Tema 2

Anillos conmutativos

Como ya se comentó en la presentación del curso, nuestro interés en este curso se va a centrar en formalizar propiedades que presentan anillos como el de los enteros $\mathbb{Z}$ o el de polinomios $\mathbb{R}[x]$. Puesto que muchas de estas propiedades son análogas, así como los argumentos que las demuestran en cada caso concreto, nos ocuparemos de estudiarlas en un marco abstracto, de manera que sean de aplicación a cada contexto concreto.

Comenzamos diciendo que, en Matemáticas, convenimos en llamar *operación (binaria)* o *ley de composición interna* en un conjunto A a cualquier aplicación $* : A \times A \to A$, mediante la cual cada par ordenado (a, b) de elementos de A tiene asignado un elemento $*(a, b)$, más usualmente denotado por $a * b$, al que uno se refiere como *el resultado de operar a con b, de acuerdo con la operación* $*$. Por ejemplo, dado cualquier conjunto S, la aplicación $\cap : \mathcal{P}(S) \times \mathcal{P}(S) \to \mathcal{P}(S)$, que asigna a cada par de subconjuntos (A, B) su intersección $A \cap B$, es una operación en el conjunto de las partes de S.

Las operaciones en las que vamos a estar interesados en este curso serán denotadas *multiplicativa* o *aditivamente*. Para las primeras utilizamos bien el símbolo "$\cdot$", o la simple yuxtaposición, y escribimos para ellos $a \cdot b$, o simplemente $a\,b$, al resultado de operar ("multiplicar", en este caso) a con b, y lo leemos como *"a por b"*. Para las segundas utilizamos símbolo $+$, y escribimos $a + b$ como resultado de operar ("sumar", en este caso) a con b, y lo leemos como *"a más b"*.

En los conjuntos $\mathbb{N}$ de números naturales, $\mathbb{Z}$ de enteros $\mathbb{R}$ de reales o $\mathbb{C}$ de complejos tenemos definida un producto y una suma.

El concepto abstracto de *anillo conmutativo*, que presentamos a continuación, es debido a E. Noether (1921).

Definición 2.0.1. *Un "anillo conmutativo" 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 las siguientes ocho propiedades:*

1. $a + (b + c) = (a + b) + c$. *(asociatividad de la suma)*
2. $a + b = b + a$. *(commutatividad de la suma)*
3. $\exists\, 0 \in A \mid a + 0 = a$. *(existencia de cero)*
4. $\forall a \in A,\ \exists - a \in A \mid a + (-a) = 0$. *(existencia de opuestos)*
5. $a(bc) = (abc)$. *(asociatividad del producto)*

6. $ab = ba$. *(commutatividad del producto)*

7. $\exists\ 1 \in A \mid a1 = a$. *(existencia de uno)*

8. $a(b + c) = ab + ac$. *(distributividad del producto respecto a la suma)*

Nota 2.0.2. Un "anillo no conmutativo" es definido exactamente como uno conmutativo, pero sin el requisito (6) de la conmutatividad del producto. Un ejemplo típico de anillo no conmutativo es $\mathcal{M}_n(\mathbb{R})$, el anillo de las matrices cuadradas de orden n, para cualquier $n \geq 2$, con las operaciones usuales de suma y producto de matrices.

Podemos ya citar diversos ejemplos de referencia:

1. *El anillo $\mathbb{Z}$ de los números enteros*, con sus operaciones usuales de suma y multiplicación.

2. *El anillo $\mathbb{Q}$ de los números racionales*, cuyos elementos son las fracciones $\frac{m}{n}$ con $m, n \in \mathbb{Z}$ y $n \neq 0$, donde, recordar, $\frac{m}{n} = \frac{m}{n}$ si $mn' = nm'$, con las operaciones usuales de suma y producto.

3. *El anillo $\mathbb{R}$ de los números reales*, con las operaciones usuales de suma y producto.

4. *El anillo $\mathbb{C}$ de los números complejos*, con las operaciones usuales de suma y producto.

5. Este, seguramente, es novedoso. Sea A el conjunto de todas las funciones reales de variable en el intervalo $[0, 1]$, esto es, de todas las aplicaciones $f : [0, 1] \to \mathbb{R}$. Si $f, g \in A$, se define su suma $f + g$ como la función tal que $(f + g)(t) = f(t) + g(t)$, y su producto fg como la función tal que $(fg)(t) = f(t)g(t)$, para cada real $t \in [0, 1]$. De las propiedades de la suma y producto de los números reales se deduce fácilmente que A es un anillo conmutativo. Hay un cero $0 : [0, 1] \to \mathbb{R}$, que es la función constante nula, es decir, tal que $0(t) = 0\ \forall t$, y también un uno $1 : [0, 1] \to \mathbb{R}$, es la función constante uno, es decir, tal que $1(t) = 1\ \forall t$. La opuesta de una función $f : [0, 1] \to \mathbb{R}$ es la función $-f : [0, 1] \to \mathbb{R}$ definida por $(-f)(t) = -f(t)$, $\forall t$.

2.1 Los anillos $\mathbb{Z}_n$

Comenzaremos probando el famoso "*Teorema de Euclides*" sobre la división de números enteros (Euclides, 300 ac)

Teorema 2.1.1. *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. $0 \leq r < |b|$.

*El número q es llamado el "*cociente de dividir *a* por *b" y r el "*resto*".*

Demostración. Observemos en primer lugar que, si existen tales q y r, estos son únicos: Supongamos que $a = bq + r = bq' + r'$, donde $0 \leq r, r' < |b|$ y que $q \neq q'$. De la igualdad anterior se deduce la igualdad $b(q - q') = r' - r$, de donde también $|b||q - q'| = |r' - r|$. Como $q \neq q'$, es $|q - q'| \geq 1$. Por tanto, $|r' - r| \geq |b|$. Pero esto no es posible, pues $0 \leq r, r' < |b|$

y en consecuencia $|r' - r| < |b|$. Así que necesariamente $q = q'$, de donde la igualdad $r = r'$ también se deduce.

Probaremos ahora la existencia del cociente y del resto, atendiendo primero al caso en que $a \geq 0$, $b \geq 1$. Si $a < b$, la igualdad $a = 0b + a$, nos dice que el cociente es 0 y el resto a. Nos reducimos entonces al caso en que $a \geq b$. Sea el conjunto de números naturales $S = \{a - bx \mid x \in \mathbb{N}\} \cap \mathbb{N}$. Este es no vacío, pues $a - b \in S$. Tendrá entonces un primer elemento. Sea $r = \min S$. Como $r \in S$, será $r = a - bq$, o sea $a = bq + r$, para un cierto $q \in \mathbb{N}$. Si probamos que $r < b$, la demostración estara concluida: Si fuese $r \geq b$, y llamamos $r' = r - b$, tendríamos que $0 \leq r$ y $r' = a - bq - b = a - b(q + 1)$. Entonces $r' \in S$. Pero esto no es posible, pues $r' < r = \min S$.

Este es el caso que os enseñaros en la escuela: $3254 = 17 \cdot 191 + 7$, el cociente es 191 y resto 7. Para el resto de los casos, discutimos así:
Caso $-a$ entre b: Si $a = bq$, esto es, cociente q y resto 0, entonces $-a = b(-q)$, y el cociente de dividir $-a$ entre b es $-q$ y el resto 0. Si $a = bq + r$ con $0 < r < b$, entonces $-a = b(-q) - r = b(-q) - b + b - r = b(-q - 1) + (b - r)$, donde $0 < b - r < b$, así que el cociente de $-a$ entre b es $-q - 1$ y el resto $b - r$. Por ejemplo, $-3254 = 17 \cdot (-191) - 7 = 17 \cdot (-191) - 17 + 17 - 7 = 17 \cdot (-192) + 10$; luego el cociente de dividir -3254 entre 17 es -192 y el resto 10.
Caso a entre $-b$: Si $a = bq + r$, con $0 \leq r < b$, entonces $a = (-b)(-q) + r$, luego el cociente de a entre $-b$ es $-q$, y el resto r. Por ejemplo, $3254 = (-17)(-191) + 7$, luego el cociente de dividir 3254 entre 17 es -191 y el resto 7.
Caso $-a$ entre $-b$ Si $a = bq$, esto es, cociente q y resto 0, entonces $-a = (-b)q$, y el cociente de dividir $-a$ entre $-b$ es q y el resto 0. Si $a = bq + r$ con $0 < r < b$, entonces $-a = (-b)q - r = (-b)q - b + b - r = (-b)(q + 1) + (b - r)$, donde $0 < b - r < b$, así que el cociente de dividir $-a$ entre $-b$ es $q + 1$ y el resto $b - r$. Por ejemplo, $-3254 = (-17) \cdot 191 - 7 = (-17) \cdot 191 - 17 + 17 - 7 = (-17) \cdot (192) + 10$; luego el cociente de dividir -3254 entre -17 es 192 y el resto 10.

Para cada natural $n \geq 2$, sea

$$\mathbb{Z}_n = \{0, 1, \ldots, n - 1\}$$

el conjunto de los restos posibles resultantes al dividir cualesquiera enteros entre n. Sea

$$R : \mathbb{Z} \to \mathbb{Z}_n,$$

la aplicación que asigna a cada número entero a su resto al dividirlo por n. Esto es, si $a = nq + r$ con $0 \leq r < n$, entonces $R(a) = r$. Por ejemplo, si $n = 2$, entonces $\mathbb{Z}_2 = \{0, 1\}$ y $R : \mathbb{Z} \to \mathbb{Z}_2$ es la aplicación que asigna el 0 a los pares y 1 a los impares. La aplicación $R : \mathbb{Z} \to \mathbb{Z}_n$ verifica las siguientes propiedades:

1. Si $0 \leq a < n$, entonces $R(a) = a$,
2. $R(a + a') = R(R(a) + R(a'))$ (donde en ambos términos + es la suma en $\mathbb{Z}$).
3. $R(aa') = R(R(a)R(a'))$ (donde en ambos términos el producto es en $\mathbb{Z}$).

La primera es clara. Para las otras dos, pongamos $R(a) = r$, $R(a') = r'$, $R(r + r') = s$ y $R(rr') = t$. Será por que $a = nq + r$, $a' = nq' + r'$, $r + r' = np + s$ y $rr' = np' + t$, para ciertos enteros q, q', p, p'. Pero entonces

$$a + a' = nq + r + nq' + r' = nq + nq' + np + s = n(q + q' + p) + s,$$

y por tanto $R(a+a') = s = R(r+r') = R(R(a)+R(a'))$. Análogamente,

$$aa' = (nq+r)(nq'+r') = n^2qq' + nqr + rnq' + np' + t = n(nqq' + qr + rq' + p') + t$$

y por tanto $R(aa') = t = R(rr') = R(R(a)R(a'))$.

Definimos dos operaciones $\oplus$ y $\otimes$ en $\mathbb{Z}_n$, por las fórmulas

$$\begin{cases} r \oplus s &= R(r+s), \\ r \otimes s &= R(rs). \end{cases}$$

Proposición 2.1.2. *Con tales operaciones $\mathbb{Z}_n$ es un anillo conmutativo. Es llamado el anillo de restos módulo n.*

Demostración. Claramente son conmutativas. Son asociativas:

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

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

y la asociatividad de la suma $\oplus$ se deduce de la asociatividad de la suma en $\mathbb{Z}$. Análogamente,

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

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

y la asociatividad del producto $\otimes$ se deduce de la asociatividad del producto en $\mathbb{Z}$.

En $\mathbb{Z}_n$ tenemos un cero, el 0, pues $0 \oplus r = R(0+r) = R(r) = r$, y también un uno, el 1, pues $1 \otimes r = R(1 \cdot r) = R(r) = r$. Hay opuestos, $-0 = 0$ y, para $0 < r < n$, $-r = n - r$, pues $r \oplus (n-r) = R(r+n-r) = R(n) = 0$. Y se verifica la distributividad:

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

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

y la distributividad en $\mathbb{Z}_n$ se deduce de la distributividad en $\mathbb{Z}$. □

En adelante, utilizaremos la notación habitual de suma $r+s$ y producto rs para las operaciones en $\mathbb{Z}_n$. Así, en $\mathbb{Z}_6$

$$2+3=5, \quad 4+5=3, \quad -2=4, \quad 2\cdot 2=4, \quad 2\cdot 3=0, \quad 2\cdot 5=4, \quad 3\cdot 3=3, \quad \textit{etc.}$$

2.2 Generalidades

Mostramos a continuación una primera selección de propiedades sobre los anillos conmutativos, que se deducen directamente de los axiomas y son, por tanto, de aplicación a cualesquiera anillos conmutativos concretos.

En lo que sigue A es un anillo conmutativo dado, pero arbitrario.

- Unicidad del 0 y del 1.
  Si $0'$ y $1'$ fuesen otros elementos satisfaciendo los axiomas (3) y (7) repectivamente, tendríamos que $0' = 0'+0 = 0$ y $1' = 1'1 = 1$.

- Unicidad de opuestos.
  Si, para un elemento a, a' fuese otro elemento con $a+a' = 0$, tendríamos $a' = a'+0 = a'+(a+(-a)) = (a'+a)+(-a) = 0+(-a) = -a$.

- $\underline{-(-a) = a,\ -0 = 0.}$

  Puesto que $(-a) + a = 0$, el opuesto de $(-a)$ es a. Como $0 + 0 = 0$, el opuesto del cero es el mismo.

  Para dos elementos $a, b \in A$, es usual escribir $b + (-a)$ en la forma $b - a$, y rederirse a él como "b menos a".

- $\underline{0\,a = 0}$.

  En efecto, $0\,a = (0 + 0)a = 0\,a + 0\,a$. restando a ambos miembros $0a$, tenemos que $0 = 0a - 0a = (0a + 0a) - 0a = 0a + (0a - 0a) = 0a + 0 = 0a$.

- $\underline{(-a)b = -(ab),\ (-a)(-b) = ab,\ (-1)a = -a,\ (-1)(-1) = 1,\ (a - b)c = ab - ac.}$

  En efecto, $ab + (-a)b = (a + (-a))b = 0b = 0$. Luego $(-a)b = -(ab)$. También estonces $(-a)(-b) = -(-(ab)) = ab$. En particular $(-1)a = -(1a) = -a$, y $(-1)(-1) = 1$. Finalmente, $(a - b)c = (a + (-b))c = ac + (-b)c = ac - bc$.

- El anillo con un solo elemento $A = \{0\}$, con las operaciones obvias $0 + 0 = 0$, $00 = 0$, es llamado el anillo *trivial*.

- $\underline{A \text{ es no trivial} \Leftrightarrow 1 \neq 0.}$

  Obviamente si A es el anillo trivial $1 = 0$. Recíprocamente, si $1 = 0$, entonces, para todo $a \in A$, sería $a = 1a = 0a = 0$; esto es, A tiene un único elemento.

- $\underline{\text{Sumas y productos reiterados.}}$

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

$$\sum_{i=1}^{n} a_i = a_1 + \cdots + a_n, \qquad \prod_{i=1}^{n} a_i = a_1 \cdots a_n$$

  por inducción en n: Para $n = 1$, definimos $\sum_{i=1}^{1} a_i = a_1$, $\prod_{i=1}^{1} a_i = a_1$ y, para $n > 1$, recursívamente

$$\sum_{i=1}^{n} a_i = (\sum_{i=1}^{n-1} a_i) + a_n, \qquad \prod_{i=1}^{n} a_i = \Big(\prod_{i=1}^{n-1} a_i\Big) a_n.$$

  Así, $\sum_{i=1}^{2} a_i = a_1 + a_2$, $\sum_{i=1}^{3} a_i = (a_1 + a_2) + a_3$, $\sum_{i=1}^{4} a_i = ((a_1 + a_2) + a_3) + a_4$, etc.

  La propiedad *asociativa generalizada* siguiente, nos garantiza que, a efectos de cálculo, la ubicación de los paréntesis para realizar una tal suma o producto es irrelevante.

  Proposición 2.2.1. *Sean naturales $m, n \geq 1$, y $(a_1, \ldots, a_m, a_{m+1}, \ldots, a_{m+n})$ una lista de $m + n$ elementos del anillo. Entonces,*

$$\sum_{i=1}^{m+n} a_i = \Big(\sum_{i=1}^{m} a_i\Big) + \Big(\sum_{i=m+1}^{m+n} a_i\Big),$$
$$\prod_{i=1}^{m+n} a_i = \Big(\prod_{i=1}^{m} a_i\Big)\Big(\prod_{i=m+1}^{m+n} a_i\Big).$$

Notemos que, por ejemplo, si $m = 2$ y $n = 2$, la igualdad propuesta nos dice que

$$((a_1 + a_2) + a_3) + a_4 = (a_1 + a_2) + (a_3 + a_4),$$

y si $m = 1$, $n = 3$, que $((a_1 + a_2) + a_3) + a_4 = a_1 + ((a_2 + a_3) + a_4)$.

DEMOSTRACIÓN. Procedemos por inducción en n. Para $n = 1$, es la definición:

$$\sum_{i=1}^{m} a_i + \sum_{i=m+1}^{m+1} a_i = \sum_{i=1}^{m} a_i + a_{m+1} = \sum_{i=1}^{m+1} a_i.$$

Supuesto cierto para un n,

$$\sum_{i=1}^{m} a_i + \sum_{i=m+1}^{m+n+1} a_i = \sum_{i=1}^{m} a_i + \Big(\sum_{i=1}^{m+n} a_i + a_{m+n+1} \Big) = \Big(\sum_{i=1}^{m} a_i + \sum_{i=m+1}^{m+n} a_i \Big) + a_{m+n+1}$$
$$= \sum_{i=1}^{m+n} a_i + a_{m+n+1} = \sum_{i=1}^{m+n+1} a_i.$$

□

La siguiente igualdad también es importante

Proposición 2.2.2 (*Distributividad generalizada*). $\Big(\sum_{i=1}^{m} a_i \Big) \Big(\sum_{j=1}^{n} b_j \Big) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j$.

DEMOSTRACIÓN. Inducción en m. Si $m = 1$, havemos inducción en n. Si $n = 1$ es obvio: $a_1 b_1 = a_1 b_1$. Si $n > 1$:

$$a_1 \sum_{j=1}^{n} b_j = a_1 \Big(\sum_{j=1}^{n-1} b_j + b_n \Big) = \Big(a_1 \sum_{j=1}^{n-1} b_j \Big) + a_1 b_n = \sum_{j=1}^{n-1} a_1 b_j + a_1 b_n = \sum_{j=1}^{n} a_1 b_j.$$

Supuesto ahora $m > 1$, y haciendo hipótesis de inducción:

$$\Big(\sum_{i=1}^{m} a_i \Big) \Big(\sum_{j=1}^{n} b_j \Big) = \Big(\sum_{i=1}^{m-1} a_i + a_m \Big) \Big(\sum_{j=1}^{n} b_j \Big) = \Big(\sum_{i=1}^{m-1} a_i \Big) \Big(\sum_{j=1}^{n} b_j \Big) + a_m \Big(\sum_{j=1}^{n} b_j \Big)$$
$$= \Big(\sum_{i=1}^{m-1} \sum_{j=1}^{n} a_i b_j \Big) + \sum_{j=1}^{n} a_m b_j = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j. \quad \square$$

2.3 Los anillos de enteros cuadráticos $\mathbb{Z}[\sqrt{n}]$

Si A es un anillo conmutativo, un subconjunto suyo $B \subseteq A$ es llamado un "*subanillo*" si

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

Todo subanillo B de un anillo conmutativo A es por sí mismo un anillo conmutativo, donde se suma y multiplica como en el anillo ambiente A. Por ejemplo, las inclusiones $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ indican subanillos. Sin embargo, para cualquier $n \geq 2$, se verifica que $\mathbb{Z}_n \subseteq \mathbb{Z}$ como subconjunto, pero no se trata de un subanillo, pues $\mathbb{Z}_n$ no es cerrado para sumas, ni productos, ni opuestos en $\mathbb{Z}$. Además, es claro que en $\mathbb{Z}_n$ no se opera como en el anillo de los enteros $\mathbb{Z}$.

Presentamos a continuación otros subanillos de $\mathbb{R}$ o $\mathbb{C}$. Primero, fijemos una notación. Sea $\alpha \in \mathbb{R}$, $\alpha > 0$, cualquier número real positivo. Existen exactamente dos números reales $x \in \mathbb{R}$ tales que $x^2 = \alpha$, uno positivo al que nos referimos como $\sqrt{\alpha}$ y otro negativo, que es su opuesto $-\sqrt{\alpha}$. No existen, sin embargo números reales x tales que $x^2 = -\alpha$, pues el cuadrado de un número real es siempre mayor o igual que cero. Pero si que existen dos números complejos cuyo cuadrado es $-\alpha$, a saber: $i\sqrt{\alpha}$ y su opuesto $-i\sqrt{\alpha}$. Nos referimos al primero como $\sqrt{-\alpha}$. Esto es,

$$\sqrt{-\alpha} = i\sqrt{\alpha}.$$

Así, por ejemplo, $\sqrt{-1} = i$, $\sqrt{-2} = i\sqrt{2}$, $\sqrt{-4} = 2i$, etc.

Sea ahora $n \in \mathbb{Z}$ un entero que no es un cuadrado en $\mathbb{Z}$, esto es, tal que $\sqrt{n} \notin \mathbb{Z}$ (esto obviamente es cierto si $n \leq -1$). En cuyo caso se puede demostrar que $\sqrt{n}$ es un número irracional, esto es $\sqrt{n} \notin \mathbb{Q}$ (esto lo probaremos más adelante). Definimos el "*anillo de enteros cuadráticos*" como el subanillo de $\mathbb{C}$ formado por los números

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

y el "*anillo de racionales cuadráticos*"

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

Estos son efectivamente subanillos, pues claramente contienen al $0 = 0 + 0\sqrt{n}$ y al $1 = 1 + 0\sqrt{n}$, son cerrado para opuestos, pues $-(a + b\sqrt{n}) = -a - b\sqrt{n}$ y este es un entero o racional cuadrático si el primero lo és. También son cerrados para sumas y productos, pues

$$(a + b\sqrt{n}) = (a' + b'\sqrt{n}) = a + a' + (b + b')\sqrt{n},$$

$$(a + b\sqrt{n})(a' + b'\sqrt{n}) = aa' + ab'\sqrt{n} + a'b\sqrt{n} + bb'\sqrt{n}\sqrt{n} = aa' + nbb' + (ab' + ba')\sqrt{n},$$

y los resultados son enteros o racionales cuadráticos según lo sean los números que se suman o multiplican.

Notemos que $\mathbb{Z}[\sqrt{n}]$ es un subanillo de $\mathbb{Q}[\sqrt{n}]$.

Nota. Subrayemos que, si $n > 0$, entonces $\mathbb{Z}[\sqrt{n}]$ y $\mathbb{Q}[\sqrt{n}]$ son subanillos de $\mathbb{R}$ (pues $\sqrt{n} \in \mathbb{R}$), mientras que $\mathbb{Z}[\sqrt{-n}] = \mathbb{Z}[i\sqrt{n}]$ y $\mathbb{Q}[\sqrt{-n}] = \mathbb{Q}[i\sqrt{n}]$ son subanillos de $\mathbb{C}$, no de $\mathbb{R}$.

Así, por ejemplo, tenemos los anillos $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid, a, b \in \mathbb{Z}\}$ y $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, donde la suma y el producto es definido por

$$(a + b\sqrt{2}) + (a' + b'\sqrt{2}) = (a + a') + (b + b')\sqrt{2},$$
$$(a + b\sqrt{2})(a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + ba')\sqrt{2}.$$

o el llamado *anillo de los enteros de Gauss* (1800) $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, donde

$$(a + bi) + (a' + b'i) = (a + a') + (b + b')i,$$
$$(a + bi)(a' + b'i) = (aa' - bb') + (ab' + ba')i.$$

2.4 Múltiplos y potencias naturales

Si tenemos una lista de elementos $(a_1, \ldots, a_n)$ en la que todos los elementos son iguales, digamos $a_1 = a_2 = \cdots = a_n = a$, entonces el elemento suma de todos ellos $\sum_{i=1}^n a_i = \sum_{i=1}^n a$ es precisamente la suma reiterada de ese elemento a consigo mismo n veces. Se representa por na, y nos referimos a este elemento como *producto del número entero $n \geq 1$ por a*. Convenimos también en poner $0a = 0$, de manera tenemos definido el producto de cualquier número natural por cualquier elemento del anillo. Similármente, el elemento producto de todos ellos $\prod_{i=1}^n a_i = \prod_{i=1}^n a$ es el producto reiterado de ese elemento a consigo mismo n veces. Se representa por a^n. Y , convenimos en poner $a^0 = 1$.

Proposición 2.4.1. *Para cualesquiera $m, n \in \mathbb{N} = \{0, 1, 2, ...\}$, $a, b \in A$, se verifican las igualdades*

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. $(ab)^n = a^n b^n$.
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. $(a+b)^3 = a^3 + 3a^2 b + 3ab^2 + b^3$.
11. $(a-b)(a+b) = a^2 - b^2$.

Demostración. (1) y (5): Para $m, n \geq 1$, son directa consecuencia de la asociatividades generalizadas de la suma y el producto. Que son ciertas también si $m = 0$ o $n = 0$ es inmediato desde que $0a = 0$ y $a^0 = 1$.

(2) y (6): Para $n = 0, 1$ son inmediatas. Para $n \geq 1$ procedemos inductívamente:

$$\begin{aligned}(n+1)(a+b) &= n(a+b) + a + b = na + nb + a + b = na + a + nb + b \\ &= (n+1)a + (n+1)b,\end{aligned}$$

$$(ab)^{n+1} = (ab)^n ab = a^n ab^n b = a^{n+1} b^{n+1}.$$

(3) y (7): Para $m = 0$ son claras. Para $m \geq 1$ (n arbitrario), hacemos inducción:

$$(m+1)(na) = m(na) + na = (mn)a + na = (mn + n)a = ((m+1)n)a,$$

$$(a^m)^{n+1} = (a^m)^n a^m = a^{mn} a^m = a^{mn+m} = a^{m(n+1)}.$$

(4): Para $m, n \geq 1$, la igualdad se sigue de la distributividad generalizada, y resulta evidente si $m = 0$ o $n = 0$.

(8) Recordemos el significado de los términos binomiales

$$\binom{n}{i} = \frac{n!}{i!(n-i)!} = \frac{n(n-1)\cdots(n-i+1)}{i(i-1)\cdots 2\cdot 1}.$$

Y tengamos en cuenta la fórmula

$$\begin{aligned}\binom{n}{j} + \binom{n}{j-1} &= \frac{n!}{j!(n-j)!} + \frac{n!}{(j-1)!(n-j+1)!} = \frac{n!(n-j)!(j-1)!(n-j+1+j)}{j!(n-j)!(j-1)!(n-j+1)!} \\ &= \frac{n!(n+1)}{j!(n-j+1)!} = \binom{n+1}{j}.\end{aligned}$$

Procedemos entonces inductívamente en $n \geq 1$. Para $n = 1$ es fácil

$$\binom{1}{0}a^0b^1 + \binom{1}{1}a^1b^0 = b + a = a + b = (a+b)^1.$$

Supuesta la validez para un n, entonces

$$\begin{aligned}(a+b)^{n+1} = (a+b)(a+b)^n = (a+b)\sum_{i=0}^{n}\binom{n}{i}a^ib^{n-i} &= \sum_{i=0}^{n}\binom{n}{i}a^{i+1}b^{n-i} + \sum_{i=0}^{n}\binom{n}{i}a^ib^{n+1-i} \\ &= \sum_{i=1}^{n+1}\binom{n}{i-1}a^ib^{n+1-i} + \sum_{i=0}^{n}\binom{n}{i}a^ib^{n+1-i} \\ &= \sum_{i=1}^{n+1}\binom{n+1}{i}a^ib^{n+1-i} + b^{n+1} = \sum_{i=0}^{n+1}\binom{n+1}{i}a^ib^{n+1-i}. \quad \square\end{aligned}$$

Por ejemplo, si $S = \{a_1, a_2, \ldots, a_n\}$ es un conjunto con n elementos, entonces $\mathcal{P}(S)$ consiste del $\emptyset$, los n conjuntos unitarios $\{a_i\}$ conteniendo un solo elemento, los $\binom{n}{2} = n(n-1)/2$ subconjuntos con dos elementos $\{a_i, a_j\}$, $i \neq j$, los $\binom{n}{i}$subconjuntos conteniendo i elementos, y así sucesivamente. Entonces, la *cardinalidad* (= número de elementos) de $\mathcal{P}(S)$ es

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = (1+1)^n = 2^n.$$

2.5 Unidades. Cuerpos

Un elemento $u \in A$, se dice que es "*invertible*" o "*unidad*" del anillo si existe un otro $v \in A$ tal que $uv = 1$. Si existiera un otro v' tal que $uv' = 1$, entonces

$$v' = v'1 = v'(uv) = (v'u)v = 1v = v,$$

necesariamente se trataría del mismo v. Esto es, si u es una unidad, hay un único v tal que $uv = 1$, al que llamamos "*inverso*" de u y escribimos u^{-1}. Naturalmente, en tal caso, u^{-1} es otra unidad, con $(u^{-1})^{-1} = 1$.

Por ejemplo, el 1 siempre es unidad, le llamamos "*la unidad*" del anillo, utilizando para ella el artículo determinado, para distinguirla de las demas unidades. También su opuesto -1 es siempre una unidad, pues $(-1)^2 = 1$, con $(-1)^{-1} = -1$. En general, no todos los elementos del anillo son unidades. Por ejemplo, en anillos no triviales, esto es, con al menos

dos elemento, el 0 no puede ser invertible: Si existiera un v tal que $0v = 1$, como $0v = 0$, sería $1 = 0$ y sabemos que entonces A es el anillo trivial.

Denotaremos por $U(A)$ al subconjunto de las unidades del anillo:

$$U(A) = \{u \in A \mid u \text{ es unidad}\}.$$

EJEMPLOS.

1. $U(\mathbb{Z}) = \{\pm 1\}$, pues si $m, n \in \mathbb{Z}$ con $|m|, |n| > 1$, entonces $|mn| > 1$, y por tanto $mn \neq 1$. Además $0 \notin U(\mathbb{Z})$, pues $\mathbb{Z}$ no es trivial.
2. $U(\mathbb{Z}/2) = \{1\}$, $U(\mathbb{Z}/3) = \{1, 2\}$, $U(\mathbb{Z}/4) = \{1, 3\}$.
3. Sea $n \in \mathbb{Z}$ un entero que no es un cuadrado. Si $\alpha = a + b\sqrt{n} \in \mathbb{Q}[\sqrt{n}]$, su "*conjugado*" es $\overline{\alpha} = a - b\sqrt{n}$. Es fácil verificar las igualdades

$$\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}, \quad \overline{\alpha\beta} = \overline{\alpha}\overline{\beta}, \quad \overline{\overline{\alpha}} = \alpha.$$

Se define la *norma* $N(\alpha)$ de α por

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

Y hagamos notar que si $\alpha \in \mathbb{Z}[\sqrt{n}]$, esto es, si $a, b \in \mathbb{Z}$, entonces $N(\alpha) \in \mathbb{Z}$. También es fácil verificar que $N(\alpha\beta) = N(\alpha)N(\beta)$ y que $N(\alpha) = 0 \Leftrightarrow \alpha = 0$.

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

DEMOSTRACIÓN. Si $N(\alpha) = 1$, entonces $\alpha^{-1} = \overline{\alpha}$. Si $N(\alpha) = -1$, entonces $\alpha^{-1} = -\overline{\alpha}$. Y recíprocamente, si existe α^{-1}, entonces $1 = N(1) = N(\alpha\,\alpha^{-1}) = N(\alpha)N(\alpha^{-1})$, luego necesariamente $N(\alpha) = 1$ o $N(\alpha) = -1$. □

Así, por ejemplo

• $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$, pues $N(a + bi) = a^2 + b^2 \geq 0$ y

$$N(a + bi) = 1 \Leftrightarrow a^2 + b^2 = 1 \Leftrightarrow (a = \pm 1 \wedge b = 0) \vee (a = 0 \wedge b = \pm 1).$$

• Si $n \geq 2$ $U(\mathbb{Z}[\sqrt{-n}]) = \{1, -1\}$, pues $N(a + bi) = a^2 + nb^2 \geq 0$ y

$$N(a + b\sqrt{-n}) = 1 \Leftrightarrow a^2 + nb^2 = 1 \Leftrightarrow a = \pm 1 \wedge b = 0.$$

• En $\mathbb{Z}[\sqrt{2}]$, $N(a+b\sqrt{2}) = a^2-2b^2$. Entonces 1 y -1 son unidades. Como $N(1+\sqrt{2}) = 1-2 = -1$, $1+\sqrt{2}$ es una unidad con $(1+\sqrt{2})^{-1} = -1+\sqrt{2}$. También, $1-\sqrt{2}$ es una unidad, pues $N(1-\sqrt{2}) = -1$, con inverso $(1-\sqrt{2})^{-1} = -1-\sqrt{2}$. Puede demostrarse que

$$U(\mathbb{Z}[\sqrt{2}]) = \{\pm 1, \pm(1+\sqrt{2})^k, \pm(1-\sqrt{2})^k, k \geq 1\}.$$

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

DEMOSTRACIÓN. Solo tenemos que probar que si $\neq 0$ entonces es invertible: Si $\alpha \neq 0$, entonces $N(\alpha) = \alpha\bar{\alpha} \neq 0$ es un racional no nulo y

$$\alpha\Big(N(\alpha)^{-1}\bar{\alpha}\Big) = N(\alpha)^{-1}N(\alpha) = 1,$$

luego existe $\alpha^{-1} = N(\alpha)^{-1}\bar{\alpha}$. □

Por ejemplo, en $\mathbb{Q}[\sqrt{2}]$, $N(3+\sqrt{2}) = 9-2 = 7$ y

$$(3+\sqrt{2})^{-1} = \frac{3}{7} - \frac{1}{2}\sqrt{2}.$$

Definición 2.5.1. *Un anillo conmutativo A es un "*cuerpo*" si es no trivial y $U(A) = A - \{0\}$, esto es, si $1 \neq 0$ y todo elemento no nulo tiene un inverso.*

Ejemplos.

1. $\mathbb{Z}$ no es un cuerpo, pero $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ sí lo son.
2. Los anillos de restos $\mathbb{Z}_2$ y $\mathbb{Z}_3$ son cuerpos, pero $\mathbb{Z}_4$ no lo es ($2 \notin U(\mathbb{Z}/4)$).
3. Ningún anillo de enteros cuadráticos $\mathbb{Z}[\sqrt{n}]$ es un cuerpo (2 no es unidad, pues $N(2) = 4 \neq \pm 1$).
4. Los anillos de racionales cuadráticos $\mathbb{Q}[\sqrt{n}]$ son cuerpos.

2.6 Múltiplos negativos y potencias de exponente negativo

Lema 2.6.1. *Sean $a_1, \ldots, a_n \in A$.*

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

Demostración. Inducción en $n \geq 1$. El caso $n = 1$ es una evidencia. Supuesto $n > 1$, y haciendo hipótesis de inducción,

$$\begin{aligned}\sum_{i=1}^n a_i + \sum_{i=1}^n -a_i &= \sum_{i=1}^{n-1} a_i + a_n + \sum_{i=1}^{n-1} -a_i - a_n = \sum_{i=1}^{n-1} a_i + a_n - a_n + \sum_{i=1}^{n-1} -a_i \\ &= \sum_{i=1}^{n-1} a_i + \sum_{i=1}^{n-1} -a_i = \sum_{i=1}^{n-1} a_i - \sum_{i=1}^{n-1} a_i = 0.\end{aligned}$$

$$\begin{aligned}\Big(\prod_{i=1}^n u_i\Big)\Big(\prod_{i=1}^n u_i^{-1}\Big) &= \Big(\prod_{i=1}^{n-1} u_i\Big)u_n\Big(\prod_{i=1}^{n-1} u_i^{-1}\Big)u_n^{-1} = \Big(\prod_{i=1}^{n-1} u_i\Big)u_n u_n^{-1}\Big(\prod_{i=1}^{n-1} u_i^{-1}\Big) \\ &= \Big(\prod_{i=1}^{n-1} u_i\Big)\Big(\prod_{i=1}^{n-1} u_i^{-1}\Big) = 1.\end{aligned}$$

□

El lema anterior nos asegura que, para cualquier entero $n \geq 1$, $-(na) = n(-a)$. Convenimos en definir este elemento como *el producto del entero negativo $-n$ por el elemento a*:

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

y representarlo simplemente como $-na$ (sin posible confusión por ubicación de paréntesis). De forma similar, para todo $u \in U(A)$ y todo $n \geq 1$, tenemos que $u^n \in U(A)$, y se verifica que $(u^n)^{-1} = (u^{-1})^n$. Convenimos en definir este elemento como *la potencia de exponente el entero negativo* $-n$ *del elemento* u, y representarlo por

$$u^{-n} = (u^n)^{-1} = (u^{-1})^n,$$

sin tampoco posible confusión por ubicación de paréntesis.

Proposición 2.6.2. *Para cualesquiera* $m, n \in \mathbb{Z}$, $a, b \in A$, $u, v \in U(A)$, *se verifican las igualdades*

1. $(m+n)a = ma + na$.
2. $n(a+b) = na + nb$.
3. $n(ma) = (nm)a$.
4. $(ma)(nb) = (mn)(ab)$.
5. $u^m v^n = u^{m+n}$.
6. $(uv)^n = u^n v^n$.
7. $(u^m)^n = u^{mn}$.

Solo tenemos que ver el caso en que intervienen enteros negativos. Sean $m, n > 0$.
(1) y (5): Si $m \geq n$, pongamos $m = n + k$, con $k = m - n \geq 0$. Entonces,

$$ma - na = (n+k)a - na = na + ka - na = na - na + ka = 0 + ka = ka = (m-n)a.$$

$$u^m u^{-n} = u^{n+k} u^{-n} = u^k u^n u^{-n} = u^k 1 = ka = u^{m-n}.$$

Análogamente, si $m \leq n$, pongamos $n = m + k$, con $k = n - m \geq 0$. Entonces,

$$ma - na = ma - (m+k)a = ma - (ma + ka) = ma - ma - ka = -ka = (m-n)a.$$

$$u^m u^{-n} = u^m u^{-(m+k)} = u^m (u^{m+k})^{-1} = u^m (u^m u^k)^{-1} = u^m (u^m)^{-1} (u^k)^{-1} = u^{-k} = u^{m-n}.$$

Finalmente,

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

$$u^{-m-n} = (u^{m+n})^{-1} = (u^m u^n)^{-1} = (u^m)^{-1} (u^n)^{-1} = u^{-m} u^{-n}.$$

(2) y (6):

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

$$(uv)^{-n} = ((uv)^n)^{-1} = (u^n)^{-1} (v^n)^{-1} = u^{-n} v^{-n}.$$

(3) y (7):

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

$$(u^m)^{-n} = ((u^m)^n)^{-1} = (u^{mn})^{-1} = u^{-mn}.$$

La igualdades $n(-ma) = (-nm)a$ y $(u^{-m})^n = u^{-mn}$ se ven similármente, y, finalmente,

$$(-n)((-m)a) = -(n(-(ma)) = (nm)a = ((-n)(-m)a),$$

$$(u^{-m})^{-n} = (((u^m)^{-1})^{-1})^m = (u^m)^n = u^{mn} = u^{(-m)(-n)}.$$

(4):

$$(-ma)(nb) = -((ma)(nb)) = -((mn)(ab)) = -(mn)(ab) = ((-m)n)(ab),$$

$$(-ma)(-nb) = (ma)(nb) = (mn)(ab) = ((-m)(-n))(ab).$$

□

2.7 Los anillos de polinomios $A[x]$

Sea A un anillo conmutativo dado, no trivial, y x cualquier símbolo que no denote elemento alguno de A, al que nos referiremos com "indeterminada" (antiguamente se le llamó "cosa") a los efectos de la siguiente construcción.

Sea $\mathbb{N} = \{0, 1, \cdots\}$ es el conjunto de los números naturales. Para cualesquiera dos naturales $m, n \in N$, vamos a usar el símbolo *delta de Kronecker*, $\delta_{m,n}$, que significará bien el 0 o el 1 del anillo A, según la simple regla

$$\delta_{m,n} = \begin{cases} 1 & si \quad m = n, \\ 0 & si \quad m \neq n. \end{cases}$$

Definición 2.7.1. *El "*Anillo de polinomios con coeficientes en A e indeterminada x*", denotado por $A[x]$, consiste de todas las aplicaciones*

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

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*".*

En este anillo, usamos el símbolo x para denotar al polinomio

$$x : \mathbb{N} \to A \mid x(n) = \delta_{1,n},$$

esto es, el polinomio cuyo único coeficiente no nulo es el de grado 1, y es el 1 de A. Además, para cada $a \in A$, denotamos también por a al polinomio cuyos coeficientes en grados > 0 son todos nulos, y en grado 0 es a, es decir,

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

Las operaciones de suma $f + g$ y producto fg en $A[x]$ están definidas por

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

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

Observemos que esas operaciones conducen efectivamente a nuevos polinomios. En relación con la suma, simplemente observar que, si $f(n) = 0$, $\forall n > r$ y $g(n) = 0$, $\forall n > s$, entonces $(f + g)(n) = f(n) + g(n) = 0$, $\forall n > \max\{r, s\}$. Y en relación con el producto, $\forall n > r + s$, $(fg)(n) = \sum_{i+j=n} f(i)g(j) = 0$, pues $i + j > r + s$ exige que bien es $i > r$ o $j > s$ y, por tanto, en cada sumando bien es $f(i) = 0$ o $g(j) = 0$.

Antes de ver como esta definición de $A[x]$ se relaciona con vuestro concepto usual de "polinomio", vamos a discutir que realmente estamos en presencia de un anillo conmutativo.
• La suma es asociativa: $f+(g+h)=(f+g)+h$ pues, $\forall\, n\in\mathbb{N}$,

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

• La suma es conmutativa: $f+g=g+f$ pues, $\forall\, n\in\mathbb{N}$,

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

• Hay un polinomio "cero", definido precisamente por el 0 de A, esto es, el polinomio tal que $0(n)=\delta_{0,n}0=0$ para todo $n\in\mathbb{N}$. En otras palabras, la aplicación constantemente cero: $f+0=f$ pues, $\forall\, n\in\mathbb{N}$,

$$(f+0)(n)=f(n)+0=f(n).$$

• Todo polinomio f tiene un opuesto $-f$, que es definido por $(-f)(n)=-f(n)$, $\forall n\in\mathbb{N}$: $f+(-f)=0$ pues, $\forall\, n\in\mathbb{N}$,

$$(f+(-f))(n)=f(n)-f(n)=0.$$

• La producto es asociativo: $f(gh)=(fg)h$ pues, $\forall\, n\in\mathbb{N}$,

$$\begin{aligned}(f(gh))(n)&=\sum_{i+m=n}f(i)(gh)(m)=\sum_{i+m=n}f(i)\sum_{j+k=m}g(j)h(k)\\&=\sum_{i+m=n}\sum_{j+k=m}f(i)(g(j)h(k))=\sum_{i+j+k=n}f(i)(g(j)h(k)).\end{aligned}$$

$$\begin{aligned}((fg)h)(n)&=\sum_{m+k=n}(fg)(m)h(k)=\sum_{m+k=n}\Big(\sum_{i+j=m}f(i)g(j)\Big)g(k)\\&=\sum_{m+k=n}\sum_{i+j=m}(f(i)(g(j))h(k)=\sum_{i+j+k=n}(f(i)g(j))h(k).\end{aligned}$$

y el resultado se deduce por comparación, teniendo en cuenta la asociatividad en A.

• Hay un polinomio "uno", definido precisamente por el 1 de A, esto es el polinomio que $1(n)=\delta_{0,n}1=\delta_{0,n}$ para todo $n\in\mathbb{N}$: $f1=f$ pues, $\forall\, n\in\mathbb{N}$,

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

• se verifica la distributividad: $f(g+h)=fg+fh$ pues, $\forall\, n\in\mathbb{N}$,

$$\begin{aligned}(f(g+h))(n)&=\sum_{i+j=n}f(i)(g(j)+h(j))=\sum_{i+j=n}f(i)g(j)+f(i)h(j)\\&=\sum_{i+j=n}f(i)g(j)+\sum_{i+j=n}f(i)h(j)=(fg)(n)+(fh)(n)=(fg+fh)(n).\end{aligned}$$

Vamos a darle un aspecto que os sea más familiar a los polinomios de $A[x]$.

Lema 2.7.2. *Para cualquier $a \in A$ y $m \geq 0$, ax^m es el polinomio con todos los coeficientes de grados distintos de m nulos y cuyo coeficiente en grado m es a. Esto es, $\forall\, n \in \mathbb{N}$,*

$$(ax^m)(n) = a\delta_{m,n} = \begin{cases} a & si \quad n = m, \\ 0 & si \quad n \neq m. \end{cases}$$

Demostración. Consideremos primero el caso en que $a = 1$. Esto es, probemos que, $x^m(n) = \delta_{m,n}$, por inducción en m. Si $m = 0$, efectivamente, $x^0(n) = 1(n) = \delta_{0,n}$. Y, supuesto para m,

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

y para $n \geq 1$

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

Finalmente, para cualquier $a \in A$, $(ax^m)(n) = \sum_{i+j=n} a(i)x^m(j) = a(0)x^m(n) = a\delta_{m,n}$. □

Naturalmente, un polinomio $f \in A[x]$ es conocido por sus coeficientes en cada grado $f(0)$, $f(1)$, etc. El siguiente resultado nos lleva a la representación familiar de los polinomios

Proposición 2.7.3. *Sea $f \in A[x]$ el polinomio con coeficientes $f(n) = a_n$, $n \geq 0$, entonces*

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

(notar que la suma es finita, pues existe un r tal que $a_m = 0$ para todo $m > r$)

Demostración. Para cualquier $n \in \mathbb{N}$,

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

Notemos que, bajo esa representación de los polinomios, las operaciones de suma y producto se realizan a modo "familiar":

$$\sum_{m\geq 0} a_m x^m + \sum_{m\geq 0} b_m x^m = \sum_{m\geq 0} a_m x^m + b_m x^m = \sum_{m\geq 0} (a_m + b_m)x^m.$$

$$\sum_{j\geq 0} a_m x^m \sum_{m\geq 0} b_m x^m = \sum_{i,j\geq 0} a_i x^i b_j x^j = \sum_{i,j\geq 0} a_i b_j x^{i+j} = \sum_{m\geq 0} \Big(\sum_{i+j=m} a_i b_j\Big) x^m.$$

Por ejemplo, si $f = -3 + 3x + 3x^7$ y $g = 3 + 2x$ son polinomios en $\mathbb{Z}_4[x]$,

$$f + g = 1 + 3x + 3x^7 + 3 + 2x = (1 + 3) + (3 + 2)x + 3x^7 = 0 + 1x + 3x^7 = x + 3x^7.$$

$$fg = (1 + 3x + 3x^7)(3 + 2x) = 3 + 2x + x + 2x^2 + x^7 + 2x^8 = 3 + 3x + 2x^2 + x^7 + 2x^8.$$

Notas.(1) Observar que los polinomios de $A[x]$ cuyos coeficientes en grados > 0 son todos nulos, son precisamente los elementos $a \in A$. Así $A \subseteq A[x]$ y es de hecho un subanillo.

(2) Debido a la expresión de un polinomio $f \in A[x]$ con coeficientes a_m, $m \geq 0$, en la forma $f = \sum_{m\geq 0} a_m x^m$, se suele de notar el polinomio como $f(x)$, haciendo alusión al símbolo x que denota la indeterminada.

2.8 Homomorfismos

Los anillos se relacionan entre sí mediante '*homomorfismos*" , que son aplicaciones entre ellos que respetan las correspondientes operaciones. Más precisamente,

Definición 2.8.1. *Sean A y A' dos anillos conmutativos. Un homomorfismo de A en A', es una aplicación $\phi : A \to A'$, de dominio A y rango A', tal que*

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

Se deducen directamente de los axiomas que estos homomorfismos preservan sumas y productos reiterados, así como el cero, opuestos e inversos (si los hay):

- $\phi(\sum_{i=1}^n a_i) = \sum_{i=1}^n \phi(a_i)$.
- $\phi(\prod_{i=1}^n a_i) = \prod_{i=1}^n \phi(a_i)$.
- $\phi(0) = 0$.
- $\phi(-a) = -\phi(a)$.
- $\phi(na) = n\phi(a) \quad (n \in \mathbb{Z})$.
- $\phi(a^n) = \phi(a)^n \quad (n \in \mathbb{N})$.
- Si $a \in U(A)$, entonces $\phi(a) \in U(B)$ y $\phi(a^{-1}) = \phi(a)^{-1}$.
- Si $a \in U(A)$, $\phi(a^n) = \phi(a)^n \quad (n \in \mathbb{Z})$.

Las dos primeras se demuestran por una simple inducción. Para la tercera, podemos proceder así: $\phi(0) = \phi(0+0) = \phi(0) + \phi(0)$, luego

$$0 = \phi(0) - \phi(0) = \phi(0) + \phi(0) - \phi(0) = \phi(0) + 0 = \phi(0).$$

Y para la cuarta: $\phi(a) + \phi(-a) = \phi(a-a) = \phi(0) = 0$, luego $\phi(-a) = -\phi(a)$. Para la última: $1 = \phi(1) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}$, luego $\phi(a) \in U(A')$ y $\phi(a)^{-1} = \phi(a^{-1})$.

- Si $\phi : A \to B$ y $\psi : B \to C$ son homomorfismos, entonces la aplicación compuesta $\psi\phi : A \to B$ es también un homomorfismo. Además la aplicación identidad $Id_A : A \to A$ es siempre un homomorfismo.

El reconocer que una aplicación entre anillos es un homomorfismo es importante, pues permite calcular la imagen de un elemento que se obtiene a partir de otros por operaciones de sumar, restar y multiplicar mediante dos formas: Bien efectuando el cálculo en el anillo dominio y luego la imagen del resultado, o bien calculando las imágenes de los elementos involucrados y hacer luego el correspondiente cálculo en el anillo rango. Por ejemplo, para cada $n \geq 2$, la aplicación

$$R : \mathbb{Z} \to \mathbb{Z}_n,$$

que asigna a cada entero su resto al dividirlo por n, es un homomorfismo de anillos, pues ya sabemos que, para cualesquiera enteros $a, b \in \mathbb{Z}$, $R(a+b) = R(a) + R(b)$, $R(ab) = R(a)R(b)$ y, es claro que $R(1) = 1$. Supongamos, para ilustrar esto, que $n = 5$ y queremos calcular $R(12^3)$. Podemos calcular 12^3 en $\mathbb{Z}$, y entonces dividir el resultado por 5 y determinar ese resto. Pero también podemos utilizar que R es un homomorfismo:

$$R(12^3) = R(12)^3 = 2^3 = 3.$$

Fácilmente se observa que, para cualquier homomorfismo $\phi : A \to B$, su imagen

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

es un subanillo de B, nos referimos a él como "*subanillo imagen de* ϕ". Si ϕ es una aplicación sobreyectiva, esto es, si $Img(\phi) = B$, se dice que es un "*epimorfismo*". Por ejemplo, los homomorfismos $R : \mathbb{Z} \to \mathbb{Z}_n$ son epimorfismos, pues para todo $r \in \mathbb{Z}_n$, $r = R(r)$. Si el homomorfismo es inyectivo ($x \neq y \Rightarrow \phi(x) \neq \phi(y)$), se le llama "*monomorfismo*". Por ejemplo, la aplicación $\eta : \mathbb{Z} \to \mathbb{Q}$ tal que $\eta(n) = \frac{n}{1}$ es un monomorfismo.

Definición 2.8.2. *Un isomofismo de anillos es un homomorfismo $\phi : A \to B$ que tiene un inverso, esto es, tal que existe otro morfismo $\phi^{-1} : B \to A$ que cumple $\phi\phi^{-1} = Id_B$ y $\phi^{-1}\phi = 1d_A$.*

Los isomorfismos de anillos son los homomorfismos biyectivos, como nos indica la siguiente

Proposición 2.8.3. *Un homomorfismo $\phi : A \to A'$ de anillos es un isomorfismo si, y sólo si, la aplicación phi es biyectiva.*

Demostración. Claramente si ϕ es isomorfismo entonce como aplicación es biyectiva por tener un inverso. Recíprocamente, si ϕ es un morfismo, que como aplicación es biyectiva, la aplicación inversa $\phi^{-1} : A' \to A$ es también un isomorfismo, en efecto:

Sean $a'_1, a'_2 \in A'$, y supongamos que $\phi^{-1}(a'_i) = a_i$, de manera que $\phi(a_i) = a'_i$. Entonces $a'_1 + a'_2 = \phi(a_1) + \phi(a_2) = \phi(a_1 + a_2)$ y $a'_1 a'_2 = \phi(a_1)\phi(a_2) = \phi(a_1 a_2)$. Luego $\phi^{-1}(a'_1 a'_2) = a_1 + a_2 = \phi^{-1}(a'_1) + \phi^{-1}(a'_2)$ y $\phi^{-1}(a'_1 a'_2) = a_1 a_2 = \phi^{-1}(a'_1)\phi^{-1}(a'_2)$. Claramente también $\phi^{-1}(1) = 1$. Así que, $\phi^{-1} : A' \cong A$ es un isomorfismo. ■

Diremos que dos anillos A y A' son isomorfos si existe un isomorfismo $\phi : A \to A'$ entre ellos. En este caso, los anillos A y A' son *esencialmente* iguales, pues ϕ y ϕ^{-1} son diccionarios univocos e inversos que nos permiten trasladar cualquier calculo o resultado obtenido en uno de ellos mediante sus operaciones al otro. Escribiremos $A \cong A'$ cuando dos anillos sean isomorfos.

Los anillos de polinomio $A[x]$ tienen una propiedad muy importante (se conoce como su "*propiedad universal*"), que se expresa como sigue.

Teorema 2.8.4. *Sean A, B anillos conmutativos y $\phi : A \to B$ un homomorfismo. Para cualquier $b \in B$ existe un único homomorfismo $\Phi : A[x] \to B$ tal que*

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

2. $\Phi(x) = b$.

Demostración. Solo puede existir un tal homomorfismo, pues para cualquier polinomio $f(x) = \sum_{m \geq 0} a_m x^m$ ha de ser

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

Y existe, pues propuesto de esta forma, vemos que

$$\begin{aligned}\Phi\Big(\sum_{m\geq 0} a_m x^m\Big)\Phi\Big(\sum_{m\geq 0} a'_m x^m\Big) &= \Big(\sum_{m\geq 0}\phi(a_m)b^m\Big)\Big(\sum_{m\geq 0}\phi(a'_m)b^m\Big) = \sum_{i,j\geq 0}\phi(a_i)b^i\phi(a'_j)b^j\\ &= \sum_{i,j\geq 0}\phi(a_i)\phi(a'_j)b^{i+j} = \sum_{m\geq 0}\Big(\sum_{i+j=m}\phi(a_i)\phi(a'_j)\Big)b^m\\ &= \sum_{m\geq 0}\phi\big(\sum_{i+j=m} a_i a'_j\big)b^m = \Phi\Big(\sum_{m\geq 0}\big(\sum_{i+j=m} a_i a'_j\big)x^m\Big)\\ &= \Phi\Big(\sum_{m\geq 0} a_m x^m \sum_{m\geq 0} a'_m x^m\Big),\end{aligned}$$

$$\begin{aligned}\Phi\Big(\sum_{m\geq 0} a_m x^m + \sum_{m\geq 0} a'_m x^m\Big) &= \Phi\Big(\sum_{m\geq 0}(a_m + a'_m)x^m\Big) = \sum_{m\geq 0}\phi(a_m + a'_m)b^m\\ &= \sum_{m\geq 0}\Big(\phi(a_m)b^m + \phi(a'_m)b^m\Big) = \sum_{m\geq 0}\phi(a_m)b^m + \sum_{m\geq 0}\phi(a'_m)b^m\\ &= \Phi\Big(\sum_{m\geq 0} a_m x^m\Big) + \Phi\Big(\sum_{m\geq 0} a'_m x^m\Big),\end{aligned}$$

y, claramente, verifica que $\Phi(a) = \phi(a)$, para $a \in A$, y en particular $\Phi(1) = \phi(1) = 1$, y $\Phi(x) = b$. ■

Si $A \subseteq B$ es un subanillo, y $\phi = in : A \to B$ es la inclusión, $a \mapsto a$, resulta que, para cada $b \in B$, existe un único homomorfismo de anillos, al que denotaremos

$$E_b : A[x] \to B$$

y llamaremos el "*homomorfismo de evaluación en b*", tal que $E_v(a) = a$, para todo $a \in A$, y $E_b(x) = b$. Si $f(x) = \sum_{m\geq 0} a_m x^m$, entonces

$$E_b(f(x)) = \sum_{m\geq 0} a_i b^m,$$

y debido a tal expresión, se denota $E_b(f(x)) = f(b)$, que leemos como "*el resultado de evaluar $f(x)$ en b*". Si $f(b) = 0$, se dice que b es una "*raíz de $f(x)$ en B*".

Unos ejemplos,

1. Si $f(x) = 2 + x^2 \in \mathbb{Z}[x]$ y consideramos $\frac{1}{2} \in \mathbb{Q}$, entonces $f(\frac{1}{2}) = 2 + (\frac{1}{2})^2 = 2 + \frac{1}{4} = \frac{9}{4}$.
2. Si $f(x) = 1 + 2x + x^2$, entonces $f(-1) = 1 - 2 + 1 = 0$. Así que -1 es una raíz del polinomio en $\mathbb{Z}$.
3. Si $f(x) = (x^2+1)^2 + (x-1)^2 \in \mathbb{Z}[x]$ y consideramos el complejo $i = \sqrt{-1} \in \mathbb{C}$, podemos calcular $f(i)$ de ds formas.
   (a) Como $f(x) = 1+2x^2+x^4+x^2-2x+^1 = 2-2x+3x^2+x^4$, será $f(i) = 2-2i-3+1 = -2i$.
   (b) $f(i) = (i^2+1)^2 + (i-1)^2 = (-1+1)^2 + (i^2 - 2i + 1 = -2i$.

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 la "*función polinómica definida por el polinomio* $f(x)$. Es importante no confundir la función polinómica con el polinomio, como muestra este ejemplo: Sean los polinomios de $\mathbb{Z}_2[x]$, $f(x) = 1 + x$ y $g(x) = 1 + x^2$. Sus correspondientes funciones polinómicas $f(x), g(x) : \mathbb{Z}_2 \to \mathbb{Z}_2$, funcionan así: $f(0) = 1 = g(0)$, $f(1) = 0 = g(1)$, esto es, son la misma! y los polinomios distintos.