(1 \cdot r)$
$= R(r) = r$

Hay opuesto $-0 = 0$, para $0 < r < n$, $-r = n - r$, $r \oplus (n-r) = R(r + n - r)$
$= R(n) = 0$

Se verifica la propiedad distributiva.

$r \otimes (s \oplus t) = R(r) \otimes R(s+t) = R(R(r) \cdot R(s+t)) = R(r(s+t))$

$(r \otimes s) \oplus (r \otimes t) = R(rs) \oplus R(rt) = R(R(rs) + R(rt)) = R(rs + rt)$.

Generalidades

- Unicidad del 0 y del 1

$0' = 0' + 0 = 0$ y $1' = 1' 1 = 1$

- Unicidad del opuesto.

Sean a y a' tales que $a + a' = 0$

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

- $-(-a) = a$, $-0 = 0$

$-a + a = 0$ $\qquad$ $0 + 0 = 0$; el opuesto del cero es él mismo.

el opuesto de $-a$
es a

- $0a = 0$

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

Proposición 2.2.2 Distributividad generalizada

$$\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j$$

Los anillos de los enteros cuadráticos.

Sea A anillo conmutativo, un $B \subseteq A$ es "subanillo" si:

1. $\forall x, y \in B$, su suma $x+y$ y su producto xy están en B
2. $0, 1 \in B$
3. $\forall x \in B$, $-x \in B$.

Sea $n \in \mathbb{Z}$ tq $\sqrt{n} \notin \mathbb{Z}$; $n \notin \mathbb{Q}$ se denomina "anillo de enteros cuadráticos" al subanillo de $\mathbb{C}$:

$$\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}$$

y el anillo del ~~ℤ~~ racionales cuadráticos.

$$\mathbb{Q}[\sqrt{n}] = \{a + b\sqrt{n} \mid a, b \in \mathbb{Q}\}$$

En $\mathbb{Z}[\sqrt{n}]$
$$\begin{cases} (a+b\sqrt{n})(c+d\sqrt{n}) = ac + bdn + (ad+bc)\sqrt{n} \\ (a+b\sqrt{n})+(c+d\sqrt{n}) = (a+c)+(b+d)\sqrt{n} \end{cases}$$

$\mathbb{Z}[\sqrt{n}]$ es subanillo de $\mathbb{Q}[\sqrt{n}]$

Múltiplos y potencias naturales

Si $a_1 = a_2 = a_3, \dots, = a_n$ El elemento suma de todos ellos es $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} a$ esto es la suma reiterada de ese a, consigo mismo n veces.

Es decir na, siendo $n \geq 1$

Además $0a = 0$

Hemos definido el producto de cualquier número natural por cualquier elemento del anillo.

Lo mismo para $\prod_{i=1}^{n} a_i = \prod_{i=1}^{n} a$, es el producto reiterado de ese elemento a consigo mismo, n veces; a^n

Convenimos en que $a^0 = 1$.

Proposición

$\forall\, m,n \in \mathbb{N} = \{0,1,2,\dots\}$, $a,b \in A$ se verifica:

1. $(m+n)a = ma + na$
2. $n(a+b) = na + nb$
3. $m(na) = (mn)a$
4. $(ma)(nb) = (mn)ab$
5. $a^n a^m = a^{n+m}$
6. $(ab)^n = a^n \cdot b^n$
7. $(a^m)^n = a^{mn}$
8. $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$
9. $(a+b)^2 = a^2 + 2ab + b^2$
10. $(a+b)^3 = a^3 + 3a^2b + 3b^2a + b^3$
11. $(a-b)(a+b) = a^2 - b^2$

Unidades. Campos.

Un $u \in A$ es "invertible" o "unidad" del anillo $\Leftrightarrow \exists\ v \in A$ tq $uv = 1$

Es único (si $\exists$ otro v' tq $uv' = 1 \Rightarrow v' = v' \cdot 1 = v'(uv) = v'u(v) = 1 \cdot v = v$.)

Si u es una unidad, $\exists!\ v$ tq $uv = 1 \Rightarrow$ se llama "inversa" de u; $\boxed{u^{-1}}$

y u^{-1} es otra unidad.

Sea entonces $U(A) = \{ u \in A \mid u$ es unidad $\}$

Sea $n \in \mathbb{Z} \neq$ cuadrado. Si $\alpha = a + b\sqrt{n} \in \mathbb{Q}[\sqrt{n}]$, su "conjugado" es $\bar{\alpha} = a - b\sqrt{n}$.

Se define la norma $N(\alpha)$ de α:

$$N(\alpha) = \alpha \cdot \bar{\alpha} = (a + b\sqrt{n})(a - b\sqrt{n}) = a^2 - nb^2 \in \mathbb{Q}$$

Si $\alpha \in \mathbb{Z}[\sqrt{n}]$, si $a, b \in \mathbb{Z}$, $\Rightarrow N(\alpha) \in \mathbb{Z}$.

$N(\alpha\beta) = N(\alpha) \cdot N(\beta)$

$N(\alpha) = 0 \Leftrightarrow \alpha = 0$.

Proposición.

Sea $\alpha \in \mathbb{Z}[\sqrt{n}]$. Entonces $\alpha \in U\mathbb{Z}[\sqrt{n}] \Longleftrightarrow N(\alpha) = \pm 1$

Si $N(\alpha) = 1$, entonces $\alpha^{-1} = \bar{\alpha}$. Si $N(\alpha) = -1$, entonces $\alpha^{-1} = -\bar{\alpha}$. Si $\exists\ \alpha^{-1} \Rightarrow 1 = N(1) = N(\alpha \cdot \alpha^{-1}) = N(\alpha) N(\alpha^{-1})$ necesariamente $N(\alpha) = 1$ ó $N(\alpha) = -1$.

Proposición

Sea $\alpha \in \mathbb{Q}[\sqrt{n}]$. Entonces $\alpha \in U(\mathbb{Q}[\sqrt{n}]) \Longleftrightarrow \alpha \neq 0$

Demo

Si $\alpha \neq 0$ entonces es invertible, y $N(\alpha) = \alpha \cdot \bar{\alpha} \neq 0$ es un racional no nulo,

y $\alpha(N(\alpha)^{-1}\bar{\alpha}) = N(\alpha)^{-1} N(\alpha) = 1$, luego $\exists\, \alpha^{-1} = N(\alpha)^{-1}\bar{\alpha}$

Definición 2.5.1

Un anillo conmutativo A es un "cuerpo" si no es trivial y $U(A) = A \setminus \{0\}$, esto es si $1 \neq 0$ y, todo elemento no nulo tiene inversa.

Múltiplos negativos y potencias de exponente negativa

Lema 2.6.1

Sean $a_1, \dots, a_n \in A$

1. $-\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} (-a_i)$

2. Si $a_1, \dots, a_n \in U(A)$, entonces $\prod_{i=1}^{n} a_i \in U(A)$ y su inverso es $\left(\prod_{i=1}^{n} a_i\right)^{-1} = \prod_{i=1}^{n} a_i^{-1}$

Este lema asegura que $\forall\, n \in \mathbb{Z}$ tq $n \geq 1$, $-(na) = n(-a)$

Convenimos en definir este elemento como el producto del entero negativo $-n$ por el elemento a:

$$-n(a) = -(na) = n(-a)$$ y representarlo así: $-na$

Tma $\forall\, u \in U(A)$ y todo $n \geq 1$. $u^n \in U(A)$ y se verifica $(u^n)^{-1} = (u^{-1})^n$

Proposición 2.6.2

$\forall m,n \in \mathbb{Z}$, $a,b \in A$, $u,v \in U(A)$ se verifica:

1 $(m+n)a = ma + na$

$(m-n)a = ma - na$

2. $n(a+b) = na + nb$

$-(n)(a+b) = -na - nb$

3 $n(ma) = (nm)a$

$(-n)(ma) = -(n(ma)) = -(nma) = -((nm)a) = (-nm)a$

4 $(ma)(nb) = (mn)(ab)$

5 $u^m v^n = u^{m+n}$

6. $(uv)^n = u^n \cdot v^n$ $\quad (uv)^{-n} = ((uv)^n)^{-1} = (u^n \cdot v^n)^{-1} = u^{-n} \cdot v^{-n}$

7 $(u^m)^n = u^{mn}$ $\quad (u^m)^{-n} = ((u^m)^n)^{-1} = (u^{mn})^{-1} = u^{-mn}$

Los anillos de polinomios

El "Anillo de polinomios con coeficientes en A e indeterminada x"; $A[x]$ consiste de todas las aplicaciones

$f: \mathbb{N} \to A \mid \exists r \in \mathbb{N}$ de manera que $f(n) = 0 \ \forall n > r$

a las que nos referimos como polinomios. Para un tal polinomio f, y cada natural

$n \in \mathbb{N}$, el elemento $f(n) \in A$ se llama su "coeficiente de grado n"

$\boxed{\text{Polinomio } X}$ $\to$ $X : \mathbb{N} \to A \mid X(n) = \delta_{1,n}$ $\qquad \delta_{1,n} = \begin{cases} 1 & \text{si } 1 = n \\ 0 & \text{si } 1 \neq n \end{cases}$

↳ Polinomio cuyo único coeficiente no nulo es el de grado 1 y es el 1 de A

$\forall a \in A$, denotamos por a al polinomio cuyos coeficientes en grado > 0 son todos nulos y en grado 0 es a:

$$a : \mathbb{N} \to A \mid a(n) = a\delta_{0,n} = \begin{cases} a & \text{si } n = 0 \\ 0 & \text{si } n \neq 0 \end{cases}$$

Suma.

$(f+g)(n) = f(n) + g(n)$

producto $(fg)(n) = \sum_{i=0}^{n} f(i)g(n-i) = \sum_{i+j=n} f(i)g(j) = f(0)g(n) + f(1)g(n-1) + \dots + f(n)g(0)$

Propiedades

Asociativa

$f + (g+h) = (f+g)+h$

Conmutativa

$f+g = g+f$

Polinomio 0

$0(n) = \delta_{0,n} 0 = 0 \qquad f + 0 = f$ pq $(f+0)(n) = f(n) + 0 = f(n)$

Opuesto

$(-f)(n) = -f(n) \quad \forall n \in \mathbb{N} \qquad f + (-f) = 0 \quad \forall n \in \mathbb{N}$

Escaneado con CamScanner

Producto asociativo

$$f(gh) = (fg)(h)$$

Polinomio 1

1 del A. $\quad 1(n) = \delta_{0,n} = \delta_{0,n} \quad \forall n \in \mathbb{N} \qquad f1 = f$

$$(f1)(n) = \sum_{j+i=n}^{n} f(i)\,1(j) = f(n)$$

Distributividad

$$(f+(g+h))(n) = fg + fh$$

Lema 2.7.2

$\forall a \in A$ y $m \geq 0$, $a x^m$ es el polinomio con todos los coeficientes de grados distintos de m nulos y cuyo coeficiente en grado m es a.

$$\forall m \in \mathbb{N} \qquad (ax^m)(n) = a\,\delta_{m,n} = \begin{cases} a & \text{si } n = m \\ 0 & \text{si } n \neq m \end{cases}$$

Demo

$a = 1$ $\qquad x^{m+1}(0) = (x^m x)(0) = \sum_{i+j=0} (x^m(i)\,x(j)) = x^m(0)\,x(0) = 0 = \delta_{m+1,0}$

$n \geq 1$ $\qquad (x^{m+1})(n) = (x^m)(x)(n) = \sum_{i+j=n} (x^m)(i)\,x(j) = \sum_{i+j=n} \delta_{m,i}\,\delta_{1,j}$

$$= \delta_{m,n-1}\,\delta_{1,1} = \delta_{m,n-1} = \delta_{m+1,n}$$

$a \in A$ $\quad (ax^m)(n) = \sum_{i+j=n} a(i)(x^m)(j) = a(0)\,x^m(n) = a\,\delta_{m,n}$

Proposición

Sea $f \in A[X]$ el polinomio con coeficientes $f(n) = a_n$, $n \geq 0$, entonces

$$f = \sum_{m \geq 0} a_m x^m = a_0 + a_1 x + a_2 x^2 + \dots$$

La suma es finita, porque $\exists v \in \mathbb{N}$ tq $a_m = 0 \ \forall m \geq v$ (definición de polinomio

Demo

$$\left(\sum_{m \geq 0} a_m x^m \right)(n) = \sum_{m \geq 0} (a_m x^m)(n) = \sum_{m \geq 0} a_m \delta_{m,n} = a_n = f(n)$$

Ej: $f = -3 + 3x + 3x^7$ $\quad g = 3 + 2x$ polinomios en $\mathbb{Z}_4[X]$

$$f + g = x + 3x^7$$

$$fg = 2x^8 + x^7 + 2x^2 + 3x + 3$$

Nota

observar que los polinomios de $A[X]$ cuyos coeficientes en grado > 0 son son precisamente los elementos $a \in A$. Así $A \subseteq A[X]$ y es de hecho un subanillo.

Homomorfismos

Los anillos se relacionan entre sí mediante homomorfismos, aplicaciones entre ellos que respetan las operaciones

Sean A, A' anillos conmutativos $\Rightarrow$ Homomorfismo $= \phi : A \to A'$ con dominio A y rango A'

Propiedades

$\phi(a+a') = \phi(a) + \phi(a')$

$\phi(aa') = \phi(a)\phi(a')$

$\phi(1) = 1$

Preservan sumas, productos (reiterados), el cero, opuestos e inversos (si los hay):

$\phi\left(\sum_{i=1}^{n} a_i\right) = \sum_{i=1}^{n} \phi(a_i)$

$\phi\left(\prod_{i=1}^{n} a_i\right) = \prod_{i=1}^{n} \phi(a_i)$

$\phi(0) = 0$

$\phi(-a) = -\phi(a)$

$\phi(na) = n\phi(a) \quad n \in \mathbb{Z}$

$\phi(a^n) = \phi(a)^n \quad n \in \mathbb{Z}$

Si $a \in U(A) \Rightarrow \phi(a) \in U(A')$ y $\phi(a^{-1}) = \phi(a)^{-1}$

Si $a \in U(A) \Rightarrow \phi(a^n) = \phi(a)^n \quad \forall n \in \mathbb{Z}$

Si $\phi: A \to B$ y $\varphi: B \to D$ son homomorfismos, la aplicación compuesta $\varphi\phi: A \to B$ es también un homomorfismo.

Es importante reconocer que una aplicación es un homomorfismo (se pueden facilitar los cálculos)

Para cualquier homomorfismo $\phi: A \to B$ su imagen

$$Img(\phi) = \{\phi(x) \mid x \in A\}$$

es un subanillo de B "subanillo imagen de ϕ"

Si ϕ es sobreyectiva ($Img(\phi) = B$) $\Rightarrow$ Epimorfismo

Si ϕ es inyectiva ($x \neq y \Rightarrow \phi(y) \neq \phi(x)$) $\Rightarrow$ Monomorfismo

Si ϕ es biyectiva $\Rightarrow$ Isomorfismo $\phi: A \cong B$

La aplicación inversa ϕ^{-1} es tmb isomorfismo

Propiedad universal del anillo de polinomios

Teorema 2.8.2

↳ Sean A, B anillos conmutativos y $\phi: A \to B$ un homomorfismo

$\forall b \in B$, $\exists!$ homomorfismo $\Phi: A[x] \to B$ tq

1. $\Phi(a) = \phi(a)$, $\forall a \in A$

2. $\Phi(x) = b$

Sea $f(X) = \sum_{m\geq 0} a_m X^m$

$\phi(X) = b$

$$\Phi(f(x)) = \sum_{m\geq 0} \phi(a_m) b^m$$

Homomorfismo de evaluación

Si $A \subseteq B$ subanillo y $\phi = in : A \longrightarrow B$ = inclusión $a \longmapsto a$

$\Rightarrow \forall b \in B \ \exists!$ homomorfismo de anillos: $E_b : A[X] \longrightarrow B$

$$E_b(a) = a \quad \forall a \in A$$
$$E_b(X) = b$$

Si $f(X) = \sum_{m\geq 0} a_m X^m \Rightarrow E_b(f(X)) = \sum_{m\geq 0} a_i b^m$

Debido a esta expresión, se denota $E_b(f(X)) = f(b)$ que leemos "el resultado de evaluar $f(X)$ en b".

Si $f(b) = 0 \Rightarrow b$ es una raíz de $f(X)$ en B!

Cada polinomio $f(X) \in A[X]$ define una aplicación $A \to A$ que asigna como imagen a cada elemento $a \in A$, el resultado de evaluar $f(X)$ en a, esto es $f(a)$. Se denota igual que el polinomio $f(X) : A \to A$ y se le llama "función polinómica definida por el polinomio $f(X)$.