

# Álgebra I

## Doble Grado de Informática y Matemáticas

Curso 2016/17

### 1. Anillo conmutativo

**Definición (Anillo conmutativo).** Un conjunto  $A$  es un anillo conmutativo si en él hay definidas dos operaciones; una aplicación de adición y una aplicación de multiplicación, tales que cumplen las siguientes propiedades:

- (i) Asociativa:  $a + (b + c) = (a + b) + c$        $a(bc) = (ab)c$
- (ii) Conmutativa:  $a + b = b + a$        $ab = ba$
- (iii) Existencia elemento neutro:  $a + 0 = a$        $a * 1 = a$
- (iv) Existencia del elemento opuesto:  $a + (-a) = 0$
- (v) Distributiva del producto en la suma:  $a(b + c) = ab + ac$

**Definición (Grupo conmutativo).** Denominamos un grupo conmutativo o abeliano a aquellos conjuntos que cumplen las propiedades asociativa, conmutativa y existencia de elemento neutro para la suma, y existencia de elemento opuesto.

**Definición (monoide).** Denominamos monoide a un conjunto con una operación binaria interna que cumple la propiedad asociativa y tiene un elemento neutro a izquierda y derecha. En el caso del producto, se denomina monoide multiplicativo.

*Nota.* Llamaremos anillo aquellos conjuntos que cumplan todas las propiedades excepto la propiedad conmutativa para la multiplicación.

### 2. Caracterización de $\mathbb{Z}_n$ .

Llamaremos  $R_n : \mathbb{N} \rightarrow \mathbb{Z}_n$  a la aplicación definida como:

$$R_n(a) = a - nq = a - nE\left(\frac{a}{n}\right)$$

Para esta aplicación, definimos las siguientes propiedades:

- Si  $0 \leq a < n - 1 \rightarrow R_n(a) = a$
- $\forall a, b \in \mathbb{N}$ 
  - $R_n(a + b) = R_n(R_n(a) + R_n(b))$
  - $R_n(ab) = R_n(R_n(a) * R_n(b))$

Una vez que tenemos definida una suma y producto con la aplicación  $R_n$ , definimos la suma y el producto de  $\mathbb{Z}_n$ .

**Definición (Suma y producto en  $\mathbb{Z}_n$ ).** Se define la suma y el producto en  $\mathbb{Z}_n$  de la forma:

- $a \oplus b = R_n(a + b)$
- $a \otimes b = R_n(ab)$

Es fácil verificar que  $\mathbb{Z}_n$  es un anillo conmutativo con estas operaciones.

**Definición (Unidad).** Si  $A$  es un anillo conmutativo (a.c)  $a \in A$  es una "unidad" o "invertible" si  $\exists a^{-1}$  t.q.  $aa^{-1} = 1$ .  
 $U(A) = \{a \in A \text{ t.q. } a \text{ es una unidad}\} = \text{conjunto de las unidades de } A$ .

**Definición (Cuerpo).** Se dice que  $A$  es un **cuerpo** si siendo un anillo conmutativo,  $U(A) = A - \{0\}$ , es decir,  $\exists a^{-1} \forall a \in A$  con  $a \neq 0$ .

**Proposición (Asociatividad generalizada).** Sea  $A$  un anillo conmutativo, y  $a_1 \dots a_n$  una lista de elementos de  $A$ . La propiedad de la **asociatividad generalizada** nos dice que:  $\forall m$  tal que  $1 \leq m < n$  entonces:

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

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

**Definición (Distributividad generalizada).** Definimos también la distributividad generalizada en un anillo como:

$$\left( \sum_{i=0}^n a_i \right) \left( \sum_{j=1}^m b_j \right) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j \quad \forall a, b \in A$$

**Definición (Subanillo).** Si  $A$  es un anillo conmutativo y  $B$  es un subconjunto de  $A$ . Se dice que  $B$  es un **subanillo** de  $A$  ( $B \leq A$ ) si se verifican:

- $1, -1 \in B$
- $B$  es cerrado para la suma y el producto.

## 2.1. Ejemplos- Anillos de números cuadráticos

- $\mathbb{Z}[\sqrt{n}]$ . Definimos este conjunto de la siguiente forma:

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

Podemos definir también  $\mathbb{Q}[\sqrt{n}]$  de la misma forma:

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

Se puede comprobar que  $\mathbb{Z}[\sqrt{n}] \leq \mathbb{Q}[\sqrt{n}]$  y que  $\mathbb{Q}[\sqrt{n}]$  es un cuerpo.

**Definición (Conjugado).** Si  $\alpha = a + b\sqrt{n} \in \mathbb{Q}[\sqrt{n}]$  se define su conjugado como  $\bar{\alpha} = a - b\sqrt{n}$ . Este verifica que:

1.  $\overline{(\alpha + \beta)} = \bar{\alpha} + \bar{\beta}$
2.  $\overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$
3.  $\alpha = \bar{\alpha} \Leftrightarrow b = 0$

**Definición (Norma).** Se define entonces la Norma  $N(\alpha) = \alpha\bar{\alpha} = a^2 - nb^2 \in \mathbb{Q}$ . Así:

1.  $N(\alpha\beta) = N(\alpha) * N(\beta)$
2.  $N(\alpha) = 0 \Leftrightarrow \alpha = 0$

**Proposición.**  $\alpha \in a + b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$  es invertible  $\Leftrightarrow N(\alpha) \in \{-1, 1\}$

■ Anillos de series.

**Definición.** Si  $A$  es un anillo conmutativo y  $X$  es un símbolo que no denota ningún elemento de  $A$ . El anillo de series con coeficientes en  $A$ , denotado con  $A[[x]]$  esta definido como:

$$A[[x]] = \{a = \sum_{i=1}^n a_i x^i = a_0 + a_1 x^1 + \dots + a_n x^n\} \quad a_i \in A$$

Y definimos la suma y el producto de la siguiente forma:

$$(a + b) = \sum_{i=0}^n (a_i + b_i) x^i$$

$$(ab) = \sum_{k=0}^n \sum_{i=0}^k a_i b_{k-i}$$

Se puede probar que con estas operaciones de suma y producto,  $A[[x]]$  es un anillo y  $A[x]$  es un subanillo de  $A[[x]]$

### 3. Homomorfismos

**Definición.** Si  $A, B$  son anillos conmutativos, una aplicacion  $\varphi : A \rightarrow B$  es un homomorfismo si:

1.  $\varphi(1) = 1$
2.  $\varphi(a + b) = \varphi(a) + \varphi(b)$
3.  $\varphi(ab) = \varphi(a)\varphi(b)$

Además, decimos que:

1. Es monomorfismo si es inyectivo.
2. Es epimorfismo si es sobreyectivo.
3. Es isomorfismo si es biyectivo.

## Propiedades de los homomorfismos

- $\varphi(0) = 0$
- $\varphi(-a) = -\varphi(a)$
- $\varphi(\sum_{i=1}^n a_i) = \sum_{i=1}^n \varphi(a_i)$   
 $\varphi(\prod_{i=1}^n a_i) = \prod_{i=1}^n \varphi(a_i)$
- $\varphi(na) = n\varphi(a)$

Ya sabemos que  $Im(\varphi) = \{\varphi(x) : x \in A\} \leq B$  es un subanillo.

**Proposición.** Si  $\varphi$  es monomorfismo, entonces la aplicación restringida:

$$A \rightarrow Im(\varphi)$$

$$a \mapsto \varphi(a)$$

es un epimorfismo y por ello es un isomorfismo, podemos decir que  $A \cong Im(\varphi)$ .

*Nota.* Se puede probar que  $R_n : \mathbb{Z} \rightarrow \mathbb{Z}_n$  es un homomorfismo, llamado *Homomorfismo de reducción módulo  $n$*

**Proposición (1).** Dado  $A$  cualquier anillo conmutativo, conocido  $A[x]$ .

Si  $\varphi : A \rightarrow B$  es homomorfismo de anillos conmutativos, entonces:

$$\exists \varphi : A[x] \rightarrow B[x] : \varphi \left( \sum_i a_i x^i \right) = \sum_i \varphi(a_i) x^i$$

**Proposición (Sustición en un polinomio(2)).** Si  $A$  es cualquier conjunto y  $a \in A$  entonces: existe un homomorfismo  $E_a : A[x] \rightarrow A$  tal que  $E_a(\sum_i a_i x^i) = \sum_i a_i a^i$ .

**Proposición (3).** Si  $A \leq B$  es un subanillo y  $b \in B$ , la aplicación  $E_b : A[x] \rightarrow B$  definida como  $E_b(\sum_i a_i x^i) = \sum_i a_i b^i$  es un homomorfismo

**Proposición (Engloba a las anteriores).** Si  $\varphi : A \rightarrow B$  es un homomorfismo y  $b \in B$ , la aplicación  $\Phi : A[x] \rightarrow B$  definida como  $\Phi(\sum_i a_i x^i) = \sum_i \varphi(a_i) b^i \in B$  es un homomorfismo

*Demostración.* Veamos primero cómo (4) engloba a las demás:

- (i)  $4 \Rightarrow 3$ . Se ve tomando como  $\varphi$  la inclusión en  $B$
- (ii)  $4 \Rightarrow 2$ . Tomamos esta vez como  $\varphi$  la identidad
- (iii)  $4 \Rightarrow 1$ . Suponemos 4 válido. probaremos que  $\varphi : A \rightarrow B[x]$  que lleva  $a \rightarrow \varphi(a)$ . Ahora, podemos ver que esa aplicación es como usar primero  $\varphi$  para ir de  $A$  a  $B$  y luego usar la inclusión de  $B$  en  $B[x]$ :

$$A \rightarrow B \rightarrow B[x]$$

$$a \rightarrow a \rightarrow \varphi(a)$$

De esta forma, tomamos  $x \in B[x]$ . Entonces:

$$\begin{aligned} A[x] &\rightarrow B[x] \\ \sum_i a_i x_i &\rightarrow \sum_i \varphi(a_i) x_i \end{aligned}$$

Que es justamente el enunciado de la primera proposición.

Pasamos ahora a la demostración de la Proposición 4.

Sean  $f = \sum a_i x_i$  y  $g = \sum b_i x_i \in A[x]$ . Entonces:  $f + g = \sum c_i x_i$  con  $c_i = a_i + b_i$

Si ahora aplicamos  $\Phi(f + g) = \sum \varphi(c_i) b^i = \sum \varphi(a_i + b_i) b^i$ .

Como  $\varphi$  es homomorfismo, eso es igual a:  $\sum (\varphi(a_i) + \varphi(b_i)) b^i$ .

Usando que  $B$  es un anillo y por ello hay distributividad, eso es igual a:  $\sum (\varphi(a_i) b^i + \varphi(b_i) b^i)$ .

Por la asociatividad generalizada eso es igual a:  $\sum \varphi(a_i) b^i + \sum \varphi(b_i) b^i = \Phi(f) + \Phi(g)$  Por lo que queda probado para la suma.

Ahora probaremos el producto:

$$fg = \sum c_i x^i \text{ con } c_i = \sum_{i+j=n} a_i b_j$$

Así:

$$\Phi(fg) = \sum_n \varphi(c_n) b^n = \sum_n \varphi\left(\sum_{i+j=n} a_i b_j\right) b^n = \sum_n \left(\sum_{i+j=n} \varphi(a_i) \varphi(b_j)\right) b^n$$

Desarrollamos por otro lado

$$\begin{aligned} \Phi(f) + \Phi(g) &= \left(\sum_i \varphi(a_i) b^i\right) \left(\sum_j \varphi(b_j) b^j\right) \stackrel{(1)}{=} \sum_{i,j} \varphi(a_i) b^i \varphi(b_j) b^j \stackrel{(2)}{=} \sum_{i,j} \varphi(a_i b_j) b^{i+j} = \\ &= \sum_n \left(\sum_{i,j:i+j=n} \varphi(a_i b_j) b^n\right) \end{aligned}$$

Donde en (1) hemos usado la distributividad general y en (2) hemos usado que estamos en un anillo conmutativo y que  $\varphi$  es un homomorfismo.

Así, hemos llegado a dos expresiones que son iguales, probando así el resultado.

□