# Teoría de Anillos

José Luis Tábara

jltabara@gmail.com

## Índice

# 1. Definiciones básicas

**Definición 1.1** *Un* anillo *$A$ es un conjunto dotado de dos operaciones, llamadas* suma *$(+)$ y* producto *$(\cdot)$ que cumplen:*

- *$(A, +)$ es un grupo abeliano.*
- *El producto es asociativo: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para todo $a, b, c$ de $A$.*
- *El producto es distributivo respecto a la suma*

$$(a + b) \cdot c = a \cdot c + b \cdot c \quad y \quad a \cdot (b + c) = a \cdot b + a \cdot c$$

En principio un anillo debería ser denotado por $(A, +, \cdot)$ para hacer clara referencia a las operaciones. Sin embargo nosotros seguiremos el convenio habitual y lo denotaremos simplemente por $A$.

Si el producto es conmutativo, el anillo se llama conmutativo. En el caso en que la operación producto tenga elemento neutro, el anillo se dirá que es un anillo con unidad. La unidad del anillo se denotará siempre por 1 y cumple

$$a \cdot 1 = 1 \cdot a = a$$

El elemento neutro para la suma se denota por 0 y el opuesto de $a$ para esta operación es $-a$. También es costumbre denotar el producto por la yuxtaposición y suprimir el punto. Así $ab$ significa el producto de $a$ por $b$ en el orden indicado.

En todo grupo abeliano $(G, +)$ se puede introducir una estructura de anillo definiendo $ab = 0$ para todos los elementos de $G$. Decimos en este caso que es un anillo trivial. Nosotros siempre supondremos que los anillos no son triviales. En el caso en que el grupo este formado por solo un elemento diremos que el anillo es el anillo cero y se suele denotar por 0. Este es el único anillo trivial que consideraremos.

**Proposición 1.1** *Dado un anillo $A$, se cumple:*

- $(a - b)c = ac - bc \quad y \quad a(b - c) = ab - ac$

- $0a = a0 = 0$
- $(-a)b = a(-b) = -(ab)$
- $(-a)(-b) = ab$
- $(-1)a = -a$

**Demostración.**

Demostraremos la primera afirmación y dejamos el resto para el lector, que debe utilizar razonamientos similares. Aplicando los axiomas

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

Sumamos a cada miembro $-bc$ y conseguimos pasar $bc$ al otro lado de la igualdad con el signo contrario. □

**Corolario 1.2** *Un anillo $A$ con más de un elemento no es trivial si $1 \neq 0$.*

Si $n$ es un entero positivo $na$ es la suma de $n$ veces el elemento $a$

$$na = a + \overset{n)}{\cdots} + a$$

Si $n$ es negativo entonces definimos

$$na = -a - \overset{-n)}{\cdots} - a$$

**Proposición 1.3** *Si $m, n \in \mathbb{Z}$ y $a, b \in A$ se cumple:*

- $(m+n)\, a = ma + na.$
- $(mn)\, a = m(na) = n(ma).$
- $m(a+b) = ma + mb.$
- $1a = a.$

**Demostración.**

Al lector. □

**Observación.** Estas propiedades demuestran que todo anillo tiene una estructura natural de módulo sobre anillo de los enteros. □

**Ejemplos**

- $\mathbb{Z}$ con la suma y el producto habitual es un anillo conmutativo y con unidad. Asimismo $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ son anillos.
- Si $n$ es un número natural el conjunto $n\mathbb{Z}$ de los múltiplos de $n$ es un anillo conmutativo sin elemento unidad.
- Sea $A$ un anillo y $X$ un conjunto cualquiera. Consideramos el conjunto $\mathrm{Apli}(X, A)$ que está constituido por las aplicaciones $f : X \to A$. Dadas dos funciones $f$ y $g$ de $X$ en $A$ definimos su suma y su producto por las fórmulas:

$$\begin{aligned} (f+g)(x) &= f(x)+g(x) \\ (f\cdot g)(x) &= f(x)\cdot g(x) \end{aligned}$$

  Con estas operaciones, $\mathrm{Apli}(X, A)$ es un anillo. Si $A$ es conmutativo, también lo es este anillo, y si $A$ tiene unidad, la función que a todo elemento de $X$ le hace corresponder la unidad de $A$ es el elemento neutro de $\mathrm{Apli}(X, A)$.
- Si $A$ es un anillo, el conjunto $M_2(A)$ de las matrices $2\times 2$ con elementos en $A$ es un anillo con las operaciones matriciales:

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} + \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} = \begin{pmatrix} a_1+b_1 & a_2+b_2 \\ a_3+b_3 & a_4+b_4 \end{pmatrix}$$

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} = \begin{pmatrix} a_1b_1+a_2b_3 & a_1b_2+a_2b_4 \\ a_3b_1+a_4b_3 & a_3b_2+a_4b_4 \end{pmatrix}$$

Si $A$ tiene unidad, este anillo tiene unidad, siendo ésta la matriz identidad

$$\mathrm{Id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Pero aunque el anillo sea conmutativo, las matrices no forman un anillo conmutativo. Puede comprobar el lector que las matrices

$$\begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$$

no conmutan en general, siendo $a$ y $b$ elementos del anillo $A$. Este ejemplo se puede generalizar para matrices cuadradas de orden $n$.

- Si $G$ es un grupo abeliano, el conjunto de sus endomorfismos es un anillo. La suma, es la suma como aplicaciones y el producto la composición de aplicaciones. La unidad es el endomorfismo identidad y en general el anillo no será conmutativo.

- Si $E$ es un espacio vectorial, el conjunto de las aplicaciones lineales de $E$ en $E$ es un anillo, que denotamos $\mathrm{End}(E)$.

- Si $A$ y $B$ son anillos, introducimos en el producto cartesiano $A \times B$ las operaciones:

$$\begin{aligned} (a,b) + (a',b') &= (a+a', b+b') \\ (a,b) \cdot (a',b') &= (aa', bb') \end{aligned}$$

  $A \times B$ es un anillo, llamado producto directo de los anillos $A$ y $B$.

- Sea $\mathbb{Z}(i)$ el conjunto de números complejos cuya parte real e imaginaria son números enteros:

$$\mathbb{Z}(i) = \{a + ib \text{ con } a, b \in \mathbb{Z}\}$$

  Si en $\mathbb{Z}(i)$ consideramos las operaciones habituales como números complejos, tendremos un anillo conmutativo y con unidad denominado ani-

llo de los enteros de Gauss.

- Si $X$ es un espacio topólogico, el conjunto $C(X, \mathbb{R})$ de las funciones continuas de $X$ en $\mathbb{R}$ es un anillo con la suma y el producto funcional. Para probarlo debemos recordar que la suma y el producto de dos funciones continuas es continua.

En general y salvo que se diga lo contrario, siempre supondremos que los anillos son conmutativos y tienen unidad.

**Definición 1.2** *Sea $A$ un anillo con unidad. Decimos que un elemento $a \in A$ es una* unidad *si existe otro elemento $b$ tal que $ab = ba = 1$. El conjunto de unidades de $A$ se denota $U(A)$.*

Si el anillo es conmutativo, basta imponer solo la condición $ab = 1$. El elemento $b$, que se demuestra fácilmente que es único (problema 1.3), se denota por $a^{-1}$ y se dice que es el inverso de $a$. Como sabemos por la proposición 1.1 el cero nunca es invertible.

**Proposición 1.4** *Las unidades de un anillo forman un grupo respecto a la multiplicación.*

**Demostración.**

$1 \in U(A)$ de modo evidente. Si $a$ y $b$ son invertibles, su producto también admite inverso. El inverso de $ab$ es $b^{-1}a^{-1}$. Si $a$ es invertible, $a^{-1}$ también lo es, siendo su inverso el mismo $a$. $\square$

**Ejemplos**

- Las unidades de $\mathbb{Z}$ son $\{1, -1\}$.
- En $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ cualquier número no nulo es invertible.
- Las unidades de $\mathbb{Z}(i)$ son $\{1, -1, i, -i\}$.

- Si $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ es una matriz con coeficientes en $A$, definimos su determinante como el elemento de $A$

$$\det(M) = ad - bc$$

  Se demuestra, siguiendo el mismo esquema que en álgebra lineal, que la matriz $M$ es invertible si y solo si su determinante es una unidad de $A$.

- Las unidades de $C(X, \mathbb{R})$ son las funciones que no son nunca nulas. Esto es así debido a que $1/f$ es continua si $f$ nunca es nula.

Entre los anillos, existen unos muy especiales. Son aquellos donde además del concepto de multiplicación, existe un concepto de división. Denotamos por $A^*$ al conjunto $A - \{0\}$ de los elementos no nulos de $A$.

**Definición 1.3** *Un anillo $A$ donde todo elemento de $A^*$ es una unidad, se llama* anillo con división*. Si el anillo con división es conmutativo se denomina* cuerpo*.*

Hemos tenido que eliminar el 0 de nuestra definición, puesto que nunca puede ser invertible, debido a que $a \cdot 0 = 0$ para todo elemento $a$.

**Ejemplos**

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ son cuerpos.

- $\mathbb{Q}(i)$ es un cuerpo. Esta formado por los números complejos cuya parte real e imaginaria son fracciones.

- Sea $\mathbb{Q}(\sqrt{2})$ el conjunto de números reales que se pueden escribir en la forma $a + b\sqrt{2}$ donde $a$ y $b$ son racionales. Este anillo es un cuerpo. Lo puede probar el lector directamente, o remitirse al problema 4.9 para una demostración más elegante.

**Definición 1.4** *Un elemento $a \in A$ es un* divisor de cero *si existe otro elemento $b$ de tal modo $ab = 0$.*

En propiedad, si el anillo no es conmutativo deberían diferenciarse divisores de cero por la derecha y por la izquierda.

**Definición 1.5** *Un anillo sin divisores de cero se denomina* anillo íntegro.

En un anillo íntegro se pueden simplificar factores. Si $ab = ac$ y $a \neq 0$ entonces $b = c$. Para demostralo escribimos $ab - ac = 0$ y sacamos factor común, $a(b-c) = 0$ y como $a \neq 0$ concluimos que $b - c = 0$. Decimos que en un anillo se cumple la ley de cancelación si se pueden simplificar factores.

**Ejemplos**

- Todo cuerpo es un anillo íntegro.
- $\mathbb{Z}$ es íntegro.
- En general todo anillo que esté contenido en $\mathbb{C}$ es íntegro.
- $M_2(A)$ no es íntegro. Por ejemplo

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

- El producto directo de dos anillos no nulos nunca es íntegro.
- El anillo $C(\mathbb{R}, \mathbb{R})$ no es íntegro. Sea $f$ una función que se anula para $x \geq 0$ y $g$ una función que se anula para $x \leq 0$. Su producto se anula en todo $\mathbb{R}$.

**Proposición 1.5** *Todo anillo íntegro y finito es un anillo con división.*

**Demostración.**

Sea $A$ íntegro y finito. Consideremos un elemento cualquiera $a \in A$. Tenemos la aplicación

$$\begin{array}{rccc} \lambda_a & : A & \longrightarrow & A \\ & b & \longrightarrow & ab \end{array}$$

La ley de cancelación prueba que $\lambda_a$ es inyectiva. Como el conjunto es finito, también es epiyectiva. Así 1 pertenece a la imagen de $\lambda_a$ y entonces existe un elemento $b$ tal que $ab = 1$. $\square$

Existe un resultado, llamado teorema de Wedderburn, que afirma incluso más: Todo anillo con división con un número finito de elementos es necesariamente conmutativo. Por lo tanto todo anillo íntegro y finito es un cuerpo. Este teorema no lo demostraremos en estas notas.

**Definición 1.6** *Si $A$ es un anillo, un subconjunto $B$ es un* subanillo *si con las operaciones inducidas $B$ posee estructura de anillo. Si $1 \in B$ diremos que $B$ es un* subanillo con unidad.

Naturalmente todo subanillo es un anillo con las operaciones inducidas.

**Proposición 1.6** *Un subconjunto $B \subset A$ es un subanillo si y solo si $a, b \in B$ implica que $a - b \in B$ y $ab \in B$.*

**Demostración.**

Si $a - b \in B$ entonces $B$ es un subgrupo aditivo. Si $ab$ también pertenece, la operación producto es cerrada y cumple las propiedades asociativa y distributiva, puesto que se cumplen para todos los elementos de $A$. $\square$

Los subanillos pueden contener o no a la unidad. También puede ocurrir que un subanillo de un anillo no conmutativo, sea conmutativo.

**Ejemplos**

- En todo anillo $A$, el conjunto $A$ y el 0 son subanillos, llamados subanillos triviales. Los demás subanillos se llaman propios.
- $\mathbb{Z}$ es subanillo de $\mathbb{Q}$, de $\mathbb{R}$ y de $\mathbb{C}$.
- Si $X$ es un espacio topológico, el conjunto $C(X, \mathbb{R})$ de aplicaciones continuas es un subanillo del conjunto $\mathrm{Apli}(X, \mathbb{R})$ de todas las funciones de $X$ en $\mathbb{R}$.

- Los múltiplos $n\mathbb{Z}$ de un entero $n$ forman un subanillo sin unidad de $\mathbb{Z}$.
- Sea $A$ un anillo, posiblemente no conmutativo. Llamamos centro de $A$ y denotamos por Centro($A$) al conjunto de elementos de $A$ que conmutan con todos los elementos del anillo:

$$\text{Centro}(A) = \{a \in A \text{ tales que } ar = ra \text{ para todo } r \in A\}$$

  El centro de un anillo es un subanillo. Además siempre es conmutativo.

**Proposición 1.7** *La intersección de subanillos es un subanillo.*

**Demostración.**

Sea $B_i$ donde $i \in I$ una colección, posiblemente infinita, de subanillos de $A$. Si $a, b \in \bigcap_{i\in I} B_i$ entonces $a$ y $b$ pertenecen a $B_i$ para todo $i$. Como los conjuntos dados son subanillos tenemos que $a - b \in B_i$ y $ab \in B_i$ para todo $i$. Tanto la suma como el producto de elementos de la intersección siguen perteneciendo a la intersección. Concluimos que $\bigcap_{i\in I} B_i$ es un subanillo. Si todos los subanillos tienen unidad, su intersección también. □

**Definición 1.7** *Sea $S$ un subconjunto de $A$. A la intersección de todos los subanillos que contienen a $S$ se le llama* subanillo generado *por el subconjunto $S$.*

Para el estudio de los subanillos generados nos remitimos al capítulo 4 que trata sobre polinomios.

**Ejemplos**

- $\mathbb{Z}$ es un subanillo de $\mathbb{Q}$, de $\mathbb{R}$ y de $\mathbb{C}$.
- El conjunto $n\mathbb{Z}$ de los múltiplos de $n$ es un subanillo de $\mathbb{Z}$ que no tiene unidad.

- La intersección de los subanillos $2\mathbb{Z}$ y $3\mathbb{Z}$ es precisamente $6\mathbb{Z}$, pues un número es múltiplo de 2 y de 3 precisamente cuando es múltiplo de 6. En general $n\mathbb{Z} \cap m\mathbb{Z} = d\mathbb{Z}$, siendo $d$ el mínimo común múltiplo de $n$ y $m$.

- En el conjunto de matrices cuadradas de orden $n$ y con elementos en un anillo $A$, el conjunto de las matrices diagonales es un subanillo. Del mismo modo, el conjunto de matrices triangulares superiores es otro subanillo.

- El menor subanillo de $\mathbb{C}$ que contiene tanto a $\mathbb{Z}$ como a $i$ es justamente el anillo $\mathbb{Z}(i)$.

- Los subanillos de $\mathbb{Z}$ son precisamente los conjuntos de la forma $n\mathbb{Z}$. Sabemos por teoría de grupos que estos son los únicos subgrupos y es fácil comprobar que también son subanillos.

**Definición 1.8** *Sean $A$ y $A'$ dos anillos. Una aplicación $\varphi : A \to A'$ es un* morfismo de anillos *si cumple:*

- $\varphi(a + b) = \varphi(a) + \varphi(b)$
- $\varphi(ab) = \varphi(a) \cdot \varphi(b)$

*Si además se cumple:*

- $\varphi(1) = 1$

*diremos que es un* morfismo de anillos con unidad.

De ahora en adelante cuando utilicemos la palabra morfismo, entenderemos que es un morfismo de anillos con unidad.

Como un morfismo es también morfismo de grupos se cumple $\varphi(0) = 0$ y $\varphi(-a) = -\varphi(a)$. Además $\varphi$ será inyectivo si y solo si su núcleo es nulo.

**Proposición 1.8** *La composición de morfismos es morfismo. Si $\varphi : A \to A'$ es un morfismo biyectivo, entonces $\varphi^{-1} : A' \to A$ es también morfismo.*

**Demostración.**

Sean $\varphi : A \to A'$ y $\varphi : A' \to A''$ morfismos. Entonces

$$(\varphi'\varphi)(a+b) = \varphi'(\varphi(a+b)) = \varphi'(\varphi(a) + \varphi(b)) = \\ \varphi'(\varphi(a)) + \varphi'(\varphi(b)) = (\varphi'\varphi)(a) + (\varphi'\varphi)(b)$$

Análogamente con las otras propiedades.

Para demostrar la segunda afirmación utilizamos que $\varphi$ es un morfismo de grupos biyectivo y por lo tanto $\varphi^{-1}$ es morfismo de grupos. Del mismo modo se prueba que conserva el producto y la unidad. □

**Definición 1.9** *Un* isomorfismo $\varphi : A \to A'$ *es un morfismo biyectivo. Si* $A = A'$ *los isomorfismos se denominan* automorfismos *del anillo* $A$*. Dos anillos entre los que exista un isomorfismo, se dirá que son* isomorfos*. El conjunto de todos los automorfismos del anillo se denotará* $\mathrm{Aut}(A)$*.*

**Corolario 1.9** *El conjunto de automorfismos de un anillo forma un grupo respecto a la composición.*

**Ejemplos**

- Sea $B$ un subanillo de $A$. La inyección canónica $i : B \to A$ es morfismo.
- Sea $X$ un conjunto y $x \in X$ un punto determinado de $X$. A cada aplicación $f : X \to \mathbb{R}$ le hacemos corresponder el número real $f(x)$. Tenemos así construido una aplicación $\varphi_x$ de $\mathrm{Apli}(X, \mathbb{R})$ en $\mathbb{R}$. Resulta que $\varphi_x$ es un morfismo.
- Consideremos el anillo de los enteros de Gauss $\mathbb{Z}(i)$. La conjugación compleja

$$\begin{array}{rccc} \varphi & : \mathbb{Z}(i) & \longrightarrow & \mathbb{Z}(i) \\ & a + ib & \longrightarrow & a - ib \end{array}$$

  es un morfismo.

- Un morfismo de anillos con unidad $\varphi : A \to A'$ transforma elementos invertibles de un anillo en elementos invertibles del conjunto imagen (problema 1.18). De esta manera se induce un morfismo de grupos $\varphi : U(A) \to U(A')$ entre las unidades de los anillos.

- Si $A$ es un anillo arbitrario, existe un único morfismo de $\mathbb{Z}$ en $A$. Dicho morfismo se llama característica y se representa por $ch : \mathbb{Z} \to A$. Naturalmente debe de cumplir:

  $$ch(1) = 1 \Rightarrow ch(n) = n \cdot 1$$

  lo que prueba su unicidad.

  Como $ch$ es morfismo, en particular es morfismo de grupos. Su núcleo será de la forma $n\mathbb{Z}$ donde $n$ es un número natural. Al natural definido por la fórmula

  $$\mathrm{Ker}(ch) = n\mathbb{Z}$$

  se le denomina característica del anillo $A$. Si $ch$ es inyectivo decimos que la característica del anillo es nula.

- Sea $A = C(\mathbb{R}, \mathbb{R})$ y sea $f$ una función. La aplicación

  $$\begin{array}{rccc} \phi_f & : A & \longrightarrow & A \\ & g & \longrightarrow & gf \end{array}$$

  es un morfismo de anillos.

**Proposición 1.10** *Sea $\varphi : A \longrightarrow A'$ un morfismo de anillos. Si $B \subset A$ es subanillo, entonces $\varphi(B)$ es subanillo. Si $B' \subset A'$ es subanillo, $\varphi^{-1}(B')$ es subanillo.*

**Demostración.**

Tenemos que $\varphi(a-b) = \varphi(a) - \varphi(b)$ y $\varphi(ab) = \varphi(a)\,\varphi(b)$ puesto que $\varphi$ es morfismo. Si tanto $a$ como $b$ son elementos del subanillo $B$, concluimos por la proposición 1.6 que $\varphi(B)$ es subanillo. La demostración del otro resultado es análoga. □

## Problemas

**1.1** Verificar si son anillos o no lo son los conjuntos que a continuación se indican. Las operaciones son las habituales. Indicar si son conmutativos y si tienen unidad.

- Los enteros pares $2\mathbb{Z}$.
- Los racionales positivos $\mathbb{Q}^+$.
- El conjunto $\mathbb{Z}(\sqrt{-5})$ formado por los números complejos de la forma $a + b\sqrt{-5}$ donde $a$ y $b$ son números enteros.
- El conjunto $C^\infty(\mathbb{R}, \mathbb{R})$ de las funciones infinitamente diferenciables.
- El conjunto $\mathcal{P}(X)$ de las partes de un conjunto $X$ donde la suma es la diferencia simétrica y el producto la intersección. Recordemos que la diferencia simétrica de dos subconjuntos es $A \triangle B = (A - B) \cup (B - A)$.

**1.2** Definimos en $\mathbb{Z}$ una nueva suma y una nueva multiplicación por las fórmulas

$$a * b = a + b + 1 \qquad a \circ b = a + b + ab$$

Demostrar que $\mathbb{Z}$ es un anillo con esas nuevas operaciones.

**1.3** Demostrar la unicidad del elemento neutro para la multiplicación. Demostrar la unicidad del elemento inverso.

**1.4** Utilizando inducción demostrar:

- $x(y_1 + \cdots + y_n) = xy_1 + \cdots + xy_n$
- La expresión anterior puede escribirse

$$x\Big(\sum_{i=1}^{n} y_i\Big) = \sum_{i=1}^{n} xy_i$$

Volviendo a utilizar inducción probar la ley distributiva para un número arbitrario de sumandos.

$$\Big(\sum_{i=1}^{n} x_i\Big)\Big(\sum_{j=1}^{m} y_j\Big) = \sum_{i=1}^{n}\sum_{j=1}^{m} x_i y_j$$

**1.5** Demostrar que en un anillo se cumplen las propiedades de las potencias ($n$ y $m$ son enteros positivos):

$$(a^n)^m = a^{nm}, \quad a^n a^m = a^{n+m}, \quad (ab)^n = a^n b^n \text{ si } a, b \text{ conmutan}$$

Si los elementos del anillos son invertibles probar las propiedades en el caso general ($n$ y $m$ enteros no necesariamente positivos).

**1.6** Sea $p$ un número primo prefijado de antemano. Sea $A$ el subconjunto de $\mathbb{Q}$ formado por las fracciones que en su forma irreducible no tienen a $p$ como factor del denominador

$$A = \{\frac{m}{n} \text{ tales que } p \text{ no divide a } n\}$$

Probar que $A$ es un anillo.

**1.7** Introduciremos en $\mathbb{R}^4$ una estructura de anillo. La suma de dos elementos se realiza componente a componente. Para la multiplicación escribimos los elementos en la forma $a + bi + cj + dk$ y definimos

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

$$(aa' - bb' - cc' - dd') + (ab' + b'a + cd' - dc')i +$$

$$(ac' + ca' + db' - bd')j + (ad' + da' + bc' - cb')k$$

Esta multiplicación se puede realizar aplicando la bilinealidad del producto y teniendo en cuenta la siguientes propiedades:

$$i^1 = j^2 = k^2 = -1, ij = k, jk = i, ki = j, ji = -ij, kj = -jk, ik = -ki$$

- $\mathbb{R}^4$ junto con esta suma y este producto es un anillo no conmutativo y con unidad. Este anillo se denota por $\mathbb{H}$ y sus elementos se llaman cuaterniones.
- Los cuaterniones tienen un subanillo isomorfo a $\mathbb{R}$ y otro subanillo isomorfo a $\mathbb{C}$.
- El subconjunto $\{1, -1, i, -i, j, -j, k, -k\}$ junto con el producto forma un grupo finito, llamado grupo cuaternión.
- El conjugado del cuaternión $q = a + bi + cj + dk$ es $\overline{q} = a - bi - cj - dk$. Operando obtenemos $q\overline{q} = a^2 + b^2 + c^2 + d^2$. Dicho número real se llama norma del cuaternión $q$ y es nula si y solo si el cuaternión es nulo.
- Si $q \neq 0$ entonces es invertible y su inverso viene dado por la fórmula

$$q^{-1} = \frac{1}{a^2 + b^2 + c^2 + d^2}\,\overline{q}$$

- Se cumple la fórmula $\overline{q_1 \cdot q_2} = \overline{q_2} \cdot \overline{q_1}$ análoga a la propiedad que cumplen los números complejos.

**1.8** Sea $\xi$ la raiz $p$-ésima de la unidad ($\xi = e^{\frac{2\pi i}{p}}$). El conjunto de números complejos que se pueden expresar en la forma

$$a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{p-1}\xi^{p-1}$$

es un anillo, denominado $\mathbb{Z}(\xi)$. Este anillo se denomina anillo de Kummer. Comprobar que es el menor subanillo de $\mathbb{C}$ que contiene a los enteros y a $\xi$.

**1.9** Encontrar todos los subanillos de $\mathbb{Z}_{20}$. Encontrar los divisores de cero y las unidades de $\mathbb{Z}_{20}$.

**1.10** Sea $A$ un anillo de tal modo que todo elemento de $A$ cumpla $a^2 = a$. Demostrar que $A$ es conmutativo. (Los elementos cuyo cuadrado coincide con ellos mismos se denominan idempotentes)

**1.11** Probar que en todo anillo conmutativo es válida la fórmula del binomio de Newton.

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

En el caso no conmutativo también es cierta si los dos elementos del binomio conmutan.

**1.12** Probar que el producto de un divisor de cero y otro elemento es un divisor de cero (suponer $A$ conmutativo).

¿Si el producto de dos elementos es un divisor de cero, entonces alguno de los dos es un divisor de cero?

**1.13** Probar que un anillo $A$ es íntegro si y solo si $A^*$ es cerrado por la operación de multiplicación. Probar que un anillo es íntegro si y solo si se satisface en él la ley de cancelación.

**1.14** Un elemento $a \in A$ es nilpotente si $a^n = 0$ para cierto número natural. Si $a$ es nilpotente, entonces $1 - a$ y $1 + a$ son invertibles.

**1.15** Sea $a$ un elemento idempotente ($a^2 = a$). El conjunto

$$S = \{ara \text{ tal que } r \in A\}$$

es un subanillo.

**1.16** Sea $\varphi : A \to A$ un morfismo. Los puntos fijos del morfismo

$$S = \{a \in A \text{ tales que } \varphi(a) = a\}$$

forman un subanillo.

**1.17** Demostrar que el conjunto de matrices reales de la forma

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

forman un anillo isomorfo al cuerpo de los números complejos.

**1.18** Sea $\varphi : A \to A'$ un morfismo de anillos. Demostrar que si $a$ es invertible, entonces $\varphi(a^{-1}) = \varphi(a)^{-1}$.

**1.19** Sea $a$ invertible. La aplicación $\varphi_a$ definida como $\varphi_a(x) = axa^{-1}$ es un endomorfismo de anillos. Este endomorfismo se llama endomorfismo interior.

**1.20** En este ejercicio haremos un estudio de la caraterística en el caso en el que el anillo no posea unidad.

- Si en un anillo $A$ existe un número natural $n$ que cumple $na = 0$ para todos los elementos del anillo, al menor de esos números se le denomina característica del anillo $A$. Si no existe el natural antes mencionado decimos que la característica es nula.
- En un anillo íntegro la característica es siempre o nula o un número primo.
- En un anillo íntegro todos los elementos no nulos tienen el mismo orden considerados como elementos del grupo aditivo $(A, +)$.
- Un anillo tiene característica no nula si existe un natural $n$ y un elemento $a$ que cumplan $na = 0$.
- En el caso en el que el anillo tenga unidad demostrar que las dos definiciones dadas de caraterística coinciden.

**1.21** En un cuerpo $k$ denotamos $a/b$ al elemento $ab^{-1}$. Demostrar las propiedades de las operaciones con fracciones.

**1.22** Sea $A$ un anillo sin unidad. Definimos en $A \times \mathbb{Z}$ las operaciones

$$(a, n) + (b, m) = (a + b, m + n)$$

$$(a, n) \cdot (b, m) = (ab + ma + nb, mn)$$

- $A \times \mathbb{Z}$ es un anillo con unidad y la aplicación

$$\begin{array}{rccc} \varphi & : A & \longrightarrow & A \times \mathbb{Z} \\ & a & \longrightarrow & (a, 1) \end{array}$$

  es un morfismo de anillos inyectivo.

- Si $A$ tiene característica $n$, se puede introducir, con las mismas operaciones, una estructura de anillo en $A \times \mathbb{Z}_n$. Este anillo que hemos construido tiene también característica $n$.

**1.23** Un anillo de Boole es un anillo con unidad donde todo elemento es idempotente ($a^2 = a$).

- $\mathbb{Z}_2$ es un anillo de Boole.
- Las partes $\mathcal{P}(X)$ de un conjunto $X$ es un anillo de Boole.
- $\mathrm{Apli}(X, \mathbb{Z}_2)$ es un anillo de Boole.
- Todo anillo de Boole es conmutativo.
- En todo anillo de Boole se cumple $2a = a + a = 0$ para todo elemento del anillo. Por lo tanto un anillo de Boole tiene característica 2.
- Si un anillo de Boole es íntegro, entonces necesariamente es isomorfo a $\mathbb{Z}_2$.
- La imagen de un anillo de Boole es un anillo de Boole. Si $\varphi : A \to B$ es un morfismo de anillos y $A$ es de Boole, entonces su imagen también es un anillo de Boole.
- El teorema de representación de Stone afirma que para todo anillo de Boole $A$, existe un conjunto $X$ de tal forma que $A$ es isomorfo a un subanillo de $\mathcal{P}(X)$. Para la demostración consúltese [**?**].

**1.24** Consideramos el anillo de las matrices de orden dos y coeficientes complejos. En dicho anillo consideramos el subconjunto $H$ de las matrices de la forma

$$\begin{pmatrix} a+ib & c-id \\ -c+id & a-ib \end{pmatrix}$$

Demostrar que $H$ es isomorfo al anillo de cuaterniones.

**1.25** Sea $A$ un anillo y $M_2(A)$ el anillo de las matrices cuadradas de orden 2. Dada

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

la adjunta de su traspuesta es

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

- Demostrar que $MN = NM = \det(M)\,\mathrm{Id}$.

- Demostrar la fórmula $\det(MM') = \det(M)\det(M')$.
- Si $\det(M)$ es una unidad, entonces $M$ es invertible. Calcular la inversa de $M$.
- Si $M$ es invertible, entonces $\det(M)$ es una unidad.

**1.26** Demostrar que $U(A \times B) = U(A) \times U(B)$.

**1.27** Encontrar divisores de cero en el anillo de partes de un conjunto.

**1.28** Sea $k$ un cuerpo y $E$ un espacio vectorial de dimensión $n$ sobre $k$. Consideramos los anillos $M_n(k)$ y $\mathrm{End}(E)$. Demostrar que si damos una base de $E$, tenemos un isomorfismo de anillos de $M_n(k)$ en $\mathrm{End}(E)$. Ver si el recíproco es cierto.

**1.29** Sea $X$ un conjunto arbitrario. Consideremos el anillo $\mathcal{P}(X)$ de las partes de $X$ y el anillo $\mathrm{Apli}(X, \mathbb{Z}_2)$. A cada subconjunto $U \subset X$ le asociamos la función $\varphi_U : X \to \mathbb{Z}_2$ definida como

$$\varphi_U = \begin{cases} 1 \text{ si } x \in U \\ 0 \text{ si } x \notin U \end{cases}$$

$\varphi_U$ es la función característica del subconjunto $U$.

- Demostrar que la función

$$\begin{array}{rcl} \mathcal{P}(X): & \longrightarrow & \mathrm{Apli}(X, \mathbb{Z}_2) \\ U & \longrightarrow & \varphi_U \end{array}$$

es un isomorfismo de anillos.

# 2. Ideales

Sabemos por teoría de grupos que no a todo subgrupo $G'$ de un grupo $G$ se le puede asociar el grupo cociente $G/G'$. Es necesario que el subgrupo sea normal para que la construcción no dependa de los representantes tomados. Del mismo modo, no es posible hacer cociente con cualquier subanillo. Ello nos conduce a la introducción de los ideales.

**Definición 2.1** *Un* ideal *es un subconjunto $I \subset A$ que cumple:*

- *$I$ es un subgrupo aditivo.*
- *Si $a \in I$ y $r \in A \Rightarrow ra$ y $ar$ son elementos de $I$.*

Si el anillo es conmutativo, solamente es necesario comprobar que $ra \in I$. Todo ideal es la vez un subanillo (en general sin unidad). Sin embargo no todos los subanillos tienen que ser ideales.

Si el anillo no es conmutativo es necesario dar otra definición.

**Definición 2.2** *Un subconjunto $I \subset A$ es un* ideal por la derecha *si:*

- *$I$ es un subgrupo aditivo.*
- *Para todo $r \in A$ y todo $a \in I$ se tiene $ar \in I$.*

Análogamente se define el concepto de ideal por la izquierda. Debido a esta definición, en algunas ocasiones se llama ideales biláteros a los ideales de los anillos no conmutativos. Sin embargo supondremos, salvo mención explícita de lo contrario, que todos los anillos son conmutativos.

El cero y el total son ideales. Estos ideales se llaman ideales triviales del anillo $A$. Los ideales que no son ni el nulo ni el total se denominan propios.

Si una unidad $a$ pertenece a un ideal $I$ dicho ideal es el total pues concluimos que $1 \in I$ multiplicando por el inverso y por lo tanto $r \in I$ sea cual sea $r \in A$. Así ningún ideal propio de $A$ contiene unidades.

**Ejemplos**

- Los subconjuntos de la forma $n\mathbb{Z}$ son ideales de $\mathbb{Z}$ como se comprueba fácilmente. Además estos son los únicos ideales, pues como sabemos todo ideal debe ser subgrupo aditivo y no existen en $\mathbb{Z}$ más subgrupos que los mencionados.

- Sea $A$ un anillo conmutativo. Sea $a \in A$ un elemento cualquiera no nulo. Los múltiplos de $a$ son de la forma $ra$ con $r \in A$. El conjunto de todos los múltiplos de $a$ se denota por $(a)$ y es un ideal. Se dice que es el ideal principal generado por el elemento $a$.

- Los cuerpos solo tienen ideales triviales pues todo elemento no nulo es invertible. Recíprocamente, si un anillo solo tiene ideales triviales para cada elemento $a$ el ideal principal $(a)$ es el total y por lo tanto existe un elemento $b$ que cumple $ba = 1$.

- Dada una función $f : \mathbb{R} \to \mathbb{R}$ su soporte es el cierre del conjunto de puntos donde no es nula. Decimos que una función se anula en el infinito si su soporte es un conjunto acotado. Dado el anillo $A = C(\mathbb{R}, \mathbb{R})$ sea $I$ el conjunto de todas las funciones que se anulan en el infinito. $I$ es un ideal pues es un subgrupo y el producto de una función que se anula en el infinito por cualquier otra función, siempre se anula en el infinito.

- El conjunto $I \subset C(\mathbb{R}, \mathbb{R})$ formado por las funciones que se anulan para $x = 0$ forman un ideal.

- Sean $A$ y $B$ dos anillos. Sea $I_A \subset A$ y $I_B \subset B$ ideales. El subconjunto $I_A \times I_B$ es un ideal del producto directo $A \times B$. El recíproco también es cierto (pruébese).

La importancia de los ideales radica en que sirven para definir anillos cocientes. Con más precisión, tenemos el siguiente

**Teorema 2.1** *Sea $I$ un ideal de $A$. En el grupo cociente $A/I$ se puede introducir una estructura única de anillo que hace que la proyección canónica sea un morfismo de anillos. Si $A$ tiene unidad también la tendrá $A/I$.*

**Demostración.**

Sabemos que en $A/I$ se puede introducir una estructura de grupo abeliano con las condiciones pedidas. Para que la proyección canónica $\pi : A \to A/I$ sea morfismo de anillos, la única definición posible de producto en $A/I$ es

$$\pi(a) \cdot \pi(b) = \pi(ab)$$

Si $I$ es un ideal esta definición no depende de los representantes elegidos. En efecto si

$$\pi(a) = \pi(a') \Rightarrow a = a' + r, \text{ con } r \in I$$

$$\pi(b) = \pi(b') \Rightarrow b = b' + s, \text{ con } s \in I$$

De esto concluimos que $ab = a'b' + a's + rb' + rs$. Entonces $\pi(ab) = \pi(a'b')$ puesto que $a's + rb' + rs \in I$. $\square$

**Definición 2.3** *El anillo $A/I$ que acabamos de construir se llama* anillo cociente *de $A$ módulo $I$.*

**Ejemplos**

- Si el ideal $I$ es el total el anillo cociente es el anillo trivial 0. Si el ideal $I$ es el ideal nulo, entonces el anillo y su cociente son isomorfos. Debido a esto, los ideales triviales carecen de interés.
- Consideremos el ideal $n\mathbb{Z}$ de $\mathbb{Z}$. El anillo cociente se denota en este caso por $\mathbb{Z}_n$. El estudio clásico de las congruencias es el estudio de este anillo.
- Si $n$ no es primo el anillo $\mathbb{Z}_n$ no es íntegro. Sea $n = n_1 n_2$ una descomposición en producto de factores. Entonces $0 = \pi(n) = \pi(n_1)\,\pi(n_2)$. Con mayor generalidad podemos afirmar que $\mathbb{Z}_n$ es íntegro si y solo si $n$ es primo.

**Proposición 2.2** *Sea $A$ un anillo. La intersección de ideales de $A$ es de nuevo un ideal de $A$.*

**Demostración.**

Sea $I_j$ una colección de ideales de $A$. Su intersección es un subgrupo. Además si $r \in A$ y $a \in \bigcap I_j$ tenemos que $ra \in I_j$ para todo $j$. Así $ra \in \bigcap I_j$ y concluimos que es un ideal. $\square$

**Definición 2.4** *Sea $S$ un subconjunto de $A$. A la intersección de todos los ideales que contienen a $S$ se le denomina* ideal generado *por el subconjunto $S$. En virtud de la proposición anterior este ideal existe y es único.*

**Proposición 2.3** *Sea $S \subset A$ un subconjunto posiblemente infinito. El conjunto de todas las combinaciones lineales de elementos de $S$ con coeficientes en $A$ es el ideal generado por $S$.*

**Demostración.**

Sea $\langle S \rangle = \{\sum a_j s_j$ con $a_j \in A$ y $s_j \in S\}$. La suma debe ser finita. Este conjunto es un subgrupo aditivo de $A$. Si multiplicamos un elemento de $\langle S \rangle$ por un elemento cualquiera $r$ del anillo obtenemos $r(\sum a_j s_j) = \sum (ra_j)s_j$. Así hemos probado que $\langle S \rangle$ es un ideal. Además todo ideal que contenga a $S$ debe contener a las combinaciones lineales de elementos de $S$. De este modo $\langle S \rangle$ es el menor ideal que contiene a $S$. $\square$

En el caso en que el conjunto $S$ este formado solo por un elemento $a$, el ideal generado se denota por $(a)$ y se dice que es un ideal principal.

**Definición 2.5** *Un ideal $I$ es* finito-generado *si existe un conjunto finito $S$ tal que $\langle S \rangle = I$. Un ideal $I$ es* principal *si existe un elemento $a$, no necesariamente único, tal que $(a) = I$.*

Supongamos que dos elementos del anillo $A$ generan el mismo ideal principal, $(a) = (b)$. Si el anillo es íntegro, debe de existir un elemento invertible $u$ tal que $a = bu$.

**Definición 2.6** *Sea $I$ y $J$ dos ideales. Llamamos* ideal suma *y denotamos por $I + J$ al ideal generado por el conjunto $I \cup J$. De modo análogo se define la suma de un número finito o infinito de ideales.*

*Llamamos* producto *de dos ideales, al ideal $IJ$ generado por todos los elementos de la forma $ab$ con $a \in I$ y $b \in J$. En particular esto nos permite definir las potencias de un ideal.*

*Decimos que dos ideales son* primos entre si *cuando $I + J = A$.*

Dado un anillo $A$, sea $\Sigma$ (o $\Sigma_A$ si existe peligro de confusión) el conjunto de los ideales de $A$. En este conjunto la inclusión establece una relación de orden. Dados dos ideales $I$ y$J$ el menor ideal que los contiene es precisamente $I + J$. En el conjunto ordenado, la suma de ideales es el supremo de dos o en general de un número arbitrario de ideales.

El mayor elemento contenido en $I$ y en $J$ es $I \cap J$. Este es el ínfimo de los dos ideales en cuestión. Análogamente se procede con un número finito o infinito de ideales.

Dos ideales son primos entre sí, cuando su supremo es el conjunto total. Resumiendo todas estas consideraciones tenemos el

**Teorema 2.4** *Dado un anillo $A$, el conjunto $\Sigma$ de sus ideales es un* retículo *cuyo* primer elemento *es el ideal cero, su* último elemento*, el conjunto $A$. El* supremo *de una familia de ideales es la suma de dichos ideales, y el* ínfimo *es la intersección de los ideales.*

Veamos ahora como se comportan los ideales bajo la acción de los morfismos.

**Teorema 2.5** *Sea $\varphi : A \longrightarrow A'$ un morfismo de anillos*

- *Si $I' \subset A'$ es un ideal, $\varphi^{-1}(I')$ es un ideal de $A$. En particular el núcleo $\mathrm{Ker}(\varphi) = \varphi^{-1}(0)$ es un ideal.*
- *Si $I \subset A$ es un ideal, $\varphi(I)$ es un subanillo, aunque en general no será un ideal. Si $\varphi$ es epiyectivo si es un ideal. En particular $\mathrm{Im}(\varphi)$ es un subanillo.*

**Demostración.**

*i*) $\varphi^{-1}(I')$ es un subgrupo aditivo. Sea $a \in \varphi^{-1}(I')$ y $r \in A$. Entonces $\varphi(ra) = \varphi(r)\varphi(a) \in I'$ puesto que $I'$ es ideal. Concluimos que $ra \in \varphi^{-1}(I')$ lo que demuestra que $\varphi^{-1}$ es un ideal.

*ii*) Si $a'$ y $b'$ pertenecen a $\varphi(I)$, entonces existen $a, b$, no necesariamente únicos, tal que $\varphi(a) = a'$ y $\varphi(b) = b'$. Entonces $a'b' = \varphi(a)\varphi(b) = \varphi(ab) \in \varphi(I)$ lo que prueba que es subanillo.

Si $\varphi$ es epiyectivo y $r' \in A'$, existe $r \in A$ tal que $\varphi(r) = r'$. El mismo argumento demuestra que en el caso epiyectivo la imagen de un ideal es un ideal. □

**Teorema 2.6** *Sea $\pi : A \to A/I$ la proyección canónica. Existe una correspondencia biunívoca entre ideales de $A/I$ e ideales de $A$ que contienen a $I$.*

**Demostración.**

Sea $J$ un ideal del cociente. Entonces $\pi^{-1}(J)$ es un ideal de $A$ que contiene a $I$. Del mismo modo $\pi(\pi^{-1}(J)) = J$ es un ideal por ser la proyección canónica epiyectiva. Esto prueba que la correspondencia es biunívoca. □

**Teorema 2.7 (Factorización canónica)** *Sea $\varphi : A \to A'$ un morfismo. Entonces existe un isomorfismo de anillos de $A/\operatorname{Ker}(\varphi)$ en $\operatorname{Im}(\varphi)$.*

**Demostración.**

Sabemos por teoría de grupos que existe un isomorfismo de grupos entre los anillos mencionados. Solo falta comprobar que ese isomorfismo respeta la multiplicación y que conserva la unidad. Pero esto se demuestra exactamente igual que en el caso de grupos abelianos. □

**Corolario 2.8** *Si $A$ tiene característica $n$, entonces $A$ tiene un subanillo isomorfo a $Z_n$. Si el anillo es íntegro la característica debe ser necesariamente prima.*

**Demostración.**

Sea $ch : \mathbb{Z} \longrightarrow A$ el morfismo característica. Si $n$ es la característica de $A$ entonces $\mathbb{Z}_n \sim \mathrm{Im}(ch)$.

Sabemos que $\mathbb{Z}_n$ es íntegro si y solo si $n$ es primo. Como $A$ es íntegro, necesariamente todos sus subanillos son íntegros. □

**Teorema 2.9 (2º teorema de isomorfismo)** *Sean $I$ y $J$ ideales de $A$ con $J \subset I$. Entonces se tiene un isomorfismo entre los anillos*

$$(A/J)/(I/J) \sim A/I$$

**Demostración.**

Si $\pi_J(a)$ denota la clase de equivalencia módulo $J$ del elemento $a$ definimos una aplicación

$$\begin{array}{ccc} A/J & \longrightarrow & A/I \\ \pi_J(a) & \longrightarrow & \pi_I(a) \end{array}$$

Dicha aplicación no depende del representante y por lo tanto esta bien definida. Es morfismo de anillos epiyectivo y su núcleo esta formado por los elementos $\pi_J(a)$ tales que $a \in I$. De este modo su núcleo es $I/J$ y concluimos aplicando el teorema de factorización canónica. □

**Teorema 2.10 ($3^{er}$ teorema de isomorfismo)** *Si $I, J$ son ideales de $A$ entonces se tienen un isomorfismo*

$$(I + J)/J \sim I/(I \cap J)$$

**Demostración.**

Defínase la aplicación

$$\begin{array}{ccc} I + J & \longrightarrow & I/(I \cap J) \\ a & \longrightarrow & \pi_{I \cap J}(a) \end{array}$$

Comprobar que no depende de los representantes y que es morfismo. Su núcleo es $J$. $\square$

## Problemas

**2.1** Sea $A$ conmutativo y con unidad. Un elemento $a$ es nilpotente si existe $n \in \mathbb{N}$ tal que $a^n = 0$. Probar que el conjunto de elementos nilpotentes de $A$ forman un ideal.

**2.2** En un anillo $A$ los ideales cumplen las siguientes propiedades:

- $(I + J) + K = I + (J + K)$
- $I + J = J + I$
- $I + 0 = I$
- $I + A = A$
- $(I \cdot J) \cdot K = I \cdot (J \cdot K)$
- $I \cdot J = J \cdot I$
- $I \cdot 0 = 0$
- $I \cdot A = I$
- $I \cdot J \subset I \cap J$
- $(I + J) \cdot K = I \cdot K + J \cdot K$

**2.3** Sea $A$ un anillo y $a$ un elemento. El conjunto

$$\mathrm{Ann}(a) = \{r \in A \text{ tales que } ra = 0\}$$

forman un ideal, llamado anulador del elemento $a$.

**2.4** Demostrar que el conjunto de matrices de la forma

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

donde $a, b$ son números reales es un ideal por la izquierda del anillo del $M_2(\mathbb{R})$. Demostrar que no es ideal por la derecha.

**2.5** Si $\varphi : A \longrightarrow A'$ es morfismo de anillos y $A$ es un cuerpo, entonces $\varphi$ es nulo o inyectivo.

**2.6** Sea $A$ un anillo y $S$ un subgrupo de $A$. Definimos en $A$ la relación de equivalencia $a \sim b \Leftrightarrow a - b \in S$. Demostrar que el conjunto cociente se puede dotar de una estructura de anillo, que haga que la proyección canónica sea morfismo, si y solo si $S$ es un ideal.

**2.7** Sea $A$ un anillo e $I$ un ideal bilátero.

$$C(I) = \{r \in A \text{ tales que } (ra - ar) \in I \text{ para todo } a \in A\}$$

Demostrar que $C(I)$ es un subanillo.

**2.8** El conjunto $I = \{a + 2bi \text{ con } a, b \in \mathbb{Z}\}$ es un ideal de los enteros de Gauss.

**2.9** Demostrar la ley distributiva para ideales.

$$I(J + K) = IJ + IK$$

Demostrar que $IJ \subset I \cap J$ para todo par de ideales. Generalizar los resultados para un número arbitrario de ideales, incluso un número infinito.

**2.10** Sea $\varphi : A \longrightarrow B$ un morfismo epiyectivo.

- $\varphi(I + J) = \varphi(I) + \varphi(J)$
- $\varphi(I \cdot J) = \varphi(I) \cdot \varphi(J)$
- $\varphi(I \cap J) \subset \varphi(I) \cap \varphi(J)$

**2.11** Sea $A$ un anillo no conmutativo. Llamamos conmutador de $a$ y $b$ al elemento $[a, b] = ab - ba$. Sea $[A, A]$ el ideal bilatero generado por el subconjunto de todos los conmutadores.

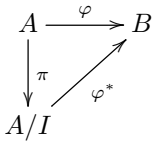
- $A$ es conmutativo $\Leftrightarrow [A, A] = 0$.
- $A/I$ es conmutativo $\Leftrightarrow [A, A] \subset I$.

**2.12** Sea $A = C(\mathbb{R}, \mathbb{R})$, e $I$ el ideal de las funciones que se anulan en el infinito. Demostrar, por contradicción, que $I$ no es finito generado.

**2.13** Sea $\varphi : A \to B$ un morfismo de anillos e $I \subset \ker(\varphi)$ un ideal. Entonces existe un único morfismo de anillos

$$\varphi^* : A \longrightarrow B$$

que hace conmutativo el diagrama



# 3. Ideales maximales y primos

**Definición 3.1** *Un ideal* $\mathfrak{m} \in A$ *es* maximal *si los únicos ideales que lo contienen son el mismo y el total.*

Si consideramos el conjunto $\Sigma$ de todos los ideales distintos del total de $A$ ordenados por inclusión, los ideales maximales son los elementos maximales de este conjunto ordenado. Aplicando el lema de Zorn veremos que todo anillo posee ideales maximales.

**Teorema 3.1** *Todo anillo A posee ideales maximales.*

**Demostración.**

Sea $I_j$ una cadena de ideales de $\Sigma$. Dados dos ideales de la cadena $I_\alpha$ e $I_\beta$ debe cumplirse $I_\alpha \subset I_\beta$ o $I_\beta \subset I_\alpha$.

Sea $\mathfrak{m} = \cup I_j$. Este conjunto es un ideal. Veamos por ejemplo que es subgrupo. Si $a, b \in \cup I_j$, entonces $a \in I_\alpha$ y $b \in I_\beta$. Podemos suponer $I_\alpha \subset I_\beta$. Por lo tanto $a - b \in I_\beta$ puesto que $I_\beta$ es subgrupo aditivo. Así $a - b \in \cup I_j$.

Por el lema de Zorn, existen en $\Sigma$ elementos maximales. Queda probada la existencia de ideales maximales. □

**Corolario 3.2** *Todo ideal I distinto del total está contenido en un ideal maximal.*

**Demostración.**

Sea $\pi : A \to A/I$ la proyección canónica. En $A/I$ existen ideales maximales Sea $\mathfrak{m}'$ un ideal maximal de $A/I$. Entonces $\pi^{-1}(\mathfrak{m}')$ es maximal y contiene a $I$ aplicando el teorema de correspondencia. □

**Corolario 3.3** *Todo elemento a no invertible está contenido en un ideal maximal.*

**Demostración.**

$(a)$ no es el ideal total puesto que $a$ no es invertible. Este ideal está contenido en ideal maximal y por lo tanto $a$ también. $\square$

Existe otra definición distinta de ideal maximal, que en muchos aspectos es más operativa. El siguiente teorema prueba que ambas definiciones son equivalentes.

**Teorema 3.4** *Un ideal $\mathfrak{m} \subset A$ es maximal $\Leftrightarrow$ $A/\mathfrak{m}$ es un cuerpo.*

**Demostración.**

Recordemos que un cuerpo es un anillo que solo tiene ideales triviales.
Aplicando el teorema de correspondencia tenemos que

$$\{\text{Ideales que contienen a } \mathfrak{m}\} = \{\text{Ideales de } A/\mathfrak{m}\}$$

Si $\mathfrak{m}$ es maximal, existen dos ideales que contienen a $\mathfrak{m}$ y por lo tanto el cociente tiene dos ideales. Esto implica que el cociente es un cuerpo.

Si $A/\mathfrak{m}$ es cuerpo, vemos que solo hay dos ideales que contienen a $\mathfrak{m}$, que es entonces maximal. $\square$

**Corolario 3.5** *Sea $\varphi : A :\to A'$ un morfismo epiyectivo de anillos. Si $A'$ es un cuerpo, el núcleo es un ideal maximal.*

**Demostración.**

Sabemos que $A/\operatorname{Ker}(\varphi)$ es isomorfo a $A'$ aplicando el teorema de factorización canónica. $\square$

**Ejemplos**

- Si $p$ es un número primo, entonces $p\mathbb{Z}$ es maximal. Para probarlo, analizamos su cociente. Como $\mathbb{Z}_p$ es íntegro y finito, es cuerpo.

- Sea $\phi_x : C(\mathbb{R}, \mathbb{R}) \to \mathbb{R}$ el morfismo "tomar valores en $x$". Si $\mathfrak{m}_x$ es el núcleo , tenemos por el teorema de factorización que $C(\mathbb{R}, \mathbb{R})/\mathfrak{m}_x \sim \mathbb{R}$ que es cuerpo. Entonces $\mathfrak{m}_x$ es maximal.

- Sea $\varphi : A \to A'$ un morfismo epiyectivo. Si $\mathfrak{m}' \subset A'$ es maximal $\Rightarrow$ $\varphi^{-1}(\mathfrak{m}')$ es maximal en $A$. Esto es debido a que la operación $\varphi^{-1}$ conserva el orden.

  Si $\varphi$ no es epiyectivo este resultado es falso. Sea $i : \mathbb{Z} \to \mathbb{R}$ la inclusión natural. La antiimagen del cero, que es maximal en $\mathbb{R}$, no es maximal en $\mathbb{Z}$.

- Un anillo $A$ es un cuerpo si y solo si 0 es un ideal maximal.

Como generalización del concepto de número primo, se puede introducir el concepto de ideal primo. La idea es que cuando el ideal sea principal, el concepto coincida con la idea de número primo. Recordemos que un número es primo si cuando divide a un producto, divide a alguno de los factores.

**Definición 3.2** *Un ideal $\mathfrak{p} \subset A$ es* primo *si $ab \in \mathfrak{p} \Rightarrow a \in A$ o $b \in A$.*

Existe otra definición de ideal primo que se obtiene directamente de esta. Un ideal $\mathfrak{p}$ es primo si $a, b \notin \mathfrak{p}$ implica que $ab \notin \mathfrak{p}$. De esta forma el complementario de un ideal primo es cerrado por la operación de multiplicación.

Sin embargo la caracterización más importante de los ideales primos viene dada por el siguiente

**Teorema 3.6** *Un ideal $\mathfrak{p} \subset A$ es primo $\Leftrightarrow$ $A/\mathfrak{p}$ es un anillo íntegro.*

**Demostración.**

$\Rightarrow$) Si $\pi(a)\,\pi(b) = 0$ entonces $\pi(ab) = 0$. Tenemos que o bien $a$ o bien $b$ pertencen a $\mathfrak{p}$. Entonces $\pi(a)$ es nulo o bien lo es $\pi(b)$. Así el anillo no tiene divisores de cero.

$\Leftarrow$) Si existieran $a, b$ tales que $ab \in \mathfrak{p}$ y ni $a$ ni $b$ están en $\mathfrak{p}$, tendríamos que $\pi(a)\,\pi(b) = 0$ y dos dos elementos no serían nulos, lo que contradice la hipótesis de que $A/\mathfrak{p}$ es íntegro. $\square$

**Corolario 3.7** *Todo ideal maximal es primo.*

**Demostración.**

Todo cuerpo es un anillo íntegro. □

**Corolario 3.8** *Sea $\varphi : A \to A'$ un morfismo de anillos. Si $A'$ es íntegro, el núcleo es un ideal primo.*

**Demostración.**

El teorema de factorización canónica nos dice que $A/\operatorname{Ker}(\varphi)$ es isomorfo a $\operatorname{Im}(\varphi)$. Como la imagen es un subanillo de un anillo íntegro, necesariamente es íntegra. □

**Proposición 3.9** *Sea $\mathfrak{p} \subset A$ e $I, J$ dos ideales tales que $IJ \subset \mathfrak{p}$. Entonces $I \subset \mathfrak{p}$ o $J \subset \mathfrak{p}$.*

**Demostración.**

Supongamos que $I \not\subset \mathfrak{p}$. Entonces existe $a \in I$ que no pertenece a $\mathfrak{p}$. Dado un elemento cualquiera $b \in J$ tenemos que $ab \in IJ \subset \mathfrak{p}$. Como $a$ no está en $\mathfrak{p}$, necesariamente $b \in \mathfrak{p}$ para todo elemento $b \in J$. Deducimos entonces que $J \subset \mathfrak{p}$. □

**Proposición 3.10** *Sea $\varphi : A \to A'$ un morfismo de anillos. Si $\mathfrak{p}'$ es primo $\Rightarrow \varphi^{-1}(\mathfrak{p}')$ es un ideal primo de $A$.*

**Demostración.**

Si $ab \in \varphi^{-1}(\mathfrak{p}') \Rightarrow \varphi(a)\varphi(b) \in \mathfrak{p}'$. Ocurre que como $\mathfrak{p}'$ es primo o bien un elemento u otro están en $\mathfrak{p}'$. Supongamos que está $\varphi(a)$. Entonces $a \in \varphi^{-1}(\mathfrak{p}')$ lo que demuestra que dicho ideal es primo. □

**Ejemplos**

- Si $p$ es un número primo, $p\mathbb{Z}$ es maximal, luego $p\mathbb{Z}$ es primo. Además 0 es primo por ser $\mathbb{Z}$ íntegro.
- La característica de un anillo íntegro siempre es prima o nula. Si $A$ tiene caracteristica $n$, entonces $\mathbb{Z}_n$ es un subanillo de $A$, que debe ser íntegro pues $A$ lo es. Aplicando el teorema $n$ es primo.
- Un anillo es íntegro si y solo si 0 es un ideal primo.

**Lema 3.11** *Sea $A$ un anillo conmutativo. El conjunto $\mathfrak{r}$ de todos los elementos nilpotentes de $A$ es un ideal. $A/\mathfrak{r}$ no tiene elementos nilpotentes.*

**Demostración.**

Sea $a \in A$ y $r \in \mathfrak{r}$. Entonces $ar$ es nilpotente puesto que $(ar)^n = a^n r^n$.

Si $r$ y $s$ son nilpotentes, entonces existen $m$ y $n$ tales que $r^m = 0 = s^n$. Aplicando la fórmula del binomio (problema 1.11) sabemos que $(r+s)^{m+n}$ es una suma de productos de distintas potencias de $r$ y de $s$. En cada sumando hay alguna potencia nula, por lo que $r + s$ es nilpotente. Asimismo $r - s$ es nilpotente. Por lo tanto $\mathfrak{r}$ es un ideal.

Si $\pi(a) \in A/\mathfrak{r}$ es nilpotente, entonces $(\pi(a))^n = 0$ para cierto $n$. Pero $\pi(a)^n = \pi(a^n) = 0$. Así $a^n$ es nilpotente y existe $m$ tal que $(a^n)^m = a^{nm} = 0$, lo que demuestra que $a$ es nilpotente y por lo tanto $\pi(a) = 0$. □

**Definición 3.3** *El ideal $\mathfrak{r}$ se denomina* nilradical *de $A$ o simplemente* radical. *El anillo cociente $A/\mathfrak{r}$ se llama* anillo reducido *y se denota $A_{red}$.*

Existe otra definición de nilradical. El teorema que sigue prueba que son equivalentes.

**Teorema 3.12** *El nilradical de $A$ es la intersección de todos los ideales primos de $A$.*

**Demostración.**

Sea $\mathfrak{r}'$ la intersección de todos los ideales primos de $A$. Si $a$ es nilpotente, tenemos que $a^n = 0 \in \mathfrak{p}$ para cualquier ideal primo $\mathfrak{p}$. Entonces $a$ o $a^{n-1}$ están

en $\mathfrak{p}$. Razonando por inducción, concluimos que $a$ está en $\mathfrak{p}$. Por lo tanto $a$ está en la intersección de todos los primos. Esto demuestra la inclusión $\mathfrak{r} \subset \mathfrak{r}'$.

Sea ahora $a$ no nilpotente. Consideramos el conjunto $\Sigma$ de todos los ideales $I$ de $A$ que no contienen a ninguna potencia de $a$. Como $a$ no es nilpotente, el conjunto $\Sigma$ no es vacio puesto que $0 \in \Sigma$. Aplicando el lema de Zorn, $\Sigma$ posee elementos maximales. Sea $\mathfrak{m}$ un elemento maximal. Probaremos que $\mathfrak{m}$ es primo.

Si $x, y \notin \mathfrak{m}$, los ideales $\mathfrak{m}+(x)$ y $\mathfrak{m}+(y)$ contienen a $\mathfrak{m}$ en sentido estricto. Como $\mathfrak{m}$ es maximal, estos ideales no están en $\Sigma$ y contienen a alguna potencia de $a$.

$$a^n \in \mathfrak{m} + (x) \qquad a^m \in \mathfrak{m} + (y)$$

De este modo $a^{m+n} \in \mathfrak{m} + (xy)$. De esto se sigue que $xy$ no pueden estar en $\mathfrak{m}$, pues de lo contrario $\mathfrak{m} + (xy) = \mathfrak{m}$. Queda así demostrado que $\mathfrak{m}$ es un ideal primo y que los elementos no nilpotentes no pueden estar en $\mathfrak{r}'$. Se concluye que $\mathfrak{r}' \subset \mathfrak{r}$, inclusión que demuestra el teorema. □

**Corolario 3.13** *Existe una biyección entre los ideales primos de $A$ y de $A_{red}$*

**Demostración.**

Utilizar el teorema de correspondencia y el hecho de que la antiimagen de un ideal primo es otro ideal primo. □

**Definición 3.4** *Sea $I \subset A$ un ideal. El* radical de $I$, $\mathrm{rad}(I)$ *es la intersección de todos los ideales primos que contienen a $I$. En particular $\mathfrak{r} = \mathrm{rad}(0)$.*

**Proposición 3.14** *El radical de $I$ es el conjunto de elementos de $A$ que tienen alguna potencia en $I$.*

**Demostración.**

Pasando a los cocientes, módulo el ideal $I$, el radical de $I$ se transforma en el nilradical, y los elementos de $A$ con alguna potencia en $I$ se transforman en elementos nilpotentes. □

**Corolario 3.15** *El radical de $I$ es la antiimagen por la proyección canónica del nilradical de $a/I$.*

# 4. Polinomios

De todos los anillos que existen, los anillos de polinomios son probablemente uno de los más importantes. Hasta finales del siglo XIX se puede decir que el álgebra es el estudio de los polinomios. Actualmente el álgebra comprende más ámbitos. Sin embargo en álgebra conmutativa y en geometría algebraica los polinomios, en una y en varias variables, son fundamentales.

Construiremos dichos anillos. Supondremos conocido el manejo elemental de polinomios con coeficientes en $\mathbb{R}$. Muchos de los resultados dados en esta sección son la generalización y formalización de resultados conocidos para polinomios con coeficientes reales.

**Definición 4.1** *Un* polinomio *de una variable sobre el anillo $A$ es un aplicación casi nula*

$$p : \mathbb{N} \longrightarrow A$$

*El conjunto de todos los polinomios sobre $A$ se denota $A(x)$.*

En nuestra definición suponemos que $0 \in \mathbb{N}$. La imagen del número $n$ se suele denotar por $a_n$. Así el polinomio será una sucesión

$$(a_0, a_1, a_2, \dots)$$

de elementos de $A$. Los elementos $a_i$ son todos nulos salvo un número finito de ellos. El mayor de los naturales $n$ tales que $a_n \neq 0$ se llama grado del polinomio y se denota $grado(p)$. Por la misma definición de polinomios, todo polinomio debe tener grado finito.

Introduciremos en $A(x)$ las operaciones de suma y producto de polinomios. El lector debe verificar que dichas operaciones introducen en $A(x)$ una estructura de anillo. Deberá tener en cuenta que estas comprobaciones pueden llegar a ser tediosas.

Si

$$p : \mathbb{N} \longrightarrow A \qquad q : \mathbb{N} \longrightarrow A$$

son dos polinomios, su suma es la aplicación

$$\begin{array}{rccl} p+q & :\mathbb{N} & \longrightarrow & A \\ & n & \longrightarrow & (p+q)(n) = p(n) + q(n) \end{array}$$

Esta aplicación es casi nula y su grado siempre es menor que el mayor de los grados de $p$ y de $q$.

El producto se define como

$$\begin{array}{rccl} p \cdot q & :\mathbb{N} & \longrightarrow & A \\ & n & \longrightarrow & (p \cdot q)(n) = \displaystyle\sum_{i+j=n} p(i)q(j) \end{array}$$

De nuevo la aplicación es casi nula, pues su grado siempre es menor que la suma de los grados de los dos factores.

**Teorema 4.1** *El conjunto $A(x)$ con las operaciones introducidas es un anillo.*

Si el anillo $A$ es conmutativo, también es conmutativo el anillo $A$. Si $A$ tiene unidad, entonces $A(x)$ también, siendo esta el polinomio

$$(1, 0, 0, \dots)$$

A todo elemento de $a \in A$ le podemos hacer corresponder un polinomio

$$(a, 0, 0, \dots)$$

Tenemos definida así una aplicación de $A$ en $A(x)$ que es un morfismo de anillos inyectivo. De este modo todo anillo se puede considerar como un subanillo de su anillo de polinomios.

En el caso en que $A$ tenga unidad, existe una notación standard para los polinomios. Para introducirla definimos el polinomio

$$x = \begin{cases} 1 \text{ si } i = 1 \\ 0 \text{ si } i \neq 1 \end{cases}$$

Utilizando la definición de producto y aplicando un argumento inductivo tenemos que

$$x^m = \begin{cases} 1 \text{ si } i = m \\ 0 \text{ si } i \neq m \end{cases}$$

Con esta notación el polinomio

$$(a_0, a_1, a_2, \dots)$$

se escribe

$$a_0 + a_1 x + a_2 x^2 + \cdots = \sum a_i x^i$$

La suma es finita puesto que casi todos los $a_i$ son nulos. Los elementos $a_i$ se denominan coeficientes. La letra $x$ se denomina variable. Debemos tener cuidado pues en matemática elemental $x$ es simplemente una letra. Sin embargo para nosotros será un polinomio.

El anillo de polinomios en dos variables $A(x, y)$ se define como $(A(x))(y)$. De modo inductivo se definen los anillos de polinomios en varias variables.

**Proposición 4.2** *Si $A$ es íntegro $A(x)$ es íntegro. En general $A(x_1, \dots, x_n)$ es íntegro.*

**Demostración.**

Si $p = a_n x^n + \cdots + a_0$ y $q = b_m x^m + \cdots + b_0$, el producto de $p$ y $q$ tiene como coeficiente de grado $n + m$ al producto $a_n b_m$ que no es nulo. □

**Teorema 4.3 (Propiedad universal)** *Dados dos anillos sea $\varphi : A \to B$ un morfimo de anillos. Para cada elemento $b \in B$ existe un único morfismo de anillos*

$$\varphi_b^* : A(x) \longrightarrow B$$

*que cumple $\varphi_b^*(x) = b$ y $\varphi_b^*(a) = \varphi(a)$ para todo elemento $a \in A$.*

**Demostración.**

Si $\varphi^*$ cumple estas propiedades, la única definición posible para $\varphi^*$ es

$$\varphi_b^*(\sum a_i x^i) = \sum \varphi(a_i) b^i$$

Veamos que con esta definición obtenemos un morfismo de anillos.

Que conserva la unidad y la suma es claro. Para ver que conserva la multiplicación debemos fijarnos en que el producto de polinomios, si entendemos que "$x$" es un elemento de $A$, no es nada más que la aplicación de la propiedad distributiva.

Es más. La definición de multiplicación dada en el anillo de polinomios es la precisa para que las aplicaciones $\varphi_b^*$ sean morfismos. □

Para el estudio de la propiedad universal de los anillos de polinomios en varias variables, vease el problema 4.7

**Corolario 4.4** *Si $\varphi : A \to B$ es un morfismo de anillos, existe un morfismo $\varphi^* : A(x) \to B(x)$ que extiende a $\varphi$ y que respeta la variable $x$.*

**Demostración.**

Si $\varphi : A \to B$ es un morfismo de anillos, podemos construir otro morfismo de anillos de $A$ en $B(x)$ sin más que componer con la inclusión canónica de $B$ en su anillo de polinomios. □

Si $\phi$ es cualquier otro morfismo de anillos tenemos que $(\varphi\phi)^* = \varphi^*\phi^*$. Así, si dos anillos son isomorfos, podemos construir un isomorfismo natural entre sus anillos de polinomios.

**Corolario 4.5** *Sea $A \subset B$ un subanillo. Si $b \in B - A$, el mínimo subanillo de $B$ que contiene a $A$ y a $b$ es la imagen de $i_b^*$. Este subanillo se denota $A(b)$.*

**Demostración.**

Sea $i : A \to B$ la inyección canónica. La imagen de $i_b^*$ es un subanillo que contiene a $A$ y a $b$. Además si otro subanillo contiene a esos dos elementos, debe de contener a todos los polinomios con coeficientes en $A$ y de variable $b$.

Si $I_b$ denota el núcleo de $i_b^*$, tenemos que $A(x)/I_b = A(b)$. $\square$

**Definición 4.2** *Sea $A \subset B$. Un elemento $b \in B$ es* algebraico *sobre $A$ si* $\mathrm{Ker}(i_b^*)$ *es no nulo. Es* transcendente *si el núcleo si es nulo. El polinomio que genera dicho ideal es el* polinomio mínimo *de $b$.*

**Ejemplos**

- $\sqrt{2}$ es algebraico sobre $\mathbb{Z}$ pues $x^2 - 2$ está en el núcleo del morfismo.
- La unidad imaginaria $i$, es algebraica sobre $\mathbb{Z}$ pues $x^2 + 1$ lo anula.
- $e$ y $\pi$ son transcendentes sobre $\mathbb{Z}$. La demostración de este hecho es complicada y no la podemos ofrecer aquí.

Otro resultado deducido de la propiedad universal es

**Proposición 4.6** *Si $b \in A$, la aplicación*

$$\begin{array}{rccc} \varphi_b & : A(x) & \longrightarrow & A \\ & \sum a_i x^i & \longrightarrow & \sum a_i b^i \end{array}$$

*que consiste en "sustituir" la indeterminada $x$ por $b$ es un morfismo de anillos.*

Para denotar que en un polinomio $p$ se ha sustituido $x$ por un elemento $a$ del anillo, introducimos la notación $p(a)$. Naturalmente $p(a) \in A$. Si $B$ es un anillo que contiene a $A$ como subanillo, tiene sentido para todos los polinomios $p \in A(x)$ sustituir la $x$ por un elemento de $b \in B$. En este caso $p(b) \in B$.

Cada polinomio $p \in A(x)$ define una función

$$\begin{array}{rccc} p & : A & \longrightarrow & A \\ & a & \longrightarrow & p(a) \end{array}$$

sin embargo debemos tener cuidado con esta construcción, pues a diferencia de lo que ocurre con los polinomios de coeficientes reales, existen anillos donde distintos polinomios inducen la misma función.

**Definición 4.3** *Sea $p \in A(x)$. El elemento $a \in A$ es una raíz de $p$ si $p(a) = 0$. Si $A \subset B$, un elemento $b \in B$ es una raíz si $p(b) = 0$.*

**Teorema 4.7 (División euclídea)** *Sea $k$ un cuerpo y $p$ y $q$ dos polinomios donde $grado(p) \geq grado(q)$. Existen polinomios $c$ y $r$, que además son únicos, que cumplen*

$$p = qc + r \text{ donde } r = 0 \text{ ó } grado(r) < grado(q)$$

*El polinomio $c$ se llama* cociente. *El polinomio $r$ es el* resto.

**Demostración.**

La demostración y el algoritmo para hallar el cociente y el resto que se emplea para polinomios reales, es válido en el caso general. □

**Corolario 4.8** *Si $k$ es cuerpo y $p \in k(x)$, el resto de la división de $p$ entre $(x - a)$ es $f(a)$.*

**Demostración.**

$f = c(x - a) + r$ donde $r$ es de grado cero o es nulo. Sustituyendo $a$ en esta expresión se acaba. □

**Corolario 4.9** *Sea $k$ un cuerpo. Un elemento $a$ es raíz de $p$ si y solo si $(x - a)$ divide a $p$. Un polinomio de grado $n$ tiene como mucho $n$ raices.*

**Demostración.**

$f(a)$ es el resto y es nulo si y solo si $(x - a)$ divide a $p$.

Si $a$ es una raíz tenemos que $p = q(x - a)$ donde el grado de $q$ es uno menos que el grado de $p$. Se termina aplicando inducción. □

**Teorema 4.10** *$k(x)$ es un dominio de ideales principales.*

**Demostración.**

Sea $I$ un ideal del anillo de polinomios. Sea $q$ un polinomio no nulo y de grado mínimo entre todos los que pertenecen a $I$. Si $p \in I$, entonces es de grado mayor o igual que $q$. Aplicando el teorema de división euclídea $p = qc + r$, lo que prueba que $r = p - qc \in I$. Como $r$ es de grado menor que $q$, necesariamente $r = 0$. De este modo $p = qc$ y concluimos que $I$ es el ideal principal generado por $q$. □

Una vez visto este teorema, todos los resultados correspondientes a la sección de divisibilidad son automaticamente válidos para los polinomios sobre un cuerpo.

Sea ahora $p$ un polinomio que genere un ideal maximal (por lo tanto no puede tener raices). El cociente de $k(x)$ módulo este ideal es un cuerpo. El polinomio $p$ se puede entender como un polinomio con coeficientes en este nuevo cuerpo. Pero en este nuevo cuerpo, el polinomio $p$ tiene como raíz al elemento $\pi(x)$. Hemos construido de este modo un cuerpo donde el polinomio irreducible $p$ tiene una raíz. Resumiendo, hemos demostrado

**Teorema 4.11 (Kronecker)** *Para todo polinomio $p$ sobre un cuerpo $k$, existe un cuerpo $K$, que contiene a $k$ como subcuerpo, donde el polinomio tiene una raíz.*

Considerando los factores primos de un polinomio y repitiendo un número finito de veces el argumento anterior, llegamos al siguiente corolario

**Corolario 4.12** *Para todo polinomio $p$ sobre un cuerpo $k$, existe un cuerpo $K$ que lo contiene, donde el polinomio tiene tantas raices como su grado.*

## Problemas

**4.1** Sea $k$ un cuerpo.

- Toda fracción algebraica $p/q$ se puede escribir en la forma

$$\frac{p}{q} = c + \frac{r}{q}$$

donde $grado(r) < grado(q)$.

- Utilizando el lema de Bezout, demostrar que si $p$ y $q$ son primos entre sí entonces

$$\frac{1}{pq} = \frac{a}{p} + \frac{b}{q}$$

- Utilizar inductivamente este argumento para demostrar que toda fracción propia sobre los complejos se puede escribir como suma de fracciones simples.

**4.2** Un anillo es euclídeo si es íntegro y existe una función

$$\delta : A \longrightarrow \mathbb{N}$$

que cumple:

- $\delta(x) = 0 \Leftrightarrow x = 0$
- $\delta(xy) = \delta(x)\delta(y)$
- Si $x$, $y$ son no nulos, entonces existen $r$ y $c$ que cumplen $y = cx + r$ y $\delta(r) < \delta(y)$.

El elemento $c$ se denomina cociente y $r$ es el resto. $\delta(x)$ el la norma de $x$. El resto y el cociente pueden no ser únicos.

- $\mathbb{Z}$ con $\delta(n) =\mid n \mid$ es euclídeo.
- Si $k$ es un cuerpo, $k(x)$ con $\delta(p) = 2^{grado(p)}$ es euclídeo.
- $\mathbb{Z}(i)$ con $\delta(a + ib) = a^2 + b^2$ es euclídeo. Para demostrarlo, considerar que el anillo está incluido en $\mathbb{Q}(i)$, que es un cuerpo.
- Las unidades de un anillo euclídeo son los elementos de norma 1.
- Si $a$ es un divisor de $b$, entonces $\delta(a) \leq \delta(b)$.
- Un anillo euclídeo es un dominio de ideales principales. Para la demostración, considérese los elementos de norma mínima del ideal.
- Probar inductivamente que todo elemento del anillo euclídeo se puede expresar como producto de elementos irreducibles. Demostrar la unicidad de esta descomposición, salvo producto por unidades.

**4.3** Sea $k \subset K$ dos cuerpos. Sea $a \in K - k$ algebraico sobre $k$. El morfismo

$$\begin{array}{rccc} \varphi_a & : k(x) & \longrightarrow & K \\ & p & \longrightarrow & p(a) \end{array}$$

valora en un cuerpo y por lo tanto el núcleo de $\varphi_a$ es un ideal primo. Como $a$ es algebraico, dicho núcleo no es nulo. El polinomio, cuyo coeficiente de mayor grado sea 1, que genera

este ideal es polinomio anulador de $a$. El cociente $k(a) = k(x)/p$ es un cuerpo. Si $q$ es otro polinomio , entonces $q(a) \in K(a)$ es no nulo y por lo tanto invertible. El problema de la racionalización consiste en encontrar otro polinomio $r$ que cumpla:

$$1/q(a) = r(a)$$

- Utilizar el lema de Bezout para resolver el problema de la racionalización.
- Aplicarlo al caso $1/(2-\sqrt{3})$ y al caso $1/(3\sqrt[3]{2}+5\sqrt[3]{2}+2)$.

**4.4** Sea $p$ y $q$ polinomios sobre un cuerpo y supongamos que $grado(p) \geq grado(q)$. Aplicando la división euclídea obtenemos

$$p = c_1 q + q_1$$

- Demostrar que $(p+q) = (q+q_1)$

Repetimos el proceso, pero ahora con los polinomios $q$ t $q_1$ y obtenemos

$$q = c_2 q_1 + q_2$$

Seguimos el proceso con $q_1$ y $q_2$. Como los grados de los polinomios van bajando, en algún momento la división es exacta

$$q_{m-1} = c_m q_m$$

- Recordando que el máximo común divisor de dos polinomios es el generador de ideal $(p+q)$ demostrar que

$$\text{m.c.d}((p,q) = q_m$$

- Generalizar este resultado al anillo $\mathbb{Z}$ y a todo anillo euclídeo.

**4.5** El teorema fundamental del álgebra afirma que todo polinomio con coeficientes complejos tiene al menos una raiz. La demostración rigurosa de este teorema se debe a Gauss. De las distintas demostraciones daremos la que se apoya en la teoría de funciones complejas. El teorema de Liouville afirma que toda función holomorfa y acotada es constante.

- Si un polinomio de grado mayor que cero $p(x)$ no tiene raices, entonces $\mid p(x) \mid > \epsilon$ para algún valor de $\epsilon$, puesto que la función es continua.
- Si $p(x)$ no tiene raices la función $1/p(x)$ es holomorfa y por el argumento anterior está acotada. Luego es una constante. Esto implica una contradicción y necesariamente el polinomio tiene al menos una raiz.

- Aplicando inducción, concluimos que todo polinomio tiene tantas raices como grado, contando las raices con su multiplicidad. Todo polinomio complejo se factoriza en polinomio de grado 1.
- Si $p(x)$ es un polinomio con coeficientes reales y $a$ es una solución compleja, entonces su conjugado, $\overline{a}$, también es solución. Las raices complejas de polinomios reales aparecen por parejas conjugadas. El polinomio real es divisible entre el polinomio $(x-a)(x-\overline{a})$ que también tiene coeficientes reales.
- Los polinomios reales irreducibles son los de grado 1 o los de grado 2 sin raices reales.

**4.6** Sea $k$ un cuerpo. Por analogía con el análisis infinitesimal definimos la derivada de un polinomio

$$p = a_n x^n + \cdots + a_1 x + a_0$$

como el polinomio

$$p' = n a_n x^{n-1} + \cdots + a_1$$

- Demostrar las fórmulas

$$(p+q)' = p' + q' \qquad (pq)' = p'q + pq'$$

- Si la derivada de un polinomio es nula, ¿necesariamente el polinomio es constante?. Analizar el caso de característica positiva y de característica nula por separado.
- Definir las derivadas de orden superior y generalizar (si es posible) la fórmula de Taylor.
- Considerar el anillo de polinomios en varias variables e introducir el concepto de derivada parcial. Ver que las derivadas parciales conmutan. Generalizar algún resultado del cálculo diferencial a esta nueva situación.
- Un elemento $a$ es raíz múltiple de un polinomio $p$ si $(x-a)^n$ divide al polinomio. Demostrar que si $a$ es una raíz múltiple, entonces es también raíz del polinomio derivado $p'$.

**4.7** Sea $\varphi : A \longrightarrow B$ un morfismo y $b_1, b_2 \in B$.

- Demostrar que existe un único morfismo

$$\varphi_{b_1,b_2} : A(x,y) \longrightarrow B$$

que cumple $\varphi_{b_1,b_2}(x) = b_1, \varphi_{b_1,b_2}(y) = b_2$ y $\varphi_{b_1,b_2}(a) = \varphi(a)$ para todo elemento $A \in A$.

- Generalizar esta propiedad a un número finito de variables.
- Demostrar que $\varphi_{b_1,b_2}(A(x,y))$ es el menor subanillo de $B$ que contiene a $\varphi(a)$ y a $b_1$ y $b_2$. En general este anillo se denota $A(b_1,b_2)$.
- Demostrar que existe un morfismo $\varphi^* : A(x,y) \longrightarrow B(x,y)$ que extiende a $\varphi$ y que conserva las variables.

Sea $A \subset B$ dos anillos. Dos elementos $b_1, b_2$ son algebraicamente independientes sobre $A$ si el morfismo $\varphi_{b_1,b_2}$ es inyectivo.

- Si $b = A(x,y)$, demostrar que los polinomios $x$ e $y$ son algebraicamente independientes sobre $A$.

**4.8** Si en la definición de polinomios en una variable quitamos la restricción de que las aplicaciones sean casi nulas, obtenemos un nuevo anillo, denotado $A[[x]]$ y llamado anillo de series formales.

- Si $A$ es íntegro el anillo $A[[x]]$ también.
- Si $s$ es una serie sin término independiente, entonces $s$ no puede ser invertible.
- Demostrar que la serie formal $1-x$ tiene inversa. Hallar dicho inverso. Como polinomio $1-x$ no es invertible.

**4.9** Consideremos en $\mathbb{Q}(x)$ el polinomio primo $x^2-2$. El cociente del anillo de polinomios, módulo el ideal $(x^2-2)$ es isomorfo al anillo $\mathbb{Q}(\sqrt{2})$.

**4.10** Sea $k$ un cuerpo y $p$ un polinomio irreducible de grado $n$.

- El cuerpo $k(x)/p$ es un espacio vectorial sobre $k$ de dimensión $n$.
- $\{1, \pi(x), \ldots \pi(x^{n-1})\}$ es una base de este espacio vectorial.

**4.11** Un anillo conmutativo es íntegro $\Leftrightarrow$ es un subanillo de un cuerpo.

**4.12** Sea $A$ un dominio de integridad. Sean $p$ y $q$ dos polinomios con coeficientes en $A$. Si el coeficiente de mayor grado de $q$ es invertible en $A$, probar que existen polinomios $c$ y $r$ que cumplen

$$p = cq + r \text{ y ádemas } grado(r) < grado(q)$$

¿Son únicos esos polinomios?

# 5. Divisibilidad

Realizaremos el estudio de la divisibilidad en el marco de los anillos de ideales principales, aunque muchas de las cuestiones estudiadas en este apartado son válidas en anillos más generales. En este apartado cuando hablemos de un anillo supondremos implícitamente que este anilo es un dominio de ideales principales.

Relacionados con la divisibilidad están varios conceptos. Por una parte el estudio del máximo común divisor y del mínimo común múltiplo. Otro tiene que ver con el Teorema fundamental de la Aritmética que afirma que todo número se puede escribir de modo único como multiplicación de números primos.

**Definición 5.1** *Un* dominio de ideales principales *(DIP) es un anillo conmutativo, con unidad, íntegro y donde todo ideal es principal.*

**Ejemplos**

- $\mathbb{Z}$ es un dominio de ideales principales.
- Si $k$ es un cuerpo $k(x)$ es un DIP, como demostramos en el teorema 4.10.
- Todo anillo euclídeo es un DIP. Para la definición de anillo euclídeo y para el estudio de sus propiedades elementales nos remitimos al problema 4.2.

**Definición 5.2** *Sean $a, b$ dos elementos de un anillo $A$. Decimos que $a$* divide *$a$ $b$ y denotamos $a \mid b$ si existe $c \in A$ que cumple $ac = b$. También se dice que $b$ es un* múltiplo *de $a$.*

Naturalmente la palabra divide en un anillo tiene siempre el sentido dado en la anterior definición, pues como sabemos la división es un concepto que no existe en los anillos, salvo para elementos invertibles.

La divisibilidad tiene unas propiedades elementales que pasamos a enunciar.

**Proposición 5.1** *En un anillo $A$ se cumple:*

*1.-* $a \mid 0$, $1 \mid a$ *y* $a \mid a$.

*2.-* $a \mid 1$ *si y solo si* $a$ *es invertible.*

*3.-* *Si* $a \mid b$, *entonces* $ac \mid bc$ *para cualquier* $c$.

*4.-* *Si* $a \mid b$ *y* $b \mid c$, *entonces* $a \mid c$. *Esta es la propiedad transitiva.*

*5.-* $a \mid b$ *si y solo si* $(b) \subset (a)$.

**Demostración.**

Las cuatro primeras propiedades se derivan directamente de la definición. Probemos la propiedad 5.

Si $a \mid b$, entonces $ac = b$ para cierto $c$. Entonces $b \subset (a)$, lo que implica que $(b) \subset (a)$.

Recíprocamente, si $(b) \subset (a)$, $b = ac$ para cierto $c$, lo que prueba que $a \mid b$ y concluye la demostración. □

La propiedad 5 nos informa que el estudio de la divisibilidad es equivalente al estudio de la estructura de orden del retículo de ideales. Aprovecharemos nuestros conocimientos sobre este retículo para demostrar cuestiones relacionadas con la divisibilidad.

Sin embargo la analogía no es completa pues puede ocurrir que dos elementos generen el mismo ideal.

**Definición 5.3** *Dos elementos* $a, b$ *de* $A$ *son* asociados *si* $a = bu$ *donde* $u$ *es una unidad.*

Esta relación es de equivalencia. La utilidad del concepto de elementos asociados se pone de manifiesto en la siguiente proposición, que a la vez sirve para dar una nueva definición de este concepto.

**Proposición 5.2** *Dos elementos son asociados si y solo si generan el mismo ideal.*

**Demostración.**

Si $a$ y $b$ son asociados $a = bu$. Luego todo múltiplo de $a$ es múltiplo de $b$. Pero también tenemos que $au^{-1} = b$. Así todo múltiplo de $b$ es múltiplo de $a$. Concluimos que $(a) = (b)$.

Si $(a) = (b)$, tenenos que $a = bc$ y $b = ad$. Sustituyendo $b$ en la primera expresión $a = adc$. Podemos cancelar $a$ al estar en un anillo íntegro y obtenemos que $1 = dc$. Esto prueba que $c$ es invertible. □

**Ejemplos**

- En $\mathbb{Z}$ los números $n$ y $-n$ generan el mismo ideal. Es costumbre tomar como generador al positivo.
- En $\mathbb{Z}(i)$, las unidades son $\{1, -1, i, -i\}$. Por lo tanto existen cuatro generadores para cualquier ideal. Para la demostración de que en efecto $\mathbb{Z}(i)$ es un DIP nos remitimos al problema 4.2.
- Si $k$ es un cuerpo, los polinomios de grado cero (o sea los elementos de $k$) son los invertibles. Así que un polinomio $p$ y todos los que se obtienen multiplicando $p$ por un elemento de $k$ generan el mismo ideal. Sin embargo si hablamos de generador de un ideal en un anillo de polinomios siempre estaremos suponiendo que el coeficiente de mayor grado es 1. Estos polinomios se denominan unitarios o mónicos.

El estudio del máximo común divisor y del mínimo común múltiplo se puede realizar para conjuntos formados por más de dos elementos. Como el introducir más elementos no aporta nada nuevo y solamente complica la notación, nos centraremos en el caso de dos elementos.

**Definición 5.4** *Sean $a_1, a_2 \in A$. Un elemento $d$ es un* máximo común divisor *si cumple:*

- $d \mid a_1$ *y* $d \mid a_2$.
- *Si $c$ divide a $a_1$ y a $a_2$, entonces $c \mid d$.*

Naturalmente si un elemento es un máximo común divisor, todo elemento asociado con el también. El máximo común divisor es un elemento que divide tanto a $a_1$ como a $a_2$. De hay proviene el apelativo "común". También es múltiplo de cualquier otro divisor común. Resulta que en el caso de $\mathbb{Z}$, es el que tiene mayor valor absoluto (de ahí lo de "máximo"). Sin embargo en un anillo que carezca de un orden no tiene sentido hablar de "máximo".

**Proposición 5.3** *El máximo comun divisor de $a_1$ y $a_2$ es el generador del ideal suma $(a_1) + (a_2)$.*

**Demostración.**

Sea $(d) = (a_1) + (a_2)$. Tenemos que $(a_i) \subset (d)$ lo que implica que $d \mid a_i$.

Si $c$ es un elemento que divide tanto a $a_i$ tendremos que $(a_i) \subset (c)$. Como la suma es el menor ideal que contiene a los ideales, $(d) \subset (c)$. Deducimos que $c \mid d$. $\square$

**Corolario 5.4 (Lema de Bezout)** *Dados dos elementos $a_1, a_2 \in A$, el máximo común divisor $d$ se puede expresar en la forma*

$$d = a_1x + a_2y \text{ para ciertos } x, y \in A$$

**Definición 5.5** *Dos elementos $a_1$ y $a_2$ son* primos entre si *o* primos relativos *si su máximo común divisor es la unidad. Esto es equivalente a que*

$$(a_1) + (a_2) = A$$

Aplicando el lema de Bezout a un par de primos relativos tenemos la fórmula

$$1 = a_1x + a_2y$$

Como aplicación de esta fórmula (llamada fórmula de Bezout) tenemos

**Corolario 5.5** *Sean $a, b, c \in A$. Si $c \mid ab$ y $a$ y $c$ son primos relativos, entonces $c \mid b$.*

**Demostración.**

Utilizando el lema de Bezout

$$1 = ax + cy$$

Multiplicamos por $b$

$$b = abx + cby$$

Como $c$ divide a cada sumando del segundo miembro (pues divide a $ab$) entonces $c$ divide a su suma, que no es otra que $b$. □

**Definición 5.6** *Dados dos elementos $a_1$ y $a_2$, decimos que un elemento $d \in A$ es un* mínimo común múltiplo *si*

- $a_1 \mid d$ *y* $a_2 \mid d$
- *Si* $a_1 \mid c$ *y* $a_2 \mid c$, *entonces* $d \mid c$

Si dos elementos son asociados y uno es un mínimo común múltiplo, entonces el otro también. Salvo esa ambigüedad, el mínimo común múltiplo es único.

**Proposición 5.6** *El mínimo común múltiplo de dos elementos es el generador del ideal intersección.*

**Demostración.**

Sean $a_1$ y $a_2$ los elementos en cuestión y sea $(d) = (a_1) \cap (a_2)$.

Tenemos que $(d) \subset (a_i)$, $\Rightarrow a_i \mid d$.

Si $a_i \mid c$, entonces $(c) \subset (a_i)$. Pero como la intersección es el mayor ideal contenido tanto en $(a_1)$ como en $(a_2)$, entonces $(c) \subset (d)$. Concluimos que $d \mid c$. □

Para el estudio de la divisibilidad debemos introducir un concepto análogo al de número primo en la aritmética.

**Definición 5.7** *Un elemento $p \in A$ es* primo *si no es invertible y si $p \mid ab \Rightarrow$ o bien $p \mid a$ o bien $p \mid b$.*

*Un elemento $m \in A$ es* irreducible *(o* no factorizable*) si en toda factorización $m = ab$, alguno de los factores es una unidad.*

Vamos a caracterizar a estos elementos por las propiedades de los ideales que generan.

**Teorema 5.7** *Sea $A$ un anillo. Se cumple:*

*1.- $m$ es irreducible si y solo si $(m)$ es un ideal maximal.*

*2.- $p$ es primo si y solo si $(p)$ es un ideal primo.*

**Demostración.**

1.– Sea $m$ irreducible. Si $(m) \subset (a)$ tenemos que $m = ab$. Si $a$ es invertible, $(a) = A$. Si el invertible es $b$ los elementos $m$ y $a$ son asociados y generan el mismo ideal. Así $(a)$ coincide con $(m)$ o es el total.

Si $(m)$ es maximal y $m$ pudiera factorizarse $m = ab$ donde ni $a$ ni $b$ fuesen invertibles, tendríamos que $(m) \subset (a)$ en sentido estricto y $(m)$ no sería maximal. Como esta contradicción no es posible debe ser imposible factorizar el elemento.

2.– Sea $p$ un elemento primo. Si $ab \in (p)$, entonces $p \mid ab$. Por lo tanto $p \mid a$ o $p \mid b$, lo que indica que $a \in (p)$ o $b \in (p)$. El ideal $(p)$ es entonces primo.

Si $(p)$ es primo y $p \mid ab$ tenemos que $ab \in (p)$. Luego uno de los dos está en $(p)$ y por lo tanto alguno es divisible entre $p$. □

**Corolario 5.8** *Todo elemento irreducible es primo.*

**Demostración.**

Todo ideal maximal es primo. □

**Corolario 5.9** *Si $a$ no es invertible en un DIP, existe un primo $p$ que lo divide.*

**Demostración.**

$(a)$ está contenido en un ideal maximal $(m)$, que es primo. Tenemos entonces $m \mid a$. $\square$

Los conceptos de irreducible y de primo son distintos en muchos anillos. Sin embargo en los DIP estos conceptos coinciden. Veamos el recíproco del corolario anterior.

**Proposición 5.10** *Sea $A$ un DIP. Todo ideal primo y no nulo es maximal.*

**Demostración.**

Sea $(p)$ un ideal primo y $(a)$ un ideal que lo contenga, $(p) \subset (a)$. Tenemos que $p = ac$ para algún elemento $c$ de $A$. Así $ac \in (p)$. Como $(p)$ es primo $a$ o $c$ deben estar en $(p)$. Si $a$ está en el ideal se cumple que $(a) = (p)$. Si es $c$ el que está tenemos que $p = ac = aad$. de donde se obtiene fácilmente que $a$ es una unidad y por lo tanto $(a) = A$. $\square$

**Corolario 5.11** *En un DIP un elemento es primo si y solo si es irreducible.*

**Corolario 5.12** *Si $A$ es un DIP, todo cociente de $A$ que sea íntegro es un cuerpo.*

**Ejemplos**

- Si $p$ es un número primo, también es irreducible, por lo que $\mathbb{Z}_p$ además de ser íntegro es un cuerpo. Este resultado ya nos era conocido pero lo hemos demostrado con otros argumentos.
- Consideremos en $\mathbb{R}(x)$ el polinomio $x^2 + 1$. Como el polinomio carece de raices, es irreducible. El cociente $\mathbb{R}(x)/(x^2 + 1)$ es un cuerpo. Designemos por $\pi$ la proyección canónica. El elemento $\pi(x)$ es solución

del polinomio $x^2+1$ en el nuevo cuerpo. Hemos encontrado un cuerpo donde el polinomio tiene solución y por lo tanto ya no es irreducible. Es fácil ver que el cuerpo $\mathbb{R}(x)/(x^2+1)$ es isomorfo a $\mathbb{C}$.

- Sea $k$ un cuerpo y $p$ un polinomio irreducible. El anillo $k(x)/(p)$ es un cuerpo. $\pi(x)$ es una raiz del polinomio en dicho cuerpo. De este modo el polinomio $p$ ya es reducible sobre dicho cuerpo. Tomando los factores de dicho polinomio y aplicando inducción vemos que siempre existe un cuerpo donde todo polinomio tiene todas las raices y por lo tanto se descompone en factores lineales.

El teorema fundamental de la aritmética nos dice que todo elemento de $\mathbb{Z}$ es producto de números primos. Además esta descomposición, salvo el orden y el producto por unidades, es única.

El proceso para encontrar la descomposición es el siguiente: tomamos un número $a \in \mathbb{Z}$. Si es primo, hemos terminado. Si no es primo, tiene un factor primo. Entonces $a = p_1 a_1$. Si $a_1$ es primo, hemos terminado. Si no lo es aplicamos el paso anterior al número $a_1$. Este proceso se sigue indefinidamente, pero debemos demostrar que en algún momento se termina. En el caso de los números enteros, se demuestra que el proceso termina puesto que $a_{i+1}$ es menor que $a_i$. El mismo razonamiento es válido también para anillos euclídeos. Sin embargo en el caso general de un DPI arbitrario necesitamos el siguiente

**Lema 5.13** *Sea $A$ un DIP. Dada una cadena creciente de ideales principales $I_1 \subset I_2 \subset \cdots \subset I_i \subset \ldots$, existe un entero $n$ tal que $I_m = I_n$ si $m > n$.*

**Demostración.**

Consideramos el conjunto unión $I = \cup I_i$. Este conjunto es un ideal del anillo. Por lo tanto está generado por un elemento $(a)$. Como dicho elemento pertenece a la unión, necesariamente estará en algún $I_i$. Sea $I_n$ el primer ideal que contiene a dicho generador. Entonces $I_m = I_n$ si $m > n$. $\square$

**Observación**

Los anillos que cumplen la propiedad enunciada en el lema anterior se denominan anillos noetherianos . Existen anillos noetherianos que nos DIP.

**Teorema 5.14** *Todo elemento de un DIP tiene una factorización como producto de elementos primos. Dicha factorización es única, salvo el orden y el producto por unidades.*

**Demostración.**

Veamos primero la existencia de la descomposición. Sea $a \in A$. Como el ideal $(a)$ está contenido en un maximal, existe un elemento primo (corolario 5.9) que divide a dicho elemento

$$a = p_1 a_1$$

Repetimos el proceso con $a_1$ y obtenemos

$$a_1 = p_2 a_2 \qquad \Rightarrow \qquad a = p_1 p_2 a_2$$

En general, aplicando inducción

$$a_i = p_{i+1} a_{i+1} \qquad \Rightarrow \qquad a = p_1 p_2 \dots p_{i+1} a_{i+1}$$

Con los elementos $a_i$ podemos formar una cadena puesto que $a_{i+1} \mid a_i$

$$(a_1) \subset (a_2) \subset \dots (a_i) \subset \dots$$

La cadena estaciona en un elemento $a_n$. Pero dicho elemento debe ser primo, pues si no lo fuera, la cadena seguiría ascendiendo.

Por lo tanto

$$a = p_1 p_2 \dots p_{i+1}$$

es una descomposición posible del elemento $a$ como producto de elementos primos.

Veamos la unicidad de la descomposición.

Sea $a = p_1 \dots p_n$ y $a = q_1 \dots q_m$. Tenemos que $p_1$ divide a $a$ y por tanto divide al producto $q_1 \dots q_m$. Como $p_1$ es primo necesariamente divide a algun elemento $q_i$. Reordenando dichos elementos podemos suponer sin perder generalidad que divide a $q_1$. Como ambos son primos, necesariamente generan el mismo ideal y los elementos están asociados. Tenemos entonces la ecuación

$$p_1 \dots p_n = u_1 p_1 q_2 \dots q_m$$

Como estamos en un anillo íntegro, podemos cancelar $p_1$ y mediante inducción probamos que $n = m$ y que los elementos $p_i$ y $q_i$ están asociados. Luego, salvo el orden y el producto por unidades, tenemos la unicidad. □

## Problemas

**5.1** Si $c \mid a$ y $c \mid b$, entonces $c \mid ax + by$ para todo $x, y$.

**5.2** Demostrar que dos elementos son asociados si y solo si se dividen mutuamente.

**5.3** Los elementos asociados con 1 son precisamente las unidades del anillo.

**5.4** Demostrar que si un anillo es íntegro, aunque no necesariamente un DIP, todo elemento primo es irreducible.

# 6. Localización

El propósito de este tema es construir anillos de fracciones. Las fracciones se construirán con elementos de un anillo $A$.

Estudiaremos en primer lugar un caso particular e importante: el cuerpo de fracciones de un anillo íntegro. Como siempre $A^*$ denota $A - \{0\}$.

**Lema 6.1** *En el conjunto $A \times A^*$ la relación $(a, b) \sim (a', b') \Leftrightarrow ab' = a'b$ es de equivalencia. La clase de equivalencia de $(a, b)$ se denota por la fracción $a/b$.*

**Demostración.**

Claramente es reflexiva y simétrica debido a la conmutatividad del anillo. Veamos que la transitividad

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc$$

$$(c, d) \sim (e, f) \Leftrightarrow cf = de$$

Tenemos que

$$adf = bcf = bde$$

Como $A$ es íntegro y $d \neq 0$ obtenemos que $af = be$ que demuestra que $(a, b) \sim (e, f)$. $\square$

**Definición 6.1** *El conjunto cociente $A \times A^*/\sim$ se designa $Q_A$ y se llama cuerpo de fracciones del anillo $A$.*

Introducimos en $Q_A$ las operaciones:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{db}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

El lector comprobará que en efecto dichas operaciones no dependen de los representantes que tomemos y que $Q_A$ es un cuerpo con dichas operaciones. Vease problema 1.21.

El elemento neutro para la suma es $0/1$, el neutro para el producto es $1/1$, el opuesto del elemento $a/b$ es $(-a)/b$ y el inverso $b/a$.

**Proposición 6.2** *La función*

$$\begin{array}{rccc} \varphi: & A & \to & Q_A \\ & a & \to & a/1 \end{array}$$

*es un morfismo de anillos inyectivo. Via este morfismo, podemos considerar a $A$ como un subanillo del cuerpo $Q_A$.*

**Demostración.**

$\varphi$ respeta la suma, el producto y el neutro gracias a la definición de las operaciones con fracciones.

Si $\varphi(a) = 0$ entonces $a/1 = 0$, lo que implica que $a = 0$ y que $\varphi$ es inyectivo. $\square$

**Proposición 6.3** *Si $A$ se puede inyectar en un cuerpo $k$, entonces $Q_A$ también se puede inyectar en el cuerpo $k$. $Q_A$ es el menor cuerpo que contiene a $A$.*

**Demostración.**

Sea $\varphi : A \longrightarrow k$ un morfismo inyectivo. Si queremos prolongar este morfismo a todo el cuerpo de fracciones, la única definición posible es asociarle a la fracción $a/b$ el elemento $\varphi(a)\varphi(b)^{-1}$. Así definimos $\varphi^* : Q_A \longrightarrow k$ por la fórmula

$$\varphi^*(\frac{a}{b}) = \varphi(a).\varphi(b)^{-1} = \frac{\varphi(a)}{\varphi(b)}$$

Si $a/b = c/d$ tenemos que $ad = cb$ y aplicando que $\varphi$ respeta la multiplicación $\varphi(a)\varphi(d) = \varphi(c)\varphi(b)$, lo que implica que la función $\varphi^*$ no depende de los representantes que tomemos.

Es rutinaria la comprobación de que en efecto $\varphi^*$ es morfismo de anillos, puesto que en el cuerpo $k$ las operaciones con fracciones son las habituales. (Problema 1.21).

Además $\varphi^*$ es inyectivo pues si

$$\varphi^*(\frac{a}{b}) = 0 \Rightarrow \varphi(a)\varphi(b)^{-1} = 0$$

Como $\varphi(b)$ no es nulo, necesariamente $\varphi(a) = 0$ y como $\varphi$ es inyectivo $a = 0$ y la fracción $a/b$ es nula.

Por lo tanto cualquier cuerpo $k$ que contenga a $A$, contiene también a $Q_A$, siendo este entonces el mínimo cuerpo que contiene a $A$. □

**Corolario 6.4** *Un anillo es íntegro si y solo si es un subanillo de un cuerpo.*

**Ejemplos**

- El cuerpo de fracciones de $\mathbb{Z}$ es $\mathbb{Q}$.
- Si $A = \mathbb{Z}(i)$, el cuerpo de fracciones es precisamente $\mathbb{Q}(i)$.
- Dado un anillo de polinomios, su cuerpo de fracciones está formado por todas las fracciones racionales.
- Si $A$ es un cuerpo, su cuerpo de fracciones es isomorfo a $A$.
- Todo cuerpo $k$ contiene un cuerpo isomorfo a $\mathbb{Z}_p$ o a $\mathbb{Q}$. En efecto, si $k$ tiene característica positiva $p$, existe un morfismo inyectivo de $\mathbb{Z}_p$ en $k$. Si $k$ tiene característica cero, $A$ es un subanillo de $k$ y por lo tanto $\mathbb{Q}$ también es subanillo de $k$. $\mathbb{Z}_p$ y $\mathbb{Q}$ son los únicos cuerpos que no poseen subcuerpos.

**Definición 6.2** *Sea $A$ un anillo. Un subconjunto $S \subset A$es* multiplicativo *si:*

- $1 \in S$
- $0 \notin S$
- *Si $a \in S$ y $b \in S$ entonces $ab \in S$*

Un subconjunto multiplicativo también se llama un sistema de denominadores de $A$.

Sea $S$ un subconjunto multiplicativo. En $A \times S$ introducimos la relación

$$(a, s) \sim (a', s') \text{ si existe } s'' \in S \text{ tal que } s''(as' - a's) = 0$$

**Lema 6.5** *La anterior relación es de equivalencia.*

**Demostración.**

Veamos la propiedad transitiva.

$$(a, s) \sim (b, t) \Leftrightarrow \text{ existe } s_1, \quad s_1(at - bs) = 0$$

$$(b, t) \sim (c, u) \Leftrightarrow \text{ existe } s_2, \quad s_2(bu - ct) = 0$$

Multiplicamos la primera igualdad por $s_2u$ y la segunda por $s_1s$. Así conseguimos eliminar la $b$ y nos queda

$$ats_1s_2u - cts_2s_1s = 0$$

Sacando factor común $ts_1s_2 \in S$ obtenemos que $(a, s) \sim (c, u)$. $\square$

El conjunto cociente de esta relación de equivalencia la denotamos $A_S$. La clase de equivalencia de $(a, s)$ se suele denotar por $a/s$ y debemos pensar en ella como en una fracción, donde los posibles denominadores son los elementos de $S$.

En $A_S$ y con nuestra notación, introducimos las operaciones

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'}$$

$$\frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}$$

**Proposición 6.6** *El conjunto $A_s$ junto con las operaciones inducidas es un anillo unitario. El neutro para la suma es $0/1$, el opuesto de $a/s$ es $-a/s$, el*

*neutro para el producto* $1/1$. *Si* $a \in S$, *entonces la fracción* $a/s$ *es invertible y su inverso es* $s/a$.

**Demostración.**

La única dificultad es demostrar que las operaciones no dependen de los representantes . Todas las propiedades de esta estructura de anillo son entonces evidentes. □

**Definición 6.3** *El anillo* $A_S$ *se dice que es el* anillo de fracciones *de* $A$ *con denominadores de* $S$.

Tenemos siempre una aplicación

$$\begin{array}{rccc} \varphi: & A & \longrightarrow & A_S \\ & a & \longrightarrow & a/1 \end{array}$$

que es morfismo de anillos. Debemos observar que, a diferencia de lo que ocurría en el cuerpo de fracciones, esta aplicación puede no ser inyectiva si el anillo $A$ no es íntegro.

**Teorema 6.7 (Propiedad universal)** *Sea* $\varphi : A \longrightarrow B$ *un morfismo de tal forma que* $\varphi(s)$ *sea invertible en* $B$ *para todo elemento de* $S$. *Entonces existe un único morfismo*

$$\varphi^* : A_S \longrightarrow B$$

*que cumple* $\varphi^*(a/1) = \varphi(a)$.

**Demostración.**

Si $\varphi^*$ debe ser morfismo, necesariamente se cumple

$$\varphi^*(a/s) = \varphi(as^{-1}) = \varphi(a)\varphi(s^{-1}) = \varphi(a)\varphi(s)^{-1}$$

Por lo tanto adoptaremos como definición de $\varphi^*$ la fórmula

$$\varphi^*(a/s) = \varphi(a)\varphi(s)^{-1}$$

Tenemos que ver que $\varphi^*$ no depende de los representantes.

Si $a/s = a'/s'$ entonces $s''(as' - a's) = 0$. Aplicando $\varphi$ a esta expresión obtenemos

$$\varphi(s'')(\varphi(a)\varphi(s') - \varphi(a')\varphi(s)) = 0$$

y como $\varphi(s'')$ es unidad es cancelable y obtenemos que

$$\varphi(a)\varphi(s') = \varphi(a')\varphi(s)$$

lo que demuestra que $\varphi^*(a/s) = \varphi(a'/s')$.

Que conserva la suma, el producto y la unidad es de fácil comprobación. □

**Ejemplos**

- Sea $a \in A$ no nilpotente. $S = \{a_n\}_{n\geq 0}$ es un subconjunto multiplicativo. Las fracciones tienen como denominadores potencias de $a$. En este caso el anillo se suele denotar $A_a$ en vez de $A_S$.

- Sea $\mathfrak{p}$ un ideal primo. $S = A - \mathfrak{p}$ es multiplcativo. En este caso $A_S$ se denota $A_\mathfrak{p}$. Los denominadores en este caso no contienen elementos de $\mathfrak{p}$. El conjunto

  $$\mathfrak{m} = \{a/s \text{ con } a \in \mathfrak{p}\}$$

  es un ideal de $A_\mathfrak{p}$. Este ideal es maximal, pues todos los elementos que no están en $\mathfrak{m}$ son invertibles. Además este es único ideal maximal del anillo.

- El cuerpo de fracciones de un anillo íntegro.

- Sea $S_0$ el conjunto de todos los elementos de $A$ que no son divisores de cero. $S_0$ es un subconjunto multiplicativo y $A_{S_0}$ se denomina anillo total de fracciones de $A$. En este caso la aplicación canónica $\varphi : A \longrightarrow A_{S_0}$ es inyectiva.

**Definición 6.4** *Un anillo $A$ es* local *si tiene un único ideal maximal.*

Todos los anillos $A_{\mathfrak{p}}$ son locales. Decimos que $A_{\mathfrak{p}}$ es el localizado de $A$ en el "punto" $\mathfrak{p}$.

El proceso que nos transforma $A$ en $A_{\mathfrak{p}}$ se denomina localización.

**Proposición 6.8** *Sea $\varphi : A \longrightarrow A_S$ el morfismo natural. Existe una correspondencia biunívoca entre los ideales primos de $A_S$ e ideales primos que no cortan a $S$, dada por la fórmula $\mathfrak{p} \longleftrightarrow \varphi^{-1}(\mathfrak{p})$.*

**Demostración.**

Al lector. □

## Problemas

**6.1** Sea $A$ un anillo íntegro y $k$ su cuerpo de fracciones.

- Si a una fracción $a/b$ se le multiplica denominador y numerador por un mismo elemento no nulo de $A$, la fracción no cambia.
- Generalizar el resultado anterior a los anillo $A_S$.
- Utilizar los resultados anteriores para simplificar fracciones.

# 7. Espectro

En teoría de anillos se introduce la noción de espectro para intentar conseguir que todos los anillos se puedan entender como anillos de funciones.

**Definición 7.1** *Sea $A$ un anillo conmutativo. El espectro de $A$ es el conjunto de los ideales primos de $A$. Lo denotaremos por* $\mathrm{Spec}(A)$. *El conjunto total no lo consideraremos ideal primo.*

Para nosotros, de ahora en adelante, un ideal primo lo podemos entender como un subconjunto de $A$ o como un punto del espacio $\mathrm{Spec}(A)$. Si pensamos en el ideal primo como un punto de $\mathrm{Spec}(A)$, lo denotaremos por una letra, por ejemplo $x$. Si lo entendemos como un subconjunto de $A$ lo denotaremos $\mathfrak{p}_x$.

**Lema 7.1** *Si $x \in \mathrm{Spec}(A)$, entonces $A/\mathfrak{p}_x$ es un anillo íntegro. El cuerpo de fracciones de este anillo se denota $k(x)$ y se dice que es el* cuerpo residual *del punto $x$.*

**Demostración.**

Sabemos que $\mathfrak{p}_x$ es un ideal primo que no es el total. Así $A/\mathfrak{p}_x$ es un anillo íntegro y no nulo. Su cuerpo de fracciones tampoco será nulo. □

Dado un elemento $f \in A$ y un punto $x$ del espectro, consideramos la clase de equivalencia de $f$ módulo $\mathfrak{p}_x$. Dicha clase de equivalencia se denota $f(x)$ y se dice que es el valor que toma la "función" $f$ en el punto $x$. Por lo tanto tenemos que $f(x) \in A/\mathfrak{p}_x$. Con ello vemos que todo elemento de $A$ se puede entender como una función con dominio $\mathrm{Spec}(A)$, pero con el problema de que el conjunto imagen cambia con el punto $x$.

**Definición 7.2** *Llamamos* puntos *a los elementos de* $\mathrm{Spec}(A)$. *Llamamos* funciones *a los elementos de $A$. Una función $f \in A$ se anula en un punto $x$ si $f(x) = 0$.*

**Ejemplos**

- La función 0 se anula en todos los puntos.
- Dado $x \in \mathrm{Spec}(A)$, el conjunto de funciones que se anulan en $x$ es precisamente $\mathfrak{p}_x$.
- Si dos funciones se anulan en $x$, su suma y su producto también se anulan en dicho punto.
- Si un producto de dos funciones se anula en un punto, alguno de los factores se anula en el punto. Esta propiedad es consecuencia de la integridad de los anillos $A/\mathfrak{p}_x$.
- Las funciones invertibles son precisamente aquellas que no se anulan nunca, pues todo elemento no invertible está contenido en un ideal maximal.
- Decimos que un punto del espectro es real cuando su cuerpo residual sea el de los números reales. Análogamente con cualquier otro cuerpo.
- Si una función se anula en todos los puntos, dicha función es nilpotente. Recordemos que la intersección de todos los ideales primos es el radical del anillo y que está formado por los elementos nilpotentes.

Si $A$ es un anillo y $\mathfrak{r}$ su radical, los ideales primos de $A$ y de $A/\mathfrak{r}$ están en correspondencia biunívoca, pues todo ideal primo de $A$ contiene a $\mathfrak{r}$. Entonces el espectro de $A$ y de $A/\mathfrak{r}$ son canónicamente isomorfos.

**Definición 7.3** *Dado un anillo $A$ se llama anillo reducido al cociente $A/\mathfrak{r}$.*

Un anillo y su anillo reducido tienen el mismo espectro, pero como el anillo reducido no tiene radical, no existen funciones no nulas que se anulen en todos los puntos.

**Ejemplos**

- El espectro de un cuerpo tiene un único punto.

- El espectro de todos los anillos íntegros tiene un punto correspondiente al ideal nulo. Dicho punto es denso puesto que el cero está contenido en todo ideal primo. Ese punto se denomina punto genérico .

- Si $k$ es un cuerpo, el espectro de $k^n$ tiene $n$ puntos. Todos esos puntos tienen de cuerpo residual $k$.

- Espectro de $\mathbb{Z}$. Está formado por todos los números primos positivos y por el cero. El 1 no pertenece puesto que el ideal que genera es el total.

- Espectro de $\mathbb{C}(X)$. Si un polinomio $p$ es primo, $p$ es de la forma $(x-a)$ donde $a \in \mathbb{C}$. Así para cada punto de $\mathbb{C}$, Spec$(\mathbb{C}(X))$ tiene un punto complejo. Como es íntegro tiene un punto genérico. El mismo esquema es válido para cualquier cuerpo algebraicamente cerrado.

- Espectro de $\mathbb{R}(X)$. Los polinomios irreducibles sobre $\mathbb{R}$ pueden ser de dos tipos. El primer tipo es $(x-a)$ donde $a \in \mathbb{R}$. Los otros polinomios irreducibles son los de segundo grado con raices complejas conjugadas. Son de la forma $(x-z)(x-\bar{z})$ donde $z \in \mathbb{C}$. Para cada número real $a$ el espectro tiene un punto real, $(x-a)$. Para cada número complejo $z$ situado en el semiplano superior el espectro tiene un punto complejo, $(x-z)(x-\bar{z})$. Tiene también un punto genérico.

- Sea $A = C(\mathbb{R}^n, \mathbb{R})$. A cada punto $x \in \mathbb{R}^n$ le podemos asociar el ideal $\mathfrak{m}_x$ formado por las funciones que se anulan en $x$. El ideal $\mathfrak{m}_x$ es maximal. De este modo podemos considerar a $\mathbb{R}^n$ como un subconjunto del espectro de su anillo de funciones. El estudio de esta construcción para espacios topólogicos más generales tiene gran importancia en topología, pues es la base de la llamada compactificación de Stone-Cech.

- Si $k$ es un cuerpo a cada polinomio mónico e irreducible le corresponde un punto del espectro. Como el anillo de polinomios es principal esta correspondencia es biunívoca. Además de estos tiene un punto genérico.

- Si $k$ es un cuerpo y $p$ es un polinomio, el espectro del anillo $k(x)/p$ tiene un punto cerrado por cada factor irreducible del polinomio $p$.

- Sea $A$ es un dominio de ideales principales. Dos elementos están asociados si se obtienen uno del otro mediante la multiplicación por una unidad. A cada clase de equivalencia de elementos irreducibles le corresponde un punto del espectro y recíprocamente. El espectro está formado por los puntos $(a)_0$ donde $a$ recorre el conjunto de clases de elementos irreducibles.

- Consideremos el anillos $k(x_1, \ldots, x_n)$ de los polinomios en $n$ variables. Dados $n$ elementos $a_i$ de $k$, consideramos la función del anillo de polinomios en $k$ definida por las relaciones $f(x_i) = a_i$. El núcleo de esta función es el ideal maximal generado por los monomios $(x_i - a_i)$. De esta forma $k^n$ puede considerarse inyectado en el espectro del anillo de polinomios de $n$ variables. Es claro que todos estos puntos tienen como cuerpo residual $k$.

- Si en el ejemplo anterior tomamos elementos de una extensión $K$ del cuerpo $k$, tendremos morfismos del anillo de polinomios $k(x_1, \ldots, x_n)$ en $K$. Ahora los morfismos no tienen porque ser epiyectivos, pero aun así el núcleo si será un ideal primo debido a la integridad de $K$. En este caso el cuerpo residual no será $k$.

El espectro de un anillo, además de ser un simple conjunto, puede ser dotado de una estructura de espacio topológico. Vamos a definir la topología dando los cerrados del espacio.

**Definición 7.4** *Sea $S$ un subconjunto de $A$. Los* ceros *de $S$ son los puntos $x \in \mathrm{Spec}(A)$ donde se anulan todas las funciones de $S$. Se denota $(S)_0$. Tenemos entonces*

$$(S)_0 = \{x \in \mathrm{Spec}(A) \text{ tales que } f(x) = 0 \text{ para todo } f \in S\}$$

**Lema 7.2** *Dado un conjunto $S$ sea $I$ el ideal que generan $I =< S >$. Entonces $(S)_0 = (I)_0$.*

**Demostración.**

Como $S \subset I$ obtenemos que $(I)_0 \subset (S)_0$. Todo elemento de $I$ se puede escribir como una combinación lineal de elementos de $S$. Si $\sum a_i s_i$ es un elemento de $I$ y $x \in (S)_0$ tenemos que $(\sum a_i s_i)(x) = \sum a_i(x) s_i(x)$ aplicando que la proyección canónica es morfismo de anillos. Pero este último resultado es nulo por lo que $x \in (I)_0$. Concluimos que $(S)_0 \subset (I)_0$. $\square$

Gracias a este resultado podremos siempre suponer que el subconjuto $S$ es un ideal, lo que nos ahorrará bastante trabajo en las demostraciones.

En particular si $f \in A$, $(f)_0$ es el conjunto de los puntos donde se anula la función $f$. También lo podemos entender como el conjunto de ideales que contienen a $f$.

**Proposición 7.3** *Se cumple:*

*1.-* $(0)_0 = \mathrm{Spec}(A)$ *donde* $0$ *denota el ideal nulo.*

*2.-* $(A)_0 = \emptyset$.

*3.-* $(\sum I_j)_0 = \cap (I_j)_0$ *para toda familia de ideales.*

*4.-* $(I \cap J)_0 = (I)_0 \cup (J)_0$

**Demostración.**

1.- La función cero se anula en todos los puntos.

2.- La función 1 no se anula nunca.

3.- Si $x \in \cap (I_j)_0$ entonces $f_j(x) = 0$ para todo elemento $f_j \in I_j$. Por lo tanto $(\sum f_j)(x) = 0$ y como todo elemento de $\sum I_j$ es de esta forma, $x \in (\sum I_j)_0$.

$I_j \subset \sum I_j$. Entonces $(\sum I_j)_0 \subset (I_j)_0$ para todo $j$. Tenemos entonces que $(\sum I_j)_0 \subset \cap (I_j)_0)$ lo que prueba la inclusión que nos faltaba.

4.- Sabemos por la proposición 3.9 que si un ideal primo $\mathfrak{p}$ contiene a $I \cap J$, entonces contiene a uno de los dos ideales. $\square$

Estas propiedades nos permiten dar la siguiente definición:

**Definición 7.5** *Llamamos cerrados de* $\mathrm{Spec}(A)$ *a los subconjuntos de la forma* $(I)_0$*, donde* $I$ *es un ideal. Estos cerrados forman la* topología de Zariski.

Siempre que nos refiramos a la topología del espectro, supondremos que es la de Zariski.

**Corolario 7.4** *Se cumple la fórmula*

$$(S)_0 = \bigcap_{f \in S} (f)_0$$

Este corolario prueba que los conjuntos $(f)_0$ forman una base de cerrados de la topología.

El complementario del subconjunto $(f)_0$ se denota $U_f$.

$$U_f = \mathrm{Spec}(A) - (f)_0 = \{x \in \mathrm{Spec}(A) \text{ tales que } f(x) \neq 0\}$$

Todo abierto de la topología es unión de este tipo de abiertos, que forman entonces una base de la topología de Zariski.

**Proposición 7.5** *El cierre de un punto* $x \in \mathrm{Spec}(A)$ *es precisamente* $(\mathfrak{p}_x)_0$.

**Demostración.**

Un cerrado $(I)_0$ contiene a $x$ si $x \in (I)_0$. Esto es equivalente a que $I \subset \mathfrak{p}_x$. Tomando ceros en esta expresión obtenemos que $(\mathfrak{p}_x)_0 \subset (I)_0$ y $(\mathfrak{p}_x)_0$ está contenido en todos los cerrados que contienen a $x$. □

**Corolario 7.6** *Un punto es cerrado si su ideal asociado es maximal.*

**Demostración.**

Si $\mathfrak{p}_x$ es maximal el conjunto $(\mathfrak{p}_x)_0$ tiene solo un punto, que es precisamente $x$. El cierre del punto $x$ coincide con $x$, lo que implica que es cerrado. □

**Teorema 7.7** *El espectro es un espacio topólogico compacto.*

**Demostración.**

Sea $(I_j)_0$ una familia de cerrados de intersección vacía. En virtud de la proposición 7.3

$$\bigcap (I_j)_0 = \emptyset = (\sum I_j)_0$$

Entonces $\sum I_j = A$ puesto que $A$ es el único ideal que no está contenido en ningún ideal primo.

Como $1 \in A$ y $A = \sum I_j$, existe un número finito de funciones tales que

$$f_1 + \cdots + f_n = 1$$

Si $f_i \in I_{j_i}$ la misma proposición nos asegura que

$$(I_{j_1})_0 \cap \cdots \cap (I_{j_n})_0 = (I_{j_1} + \cdots + I_{j_n})_0 = \emptyset$$

y una subfamilia finita de cerrados tiene intersección vacía. Esto demuestra que el espectro es compacto. $\square$

Dado un morfismo de anillos

$$\varphi : A \longrightarrow B$$

y un ideal primo $\mathfrak{p}$ de $B$, sabemos que $\varphi^{-1}(\mathfrak{p})$ es un ideal primo de $A$. Esto nos permite definir una aplicación

$$\begin{array}{rccc} \varphi^* : & \mathrm{Spec}(B) & \longrightarrow & \mathrm{Spec}(A) \\ & \mathfrak{p} & \longrightarrow & \varphi^{-1}(\mathfrak{p}) \end{array}$$

Si $\phi$ es otro morfismo, $(\varphi\phi)^* = \phi^*\varphi^*$ lo que pone de manifiesto que esta construcción es un funtor contravariante.

**Teorema 7.8** $\varphi^*$ *es una aplicación continua.*

**Demostración.**

Sea $C = (I)_0$ un cerrado de $\mathrm{Spec}(A)$. Veamos que $(\varphi^*)^{-1}$ es cerrado

$$(\varphi^*)^{-1}(I) = \{x \in \mathrm{Spec}(B) \text{ tales que } I \subset \varphi^{-1}(\mathfrak{p}_x)\}$$

Aplicando el morfismo $\varphi$ tenemos que este conjunto coincide con

$$\{x \in \mathrm{Spec}(B) \text{ tales que } \varphi(I) \subset \mathfrak{p}_x\} = (\varphi(I))_0$$

que es un cerrado de $\mathrm{Spec}(B)$, pues coincide con el conjunto de ceros del ideal generado por $\varphi(I)$. $\square$

Veamos ahora como se comporta el espectro al realizar cocientes y productos de anillos

**Corolario 7.9** *Si $I$ es un ideal de $A$ y $\pi : A \longrightarrow A/I$ la proyección canónica, $\pi^* : \mathrm{Spec}(A/I) \longrightarrow \mathrm{Spec}(A)$ establece un homeomorfismo de $\mathrm{Spec}(A/I)$ con el cerrado $(I)_0$.*

**Demostración.**

Aplicando el teorema de correspondencia, los ideales primos de $A/I$ se identifican con los ideales primos de $A$ que contienen a $I$. Pero este conjunto es precisamente $(I)_0$. Dejamos al lector la comprobación de que en efecto es un homeomorfismo. $\square$

**Lema 7.10** *Dado un producto de anillos $A_1 \times A_2$, los ideales de este anillo son de la forma $I_1 \times I_2$ donde $I_i \subset A_i$ es un ideal.*

**Demostración.**

Sea $I \subset A_i \times A_2$. Denotemos por $I_i$ la proyección de $I$ en el $i$-ésimo factor. $I_i$ es un ideal puesto que la proyección canónica es epiyectiva.

Dado un elemento $(a_1, a_2)$, tenemos que tanto $(a_1, 0)$ como $(0, a_2)$ son múltiplos de dicho elemento. Por lo tanto $(a_1, a_2) \in I$ si y solo $a_1 \in I_1$ y $a_2 \in I_2$, lo que prueba que $I = I_1 \times I_2$. $\square$

**Corolario 7.11** *Los ideales primos de $A_1 \times A_2$ son de la forma $\mathfrak{p}_1 \times A_2$ o de la forma $A_1 \times \mathfrak{p}_2$ donde $\mathfrak{p}_i \subset A_i$ es primo.*

**Demostración.**

Si hacemos el cociente de $A_1 \times A_2$ módulo el ideal $I_1 \times I_2$ obtenemos

$$(A_1 \times A_2)/(I_1 \times I_2) = A_1/I_1 \times A_2/I_2$$

Para que este producto sea íntegro debe ocurrir que un factor sea nulo y el otro factor sea íntegro. Pero esto equivale a decir que un ideal es el total y el otro un ideal primo. □

**Teorema 7.12** *El espectro del producto $A_1 \times A_2$ es la unión disjunta de los espectros de los anillos $A_1$ y $A_2$.*

**Demostración.**

Los resultados anteriores prueban que como conjuntos

$$\mathrm{Spec}(A_1 \times A_2) = \mathrm{Spec}(A_1) \oplus \mathrm{Spec}(A_2)$$

(La suma directa en la categoría de espacios topológicos es la unión disjunta)

Sea $\pi_i : A_1 \times A_2 \longrightarrow A_i$ la proyección canónica. Tenemos entonces que

$$\pi_1{}^* : \mathrm{Spec}(A_1) \longrightarrow \mathrm{Spec}(A_1 \times A_2)$$

es un homeomorfismo con su imagen, lo que prueba que la igualdad también es cierta como espacios topológicos. □

## Problemas

**7.1** Demostrar que se cumple las fórmulas

- $U_f \cap U_g = U_{fg}$
- $U_f = \mathrm{Spec}(A)$ si y solo si $f$ es una unidad.
- $U_f = \emptyset$ si y solo si $f$ es nilpotente.

**7.2** Sea $S \subset A$ un sistema de denominadores y $\varphi : A \longrightarrow A_S$ la aplicación natural de $A$ en su localizado.

Demostrar que $\varphi^* : \mathrm{Spec}(A_S) \longrightarrow \mathrm{Spec}(A)$ es inyectiva y que su imagen está formada por los ideales primos que tienen intersección vacía con $S$.

**7.3** Además de la estructura topológica, aunque asociada a ella, se puede definir un relación de orden en el espectro de un anillo.

Decimos que $x \leq x'$ si $\mathfrak{p}_x \subset \mathfrak{p}_{x'}$.

- Un punto es más "pequeño" cuanto más "grande" sea el ideal asociado.
- Esta relación de orden tiene elementos minimales. Un punto es minimal si no existen puntos menores. Los elementos minimales son los asociados a los ideales maximales del anillo.
- ¿Cuáles son los elementos maximales?

# 8. Extensiones enteras

**Definición 8.1** *Sea $B$ un anillo y $A \subset B$ un subanillo con unidad. Un elemento $b \in B$ es* entero *sobre $A$ si existe un polinomio unitario*[1]*, con coeficientes en $A$, que anula a dicho elemento.*

Si el polinomio es

$$p = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

entonces $b$ cumple la ecuación polinomial

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

El elemento $b$ es entonces una raiz de un polinomio cuyo término de mayor grado es uno.

**Observación**

En general en teoría de anillos se denomina extensión de un anillo $A$ a todo morfismo de anillos con unidad $\varphi : A \to B$. La imagen de $A$ mediante $\varphi$ es un subanillo de $B$. En esta situación diremos que un elemento de $B$ es entero sobre $A$, si entero sobre el subanillo imagen $\varphi(A)$.

**Proposición 8.1** *Sea $B$ una extensión entera de un anillo $A$. El subanillo $A(b) \subset B$, generado por el anillo $A$ y el elemento $b$, es un módulo de generación finita sobre el anillo $A$.*

**Demostración.**

Tenemos que

$$b^n = -(a_0 + a_1 b + \cdots + a_{n-1}b^{n-1})$$

y en general

$$b^{n+r} = -(a_0 b^r + a_1 b^{r+1} + \cdots + a_{n-1}b^{n+r-1})$$

[1]Decimos que un polinomio es unitario si el coeficiente de mayor grado es 1. También se dice que el polinomio es mónico.

por lo que los elementos $1, b, \ldots, b^{n-1}$ generan dicho módulo. $\square$

**Proposición 8.2** *Sea $A \subset B$ un subanillo. Si $b \in B$ es entero sobre $A$, entonces el morfismo $\varphi : A(x) \to B$ que transforma $x$ en $b$ no es inyectivo.*

**Demostración.**

Si $b$ es entero sobre $A$, existe un polinomio $p \in A(x)$ que anula al elemento $b$. Pero como $\varphi(p) = p(b)$ dicho elemento está en el núcleo de $\varphi$, que no puede entonces ser inyectivo. $\square$

**Ejemplos**

- Todo elemento de $A$ es entero sobre $A$ puesto que $x - a$ anula a dicho elemento.
- El número real $\sqrt[3]{2}$ es entero sobre $\mathbb{Z}$. Un polinomio que lo anula es precisamente $x^3 - 2$.
- El número complejo $i$ es entero sobre $\mathbb{Z}$. Encontrar un polinomio que lo anule. En general, todo elemento de la forma $a + bi$ con $a$ y $b$ enteros, es entero sobre $\mathbb{Z}$.
- Consideramos el número real $1/\sqrt{2}$. Un polinomio que anula a dicho elemento es $2x^2 - 1$. Sin embargo dicho elemento no es entero sobre $\mathbb{Z}$, pues no existe ningún polinomio unitario que lo anule.
- Si un número racional es entero sobre $\mathbb{Z}$ entonces necesariamente es un elemento de $\mathbb{Z}$. Demostremos este hecho.

  Sea $r/s$ la fracción irreducible del número racional. Entonces dicho número cumple una ecuación del tipo

$$\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1\left(\frac{r}{s}\right) + a_0 = 0$$

Multiplicamos por $s^n$ para quitar denominadores

$$r^n + a_{n-1}sr^{n-1} + \cdots + a_1rs^{n-1} + a_0s^n = 0$$

Sacando factor común $s$ deducimos

$$r^n = s(-a_{n-1}r^{n-1} - \cdots - a_1rs^{n-2} - a_0s^{n-1})$$

Entonces $s$ divide a $r^n$ y por lo tanto divide a $r$. Como la fracción es irreducible, necesariamente $s = \pm 1$ y el número es entero.

- En el caso de los cuerpos, el estudio de la dependencia entera se simplifica utilizando conceptos elementales de la teoría de espacios vectoriales. Veamos un ejemplo.

  Sea $k$ un cuerpo, $k \subset B$ y $B$ un anillo que como espacio vectorial sea de dimensión finita $n$ sobre el cuerpo $k$. Los elementos $1, b, \ldots, b^n$ no pueden ser linealmente independientes. Luego existe una combinación lineal no nula

  $$a_0 1 + a_1 b + \cdots + a_n b^n = 0$$

  Construimos de este modo un polinomio, de grado menor o igual a $n$ que anula al elemento $b$. Pero en principio este polinomio no es unitario. Si $i$ es el grado del polinomio, entonces podemos dividir entre $a_i$ y obtenemos un polinomio cuyo término de mayor grado es uno. Como conclusión, tenemos que si $B$ es de dimensión finita sobre $k$, entonces todo elemento de $B$ es entero sobre $k$.

Llamamos extensión de un anillo $A$ a cualquier anillo $B$ que lo contenga. Estamos especialmente interesados en aquellos anillos $B$ tales que todos sus elementos sean enteros sobre $A$.

**Definición 8.2** *Una extensión $A \subset B$ es* entera *si todo elemento de $B$ es entero sobre $A$. En el caso de que $A$ sea un cuerpo, las extensiones enteras se denominan extensiones* algebraicas.

**Ejemplos**

- El cuerpo $\mathbb{C}$ es una extensión entera de $\mathbb{R}$. En general toda extensión $k \subset B$ de un cuerpo, que sea de dimensión finita, es una extensión entera. El recíproco sin embargo no es cierto. Existen extensiones de dimensión infinita que son enteras.

- $\mathbb{Z} \subset \mathbb{Z}(i)$ es una extensión entera.

- $\mathbb{Z} \subset \mathbb{Q}$ no es entera, puesto que existen elementos en $Q$ que no son enteros sobre $\mathbb{Z}$.

- $\mathbb{R}$ tampoco es entero sobre $\mathbb{Q}$. En general, los números reales (o complejos) que son enteros sobre $\mathbb{Q}$ se denominan números algebraicos . Aquellos que no son enteros se denominan transcendentes.

  Es un ejercicio fácil demostrar que el conjunto de números algebraicos es numerable. Esto implica la existencia de números transcendentes. Sin embargo encontrar ejemplos explícitos de números transcendentes no es tarea fácil. Se sabe, no obstante, que $e$ y $\pi$ son números transcendentes.

Hemos dado una definición de elemento entero sobre $A$. Daremos ahora un criterio, o definición equivalente, que nos será útil en multitud de cálculos.

**Proposición 8.3** *Sea $A \subset B$ una extensión. Son equivalentes las siguientes condiciones:*

I) *El elemento $b$ es entero sobre $A$.*

II) *El módulo $A(b)$ es de generación finita sobre el anillo $A$.*

III) *El elemento $b$ está incluido en un anillo $C$ que es un $A$-módulo de generación finita.*

**Demostración.**

La implicación $i) \Rightarrow ii)$ es justamente la proposición 8.1. Para la implicación $ii) \Rightarrow iii)$ basta tomar $C = A(b)$. Veamos entonces la implicación $iii) \Rightarrow i)$.

Sea $C$ un módulo de generación finita que contenga al elemento $b$. Denotaremos por $(m_1, \ldots, m_n)$ un conjunto de generadores de $C$ como $A$-módulo. Tenemos que $bm_i$ es un elemento de $C$ y por lo tanto se puede escribir, en principio de forma no única, como una combinación lineal de elementos del conjunto generador.

$$bm_i = a_{i1}m_1 + \cdots + a_{in}m_n$$

Esto nos da un sistema de $n$ ecuaciones con $n$ incognitas. Los elementos $a_{ij}$ forman una matriz cuadrada, donde los coeficientes pertenecen al anillo $A$.

Pasamos los elementos $bm_i$ al otro miembro y obtenemos un sistema equivalente y homogéneo. La matriz de este sistema es precisamente $(a_{ij} - b\delta_{ij})$. Calculamos el determinante de esta matriz. Dicho determinante es un elemento de $B$ que tiene la forma de un polinomio unitario[2] en $B$. Si denotamos por $\Delta$ a dicho determinante, tenemos que $\Delta m_i = 0$ para todo generador del módulo. Como el anillo tiene unidad, en particular el 1 es combinación de elementos $m_i$ y obtenemos que $\Delta 1 = 0$. Necesariamente $\Delta = 0$ y hemos obtenido un polinomio unitario que anula a $b$. $\square$

**Corolario 8.4** *Sea $A \subset B$ una extensión. Si $B$ es de generación finita como $A$-módulo, entonces $B$ es una extensión entera de $A$.*

**Observación**

Si $A = k$ es un cuerpo, los anillos finito generados son precisamente aquellos que tienen dimensión finita y este resultado ya nos era conocido.

**Lema 8.5** *Sea $A \subset B \subset C$ una cadena de anillos. Si $B$ es de generación finita como $A$-módulo y $C$ es de generación finita como $B$-módulo, entonces $C$ es también de generación finita como $A$ módulo.*

**Demostración.**

Sea $(c_1, \ldots, c_n)$ un conjunto generador de $C$ como $B$ módulo. Denotamos por $(b_1, \ldots, b_m)$ un conjunto generador de $B$ como $A$-módulo.

[2]El término de mayor grado puede ser $\pm b^n$ dependiendo de si $n$ es par o impar

Dado un elemento arbitrario $c \in C$, tenemos que

$$c = \beta_1 c_1 + \cdots + \beta_n c_n \text{ donde los } \beta_i \in B$$

Cada $\beta_i$ se puede expresar como una combinación lineal finita de los elementos $b_i$

$$\beta_i = a_{i1} b_1 + \cdots + a_{im} b_m \text{ con } a_{ij} \in A$$

Sustituyendo esto en la anterior expresión de $c$, obtenemos que los elementos $b_i c_j, i = 1, \ldots, m, j = 1, \ldots, n$ generan $C$ como $A$-módulo. □

**Corolario 8.6** *Sea $A \subset B$ una extensión. Si los elementos $b_1, \ldots, b_n$ son enteros sobre $A$, entonces el anillo $A(b_1, \ldots, b_n)$ es de generación finita.*

**Demostración.**

Consideramos la cadena de anillos

$$A \subset A(b_1) \subset A(b_1, b_2) \subset \cdots \subset A(b_1, \ldots, b_n)$$

Cada extensión es de generación finita, pues si un elemento $b_i$ es entero sobre $A$, también es entero sobre $A(b_1, \ldots, b_{i-1})$. Aplicando inducción y el lema anterior concluimos. □

**Corolario 8.7** *Sea $A \subset B$ una extensión. Si $b_1$ y $b_2$ son enteros sobre $A$, entonces $b_1 + b_2$ y $b_1 b_2$ son enteros sobre $A$.*

**Demostración.**

Si $b_1$ y $b_2$ son enteros, entonces $A(b_1, b_2)$ es de generación finita y todos sus elementos son enteros sobre $A$. En particular $b_1 + b_2$ y $b_1 b_2$ , que son elementos de dicho anillo, son enteros sobre $A$. □

Del corolario anterior se deduce que el conjunto de todos los elementos enteros de una extensión es un subanillo de $B$.

**Definición 8.3** *Sea $A \subset B$ una extensión. Denotamos por $\widetilde{A}$ al conjunto de los elementos de $B$ que son enteros sobre $A$. El conjunto $\widetilde{A}$ se denomina* clausura íntegra *del anillo $A$ en $B$.*

Como ya hemos anunciado, $\widetilde{A}$ es un subanilo de $B$. Si en una extensión tenemos que $\widetilde{A} = A$, decimos que$A$ es integramente cerrado (en B). Como ya sabemos, si $\widetilde{A} = B$ decimos que $B$ es entero sobre $A$.

En el caso de un dominio de integridad, si decimos que es íntegramente cerrado estaremos suponiendo que dicho anillo es íntegramente cerrado en la extensión dada por su cuerpo de fracciones.

En el caso de los cuerpos la cosa queda más o menos así. En un cuerpo no se diferencian los polinomios unitarios y no unitarios, pues si nos dan un polinomio no unitario, simplemente lo dividimos entre el coeficiente de mayor grado y obtenemos un polinomio unitario. Los elementos algebraicos sobre un cuerpo $k$ son los elementos de un cuerpo $K$ que son raices de los los polinomios con coeficientes en $k$. Si todos los polinomios en $k$ tienen al menos una raiz en el cuerpo base, por inducción vemos que tienen tantas como su grado también en el cuerpo raiz. De este modo, si todo polinomio tiene una raiz en el cuerpo base, no pueden existir extensiones algebraicas (enteras) del cuerpo. Los cuerpos que no admiten extensiones algebraicas se denominan algebraicamente cerrados.

**Corolario 8.8** *Sea $A \subset B \subset C$. Si $B$ es entero sobre $A$ y $C$ es entero sobre $B$, entonces $C$ es entero sobre $A$.*

**Demostración.**

Sea $c \in C$. Entonces $c$ cumple una ecuación polinomial

$$c^n + b_{n-1}c_{n-1} + \cdots + b_1 c + b_0 = 0 \text{ con } b_i \in B$$

El anillo $A(b_0, b_1, , \ldots, b_{n-1}, c)$ es de generación finita sobre $A$, puesto que $c$ es entero sobre el anillo $A(b_0, b_1, \ldots, b_{n-1})$ y este último anillo es de generación finita pues todos los elementos de $B$ son enteros. De este modo concluimos que $c$ es entero sobre $A$. $\square$

**Corolario 8.9** *Sea $A \subset B$ una extensión y $\widetilde{A}$ la clausura entera de $A$ en $B$. Entonces $\widetilde{A}$ es integramente cerrado en $B$.*

**Demostración.**

Consideramos la cadena $A \subset \widetilde{A} \subset B$. Si $b \in B$ es entero sobre $\widetilde{A}$, entonces también es entero sobre $A$. De este modo $b \in \widetilde{A}$ y $\widetilde{A}$ es integramente cerrado en $B$. $\square$

**Ejemplos**

- $\mathbb{Z}$ es íntegramente cerrado en $\mathbb{Q}$. Sin embargo este mismo anillo no es íntegramente cerrado, cuando consideramos a $\mathbb{Z}$ incluido en $\mathbb{R}$ o en $\mathbb{C}$. Por lo tanto al hablar de íntegramente cerrado debemos conocer con precisión la extensión a la que nos referimos.
- Dada la extensión $\mathbb{Z} \subset \mathbb{Q}(i)$, su clausura íntegra coincide con los enteros de Gauss.
- Hemos visto que $\mathbb{Q}$ no es íntegramente cerrado en $\mathbb{C}$, pues existen números transcendentes. De este modo existe un anillo $\widetilde{\mathbb{Q}}$ que contiene estrictamente a $\mathbb{Q}$ y contenido en $\mathbb{C}$. Este anillo (que posteriormente veremos que es un cuerpo) no puede ser de dimensión finita sobre $\mathbb{Q}$, puesto que en los racionales existen polinomios irreducibles de grado arbitrariamente grande (consideresen los polinomios de la forma $x^n - 2$). Sea $a$ un elemento de la clausura algebraica y tal que el polinomio irreducible que lo anula sea de grado $n$. Entonces el anillo $\mathbb{Q}(a)$ es de dimensión $n$ y debe estar contenido en $\widetilde{\mathbb{Q}}$.

Veamos ahora el comportamiento de las extensiones enteras bajo la operaciones de localización y toma de cocientes.

**Proposición 8.10** *Sea $A \subset B$ una extensión entera de anillos. Dado un ideal $I$ de $B$, seguimos denotando por $I$ al ideal $I \cap A$ del anillo $A$. En estas condiciones tenemos una extensión $A/I \hookrightarrow B/I$ que es entera.*

**Demostración.**

Consideramos el morfismo natural de $A$ en $B/I$ resultado de la composición de la inclusión canónica y del paso al cociente. Resulta que el ideal $I$ de $A$ está contenido en el núcleo de dicho morfismo y por el teorema de factorización canónica se induce una aplicación $i_*$ que hace conmutativo el siguiente diagrama.

$$\begin{array}{ccc} A & \xrightarrow{i} & B \\ \pi\downarrow & & \downarrow\pi \\ A/I & \xrightarrow{i_*} & B/I \end{array}$$

La aplicación $i_*$ es inyectiva y consideraremos a $A/I$ incluido en $B/I$ via esta aplicación. Hemos visto entonces que es una extensión.

Sea $\pi(b)$ un elemento del cociente $B/I$. El elemento $b$ es entero sobre $A$. Entonces cumple una ecuación polinomial con coeficientes de $A$

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

Tomando clases módulo $I$ en esta ecuación obtenemos una ecuación polinomial unitaria para el elemento $\pi(b)$

$$\pi(b)^n + \pi(a_{n-1})\pi(b)^{n-1} + \cdots + \pi(a_1)\pi(b) + \pi(a_0) = 0$$

Luego el elemento $\pi(b)$ es entero sobre $A/I$. $\square$

**Proposición 8.11** *Sea $A \subset B$ una extensión entera y $S \subset A$ un subconjunto multiplicativo. Entonces $A_S \subset B_S$ es una extensión entera.*

**Demostración.**

Podemos inyectar $A_S$ en $B_S$ haciendo corresponder al elemento $a/s$ de $A_S$ el mismo elemento de $B_S$. Esta correspondencia es claramente inyectiva.

Sea $b/s$ un elemento de $B_S$. Como $b$ es entero sobre $A$. Se cumple

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

Multiplicando esta expresión por el inverso de $s^n$ obtenemos

$$\left(\frac{b}{s}\right)^n + \left(\frac{a_{n-1}}{s}\right)\left(\frac{b}{s}\right)^{n-1} + \cdots + \left(\frac{a_1}{s^{n-1}}\right) + \frac{a_n}{s^n} = 0$$

Todo elemento de $B_S$ es solución de una ecuación polinomial unitaria con coeficientes en $A_S$. □

**Proposición 8.12** *Sea $A \subset B$ una extensión y $S \subset A$ un conjunto multiplicativo. La clausura algebraica de $A_S$ en $B_S$ es precisamente $(\widetilde{A})_S$ (anillo de fracciones de la clausura algebraica).*

**Demostración.**

Debemos demostrar que $(\widetilde{A})_S = \widetilde{A_S}$. Para ello probaremos que cada conjunto es subconjunto del otro.

Como $\widetilde{A}$ es entero sobre $A$, tenemos que $(\widetilde{A})_S$ es entero sobre $A_S$. Esto demuestra que $(\widetilde{A})_S \subset \widetilde{A_S}$

Tomamos ahora un elemento $b/s$ de $B_S$ que sea entero sobre $A_S$. Entonces dicho elemento cumple una ecuación polinomial

$$\left(\frac{b}{s}\right)^n + \left(\frac{a_{n-1}}{s_1}\right)\left(\frac{b}{s}\right)^{n-1} + \cdots + \left(\frac{a_1}{s_{n-1}}\right) + \frac{a_n}{s_n} = 0$$

Denotemos por $t$ al producto de todos los denominadores. Multiplicamos esta ecuación por $(st)^n$ y conseguimos quitar denominadores. Nos queda una ecuación polinomial para el elemento $bt$ donde los coeficientes pertenecen al anillo $A$. De este modo $bt$ está en $\widetilde{A}$. Pero $b/s = bt/st$ que está contenido en la clausura algebraica. Hemos probado la otra inclusión □

**Corolario 8.13** *Si $A$ es integramente cerrado en $B$, entonces $A_S$ es integramente cerrado en $B_S$.*

Haremos ahora un estudio de la correspondencia que existe entre el retículo de ideales de una extensión entera $B$ y el retículo de ideales del anillo $A$.

Principalmente estudiaremos ideales primos, por lo que será interesante recordar los siguientes hechos, que utilizaremos continuamente.

- El espectro de $A/I$ se identifica con los puntos del espectro de $A$ que contienen al ideal $I$.
- El espectro del localizado $A_S$ lo podemos entender como el conjunto de ideales primos de $A$ que tienen intersección vacía con el conjunto $S$.

**Definición 8.4** *Sea $A \subset B$ una extensión. Decimos que un ideal $J \subset B$ está situado sobre un ideal $I \subset A$ si $J \cap A = I$*

En particular estaremos interesados en este concepto cuando ambos ideales sean primos. Resulta que un ideal primo $\mathfrak{q} \subset B$ está sobre un ideal primo $\mathfrak{p} \subset A$ si $i^*(\mathfrak{q}) = \mathfrak{p}$, donde $i$ denota la inyección canónica de $A$ en $B$.

Visualicemos este hecho. Consideramos la inclusión

$$A \xrightarrow{i} B$$

Pasando a los espectros obtenemos una aplicación

$$\mathrm{Spec}(B) \xrightarrow{i^*} \mathrm{Spec}(A)$$

entre los espectros. Un ideal $\mathfrak{q}$ está sobre $\mathfrak{p}$ si al proyectarlo mediante $i^*$ obtenemos el ideal $\mathfrak{p}$.

Este concepto se puede entonces generalizar a cualquier morfismo de anillos $\varphi : A \to B$, no necesariamente inyectivo.

Un problema fundamental de la teoría es conocer cuando la aplicación entre los espectros es epiyectiva. Naturalmente en multitud de casos la aplicación no puede ser epiyectiva.

**Ejemplos**

- Consideramos la extensión $\mathbb{Z} \subset \mathbb{R}$. El espectro de $\mathbb{R}$ consta de un solo punto y el de $\mathbb{Z}$ de infinitos. Es imposible que la aplicación sea epiyectiva.

- $\mathbb{R}(x) \subset \mathbb{C}(x)$. El espectro de $\mathbb{C}(x)$ es el conjunto de los polinomios de la forma $(x-a)$ con $a \in \mathbb{C}$. Los primos de $\mathbb{R}(x)$ son de dos tipos: $(x-a)$ con $a \in \mathbb{R}$ y $(x-a)(x-\overline{a})$ con $a \in \mathbb{C}$. La aplicación entre espectros en este caso es epiyectiva.

- Sea $\varphi : A \to A_S$ el morfismo canónico en el localizado. Sabemos que el espectro de $A_S$ está formado por los ideales primos de $A$ que no cortan a $S$. Dado un conjunto $S$ arbitrario, la aplicación entre espectros no será epiyectiva.

- Sea $\pi : A \to A/I$ la proyección canónica. El espectro de $A/I$ se identifica con los puntos del espectro de $A$ que contienen al ideal $I$. Al hacer cociente perdemos puntos del espectro, por lo que en general, la aplicación no será epiyectiva. Como ejercicio se puede ver que condición debe cumplir $I$ para que la aplicación si sea epiyectiva.

En el caso caso de las extensiones enteras la aplicación si es epiyectiva. Esto es lo que afirma el teorema de Cohen-Seidenberg , llamado también teorema del ascenso.

**Proposición 8.14** *Sea $A \subset B$ una extensión entera, donde $B$ es un dominio de integridad. Entonces $A$ es cuerpo si y solo si lo es $B$.*

**Demostración.**

Supongamos que $A$ es cuerpo. Tenemos que ver que todo elemento de $B$ es invertible.

Sea $b \in B$ no nulo. Como $b$ es entero, cumple una ecuación polinomial unitaria

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

Podemos suponer que $a_0$ es no nulo , pues en caso de que no lo fuera podemos sacar factor común a $b$ y obtener un polinomio unitario con el término independiente no nulo. Como $B$ es íntegro, este nuevo polinomio tiene que anular al alemento $b$.

Ahora que tenemos el término independiente no nulo, sacamos factor común a $b$ en la expresión anterior.

$$b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) = -a_0$$

Multiplicando por $-a_0^{-1}$ vemos que $b$ es invertible y que su inverso es precisamente

$$-a_0^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1)$$

Supongamos ahora que $B$ es cuerpo y sea $\alpha \in A$ un elemento no nulo. Naturalmente existe $\alpha^{-1}$, pero está contenido en $B$. Debemos demostrar que también está en $A$.

Como $\alpha^{-1} \in B$, es íntegro y satisface una ecuación polinomial.

$$(\alpha^{-1})^n + a_{n-1}(\alpha^{-1})^{n-1} + \cdots + a_1(\alpha^{-1}) + a_0 = 0$$

Multiplicamos esta ecuación por $\alpha^{n-1}$ y obtenemos

$$\alpha^{-1} = -(a_{n-1} + \cdots + a_1\alpha^{n-1} + a_0\alpha^n)$$

Como la parte derecha está en $A$, pues es un subanillo, entonces $\alpha^{-1}$ también pertenece al anillo $A$. $\square$

**Corolario 8.15** *Sea $A \subset B$ una extensión entera. Un punto $\mathfrak{q} \in \mathrm{Spec}(B)$ es maximal si y solo si $\mathfrak{p} = \mathfrak{q} \cap A = i^*(\mathfrak{q} \in \mathrm{Spec}(A)$ es maximal.*

**Demostración.**

Tenemos que la extensión $A_\mathfrak{p} \subset B_\mathfrak{q}$ es también entera. Uno es cuerpo si y solo si lo es el otro. De este modo $\mathfrak{q}$ es maximal si y solo si lo es $\mathfrak{p}$. $\square$

En otras palabras, esto significa que la aplicación

$$i^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$$

manda el espectro maximal dentro del espectro maximal.

Naturalmente la aplicación no será en general inyectiva. Pero si podemos afirmar que los primos $\mathfrak{q}$ que se proyectan en $\mathfrak{p}$ no pueden estar contenidos unos en otros.

**Corolario 8.16** *Sea $\mathfrak{q}_1$ y $\mathfrak{q}_2$ dos primos de $B$ que se proyectan en un primo $\mathfrak{p}$. Si $\mathfrak{q}_1 \subset \mathfrak{q}_2$ entonces necesariamente $\mathfrak{q}_1 = \mathfrak{q}_2$.*

**Demostración.**

Localizaremos en el conjunto $S = A - \mathfrak{p}$. Abusando de la notación utilizaremos $B_\mathfrak{p}$ para designar el localizado de $B$ en $S$.

La extensión $A_\mathfrak{p} \to B_\mathfrak{p}$ es entera en virtud de la proposición 8.11. El ideal maximal de $A_\mathfrak{p}$, que es un anillo local, se identifica con el ideal $\mathfrak{p}$. Los ideales $\mathfrak{q}_1$ y $\mathfrak{q}_2$, considerandolos dentro del localizado, se proyectan en $\mathfrak{p}$. Como la antiimagen es maximal, los dos ideales $\mathfrak{q}_1$ y $\mathfrak{q}_2$ deben ser maximales. Como uno está contenido dentro del otro, necesariamente coinciden.

**Teorema 8.17** *Sea $A \subset B$ una extensión entera. Dado un ideal primo $\mathfrak{p}$ existe un ideal primo $\mathfrak{q}$ en $B$ que cumple $\mathfrak{q} \cap A = \mathfrak{p}$.*

**Demostración.**

Consideramos el conjunto multiplicativo $S = A - \mathfrak{p}$. Utilizando la notación del corolario anterior tenemos que la extensión $A_\mathfrak{p} \to B_\mathfrak{p}$ es entera. Tomamos un ideal maximal $\mathfrak{q}$ del anillo $B_\mathfrak{p}$. Su antiimagen debe ser un ideal maximal del anillo local $A_\mathfrak{p}$. Pero el ideal maximal del localizado es precisamente $\mathfrak{p}$ por lo que ideal $\mathfrak{q}$ está situado sobre $\mathfrak{p}$. □

**Corolario 8.18 (Teorema del ascenso)** *Sea $A \subset B$ una extensión entera. Dados dos ideales primos $\mathfrak{p}_1 \subset \mathfrak{p}_2$, existen dos ideales primos $\mathfrak{q}_1 \subset \mathfrak{q}_2$ tales que $\mathfrak{q}_i$ está situado sobre $\mathfrak{p}_i$.*

**Demostración.**

Tenemos que $A/\mathfrak{p}_1 \to B/\mathfrak{q}_1$ es entera. Le aplicamos el teorema anterior a esta extensión y obtenemos un ideal $\mathfrak{q}_2$ situado sobre $\mathfrak{p}_2$. Como siempre,

debemos identificar los primos del cociente con los primos que contienen al ideal por el que se hace cociente. □

Este teorema se puede generalizar a cadenas de primos formadas por más de dos eslabones, sin más que aplicar inducción.

## Problemas

**8.1** Daremos ahora otra demostración de que el anillo $A(b)$ es finito generado si $b$ es íntegro sobre $A$.

Como el polinomio anulador $p$ de $b$ es unitario, podemos utilizarlo como dividendo en una división euclídea. Dado un polinomio arbitario $q$ existen polinomios $c$ y $r$ que cumplen $q = c \cdot p + r$. Tomando valores en $b$ demostrar que la extensión $A(b)$ es finita si $b$ es entero.

**8.2** Sea $A$ un dominio de integridad. Si el cuerpo de cocientes $Q_A$ es íntegro sobre $A$, entonces $A$ es un cuerpo.

**8.3** Si $B$ es una extensión entera de $A$, entonces $B(x)$ es una extensión entera de $A(x)$.

**8.4** Los dominios de factorización única son integramente cerrados.

# 9. Complementos en forma de problemas

### Cuerpos finitos

Sea $k$ un cuerpo finito con $q$ elementos.

- El polinomio $x^q - x$ induce la función nula.
- Si $p$ es la característica de $k$, entonces $\mathbb{Z}_p$ es un subcuerpo de $k$.
- $k$ es un espacio vectorial sobre $\mathbb{Z}_p$. Demostrar que la dimensión de este espacio vectorial es finita, y por lo tanto $q = p^n$.
- Si $k$ tiene característica $p$ la aplicación

$$\begin{array}{rccc} \varphi & : k & \longrightarrow & k \\ & a & \longrightarrow & a^p \end{array}$$

  es un morfismo de cuerpos, llamado automorfismo de Frobenius.

Utilizando la Teoría de Galois puede demostrarse el teorema fundamental de los cuerpos finitos, que afirma que para todo primo $p$ y para todo todo natural $n$, existe un único cuerpo con $p^n$ elementos. Dicho cuerpo se acostumbra a denotar $\mathbb{F}_{p^n}$. En particular $\mathbb{Z}_p = \mathbb{F}_p$.

### Función $\phi$ de Euler

La función $\phi$ de Euler tiene como dominio el conjunto de los números naturales. $\phi(1) = 1$ por definición y para los números mayores

$$\phi(n) = cardinal(U(Z_n))$$

- $\phi(n)$ es el número de naturales menores que $n$ y primos con $n$. Está puede ser otra definición de la función.
- Si $p$ es primo, $\phi(p) = p - 1$.
- Si $a$ y $n$ son primos entre si, entonces

$$a^{\phi(n)} \equiv 1 \quad \text{mód } (n)$$

Este resultado se conoce como teorema de Euler-Fermat.

- Demostrar que si $n$ y $m$ son primos entre sí

$$\mathbb{Z}_{nm} \sim \mathbb{Z}_n \times \mathbb{Z}_m$$

- Utilizar el resultado anterior para demostrar que $\phi(mn) = \phi(m)\phi(n)$ si los dos números son primos entre si.
- Si $p$ es primo , entonces $\phi(p^n) = p^n - p^{n-1} = p^n(1 - 1/p)$.
- Finalmente demostrar que si la $n = p_1^{k_1} \dots p_r^{k_r}$ es la descomposición en factores primos de $n$

$$\phi(n) = n(1 - \frac{1}{p_a})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_r})$$

### Teoría de categorías

Demostrar que los anillos conmutativos, junto con los morfismo de anillos forman una categoría.

- Las nociones categóricas de monomorfismo, epimorfismo, e isomorfismo coinciden con las introducidas en el texto.
- El producto directo de anillos es la suma directa en la categoría de anillos. Demostrar este hecho probando su propiedad universal.

### Funciones holomorfas

Sea $\mathcal{O}_1$ el conjunto de gérmenes de funciones holomorfas en el punto $0 \in \mathbb{C}$.

- Dotar de estructura de anillo a este conjunto.
- $\mathcal{O}_1$ es íntegro.
- A cada elemento de $\mathcal{O}_1$ se le puede hacer corresponder una serie de potencias con radio de convergencia no nulo.

- $\mathcal{O}_1$ es un subanillo del anillo de las series formales con coeficientes en $\mathbb{C}$.
- El anillo de fracciones de $\mathcal{O}_1$ se puede identificar con el anillo de gérmenes de las funciones meromorfas en el origen.
- Generalizar estos resultados a una superficie de Riemann arbitraria.
- Construir el anillo $\mathcal{O}_n$ de los gérmenes de funciones holomorfas en $n$ dimensiones complejas y generalizar los resultados.

### Algebras grupales

Sea $G$ un grupo finito denotado multiplicativamente y $A$ un anillo conmutativo. El conjunto de todas las funciones de $G$ en $A$ se denota $A(G)$.

Dado un elemento $g \in G$, le podemos asociar la función $\hat{g} : A \to A$ que se define como

$$\hat{g}(x) = \begin{cases} 1 \text{ si } x = g \\ 0 \text{ si } x \neq g \end{cases}$$

Abusando de la notación, en general denotaremos por $g$ a la función $\hat{g}$.

Si $a \in A$, la función $a \cdot g$ es

$$a \cdot g(x) = \begin{cases} a \text{ si } x = g \\ 0 \text{ si } x \neq g \end{cases}$$

En el conjunto $A(G)$ se define la suma de funciones habitual

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

- Si $f$ es una función

$$f = \sum_{g \in G} f(g) \cdot g$$

Por lo tanto toda función es combinación lineal de elementos de $G$ con coeficientes en $A$.

- Probar que a toda combinación lineal de elementos de $G$ le corresponde una función, siendo esta correspondencia biunívoca.

En dicho conjunto se introduce una multiplicación, llamada producto de convolución y denotado $*$. Si $f, g \in A(G)$ su producto de convolución es la función

$$f * g\,(z) = \sum_{xy=z} f(x)g(y)$$

donde la suma es finita debido a que el grupo lo es.

Utilizando la notación de las funciones como combinaciones lineales de elementos de $G$, este producto es

$$\left(\sum_i a_i g_i\right) * \left(\sum_j b_j g_j\right) = \sum_i \sum_j a_i b_j (g_i g_j)$$

- El conjunto $A(G)$ con estas operaciones es un anillo. Este anillo se llama álgebra grupal de $G$ con coeficientes en $A$.
- El anillo $A(G)$ es conmutativo si el grupo lo es.
- Si a cada $g \in G$ le hacemos corresponder la función $\hat{g}$, tenemos un morfismo de grupos de $G$ en las unidades de $A(G)$. Este morfismo es inyectivo.
- Si $e \in G$ es el elemento neutro, la función

$$\begin{array}{ccc} A & \longrightarrow & A(G) \\ a & \longrightarrow & a \cdot e \end{array}$$

  es un morfismo de anillos inyectivo. $A$ puede considerarse un subanillo de $A(G)$ y $A(G)$ un álgebra sobre $A$.
- Si $\varphi : G \to G'$ es un morfismo de grupos, entonces existe un único morfismo de anillos $\varphi^* : G \longrightarrow G'$ que cumple $\varphi^*(a) = a$ para todo $a \in A$ y $\varphi^*(g) = \varphi(g)$ para todo $g \in G$.
- Si $\varphi : A \to B$ es un morfismo de anillos, entonces existe un único morfismo $\varphi^* : A(G) \longrightarrow B(G)$ que cumple $\varphi^*(g) = g$ y $\varphi^*(a) = \varphi(a)$

Esta construcción puede generalizarse a grupos que no sean finitos. En este caso las funciones deben ser casi nulas y las combinaciones lineales de elementos de $G$ finitas.

En vez de un grupo podríamos haber considerado un monoide. Los polinomios en 1 variable son el álgebra asociado al monoide $\mathbb{N}$. Los polinomios en $n$ variables son los asociados al monoide $\mathbb{N}^n$.

### Anillos de Boole y espectro

Sea $A$ un anillo de Boole. Si $\varphi : A \longrightarrow \mathbb{Z}_2$ es un morfismo de anillos, denotamos su núcleo por $\mathfrak{p}_\varphi$.

- Cada ideal primo de $A$ es un ideal maximal.
- Si $\mathfrak{p}$ es primo, $A/\mathfrak{p}$ es un cuerpo con dos elementos isomorfo a $\mathbb{Z}_2$.
- Si $a \in A$ es no nulo, existe un morfismo $\varphi : A \longrightarrow \mathbb{Z}_2$ que cumple $\varphi(a) = 1$.
- La correspondencia

$$\begin{array}{ccc} \mathrm{Hom}(A, \mathbb{Z}_2) & \longrightarrow & \mathrm{Spec}(A) \\ \varphi & \longrightarrow & \mathfrak{p}_\varphi \end{array}$$

  es una biyección entre los dos conjuntos.

### Anillos de Boole y retículos

Sea $A$ un anillo de Boole. Definimos un orden en el anillo mediante la fórmula

$$a \leq b \Leftrightarrow a = ab$$

- Si $A = \mathcal{P}(X)$ el concepto de orden conjuntista dado por la inclusión coincide con el orden que hemos definido.
- El elemento máximo de $A$ es 1 y el elemento mínimo es 0.
- El supremo de dos elementos $a$ y $b$ se denota $a \vee b$ y es igual a $a+b+ab$.

- El ínfimo de dos elementos es $a \wedge b = ab$.
- El complementario de un elemento $a$ se denota $a^*$ y es $a^* = 1 - a$.
- Las operaciones $\vee$ y $\wedge$ son distributivas, una con respecto a la otra

$$(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c)$$
$$(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c)$$

Hemos obtenido que todo anillo de Boole es un retículo con elemento máximo y mínimo, distributivo y donde todo elemento tiene un suplementario. Estos retículos son llamados reticulos de Boole.

Partiendo de un retículo de Boole y definiendo una suma y un producto con las fórmulas

$$a + b = (a \wedge b^*) \vee (a^* \wedge b)$$
$$ab = a \wedge b$$

se obtiene un anillo de Boole.

### Anillo local

Un anillo local es un anillo que posee un único ideal maximal $\mathfrak{m}$. El cociente $k = A/\mathfrak{m}$ es el cuerpo residual.

- $A_\mathfrak{p}$ es un anillo local. Describir su ideal maximal.
- Sea $A$ un anillo y $\mathfrak{m}$ un ideal que cumpla que todo elemento que no esté en $\mathfrak{m}$ sea una unidad. Entonces $A$ es local y $\mathfrak{m}$ es su ideal maximal.
- Sea $A$ una anillo y $\mathfrak{m}$ un ideal maximal. Si todo elemento de la forma $1 + a$ con $a \in \mathfrak{m}$ es una unidad, entonces $A$ es un anillo local y $\mathfrak{m}$ es maximal.
- Sea $k$ un cuerpo y $k[[x]]$ el anillo de las series formales. El conjunto de todas las series formales sin término independiente es el ideal generado por $x$. Dicho ideal es el único ideal maximal y por lo tanto el anillo es local.

## Ampliaciones de cuerpos

Sea $k \subset E$ dos cuerpos. Decimos que $k$ es un subcuerpo de $E$ o también que $E$ es una ampliación de $k$.

- $\mathbb{R}$ es una extensión de $\mathbb{Q}$.
- $\mathbb{C}$ es una extensión de $\mathbb{Q}$ y de $\mathbb{R}$.
- $\mathbb{Q}(\sqrt{2})$ es una extensión de $\mathbb{Q}$.
- Si $k$ es un cuerpo y $p$ un polinomio irreducible, el cuerpo $k(x)/p$ es una extensión de $k$.
- Si $k$ es un cuerpo y $E$ el cuerpo de cocientes del anillo de polinomios. $E$ es el cuerpo de fracciones algebraicas. $E$ es una extensión de $k$.
- Generalizar el ejemplo anterior a los anillos de polinomios en varias variables.
- Sea $k \subset E$ una extensión y sea $L$ un anillo que contiene a $k$ y que esté contenido en $E$. Si la dimensión de $L$ es finita, entonces necesariamente es un cuerpo. Si esta dimensión es infinita, puede ocurrir que $L$ no sea un cuerpo (ejemplo de los polinomios contenidos en su cuerpo de fracciones).
- Si $k \subset L$ y $L \subset E$ son dos extensiones, entonces la extensión $k \subset E$ es de grado finito si y solo si tanto $k \subset L$ como $L \subset E$ son de grado finito. Además se cumple la fórmula

$$[E : k] = [E : L][L : k]$$

- Si $[E : k]$ es un número primo, entonces no existe ningún subcuerpo en $E$ que contenga a $k$.
- Sea $[k \subset E]$ de grado finito y $\alpha \in E$. El morfismo

$$\begin{array}{ccc} k(x) & \longrightarrow & E \\ p & \longrightarrow & p(\alpha) \end{array}$$

no puede ser inyectivo y por lo tanto tiene núcleo. El generador del núcleo de este morfismo se denota $p_\alpha$ y se llama polinomio mímimo de $\alpha$. Resulta de la definición que $p_\alpha$ es el polinomio de menor grado que tiene como raiz a $\alpha$. Las otras raices de $p_\alpha$ se llaman conjugadas de $\alpha$.

- Aplicar el ejemplo anterior a la extensión $\mathbb{R} \subset \mathbb{C}$ y al elemento $i \in \mathbb{C}$. Hacer lo mismo con $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ y $\sqrt{2}$.

La intersección de subcuerpos es de nuevo un subcuerpo. Si $k \subset E$ es una extensión y $S$ un subconjunto de $E$, el menor subcuerpo que contiene a $K$ y a $S$ se denota $K(S)$ y es una extensión de $k$. Los elementos de $K(S)$ se pueden escribir como fracciones algebraicas, donde las variables han sido sustituidas por elementos de $S$. Decimos que $k \subset E$ es finitamente generada si existe un conjunto finito $S = \{a_1, \ldots, a_n\}$ tal que $E = K(S)$.. Si conocemos el conjunto finito normalmente denotamos a $K(S)$ como $K(a_1, \ldots, a_n)$. Debemos de tener en cuenta que el conjunto $S$ en general no es único.

Si el conjunto está formado por un solo elemento $\alpha$, el cuerpo se denota $K(\alpha)$ y decimos que es una extensión simple de $k$. $\alpha$ es el elemento primitivo de la extensión y en general no será único.

Un elemento $\alpha \in E$ es algebraico si $K(\alpha)$ es una extensión de grado finito. Si por el contrario la extensión es de grado infinito, el elemento se llama transcendente. Obsérvese que los elementos algegraicos tienen polinomio mínimo y sin embargo los transcendentes no lo tienen.

- Si $k \subset E$ es de grado finito, entonces es finitogenerada.

- Si $\alpha \in E$ es algebraico, la imagen del anillo de polinomios por el morfismo de evaluación

$$\begin{array}{ccc} k(x) & \longrightarrow & E \\ p & \longrightarrow & p(\alpha) \end{array}$$

  coincide con $k(\alpha)$.

- El cuerpo de fracciones algebraicas en una variable sobre un cuerpo $k$ es finitogenerado. En efecto, $x$ genera dicho cuerpo, de ahí la notación $k(x)$ comunmente empleada para denotar a dicho cuerpo. Como dicha

notación coincide con la empleada para el anillo de polinomios, debemos prestar atención y diferenciar por el contexto el conjunto al que nos referimos.

- Utilizando argumentos sobre cardinalidad probar que $\mathbb{Q}Subset\mathbb{R}$ no puede ser finitamente generada.
- Si $S'$ es otro subconjunto, entonces $k(S)(S') = K(S \cup S')$.
- Utilizar inductivamente el resultado anterior para demostrar que si $a_1, \ldots, a_n$ son algebraicos sobre $k$, entonces $k(a_1, \ldots, a_n$ es una extensión de grado finito sobre $k$.
- Sea $k \subset E$ una extensión y $A$ el conjunto de todos los elementos algebraicos de $E$ sobre $k$. $A$ es un cuerpo que contiene a $k$.
- Una ampliación $k \subset E$ se dice que es algebraica si todo elemento de $E$ es algebraico sobre $k$. Si $k \subset E$ es de grado finito, entonces es algebraica, sin embargo el recíproco no es cierto.
- Sea $\mathbb{Q} \subset \mathbb{C}$. Sea $A$ el conjunto de números algebraicos sobr $\mathbb{Q}$. $A$ está contenido estrictamente en $\mathbb{C}$ y no puede ser de grado finito la extensión $\mathbb{Q} \subset A$.

Veamos ahora algunos resultados referentes a las raices de polinomios,

En general, sabemos que dado un polinomio $p$ con coeficientes en $k$, alguna de las raices de $p$ no están en $k$, sino en una extensión de $k$. Recordemos a este respecto el teorema de Kronecker:

Dado un polinomio $p$ sobre un cuerpo $k$, existe una extensión $E$, de grado finito, donde $p$ tiene al menos una raiz.

- Aplicando inductivamente el teorema de Kronecker se demuestra que existe una extensión $E$ de grado finito, donde $p$ se descompone en factores lineales.
- Si $k \subset E$ es una extensión de $k$ donde $p$ se descompone en factores lineales, al mínimo cuerpo $L \subset E$ donde $p$ se descompone en factores lineales se le llama cuerpo de descomposición de $p$. En virtud del

teorema de Kronecker, todo polinomio tiene al menos un cuerpo de descomposición.

- Demostrar que si $L$ y $L'$ son dos cuerpos de descomposición (en principio obtenidos de diferentes extensiones) entonces $L$ y $L'$ son isomorfos como cuerpos. En este sentido, el cuerpo de descomposición es único.

- Sea $p$ un número primo y $n$ un número natural. Consideramos el polinomio $x^{p^n} - x$ sobre el cuerpo $\mathbb{Z}_p$. El cuerpo de descomposición de este polinomio se denota $\mathbb{F}_{p^n}$ y es un cuerpo con $p^n$ elementos.

- Si $E$ es un cuerpo con $p^n$ elementos, entonces es una extensión de $\mathbb{Z}_p$. Aplicando teoría de grupos finitos, todos los elementos de $E$ son raices del polinomio $x^{p^n} - x$ y este polinoimio descompone en factores lineales. En ningún subcuerpo de $E$ este polinomio descompone en factores lineales. Así $E$ es el cuerpo de descomposición de un polinomio e isomorfo entonces a $\mathbb{F}_{p^n}$. Concluimos que para cada número primo $p$ y cada número natural $n$, existe un único cuerpo con $p^n$ elementos.

### Polinomios enteros y racionales

Dado un polinomio $p$ con coeficientes racionales, multiplicando por los divisores de los coeficientes, obtenemos un múltiplo del polinomio $p$ que tiene todos los coeficientes enteros. Las raices de ambos polinomios son las mismas. Para el estudio de las raices podemos suponer que los polinomios tienen coeficientes enteros. De ahora en adelante $p$ designará un polinomio con coeficientes enteros.

- Si $\alpha$ es una raiz entera de $p$, entonces $\alpha$ es un divisor del término independiente.

- Si $\alpha$ es una raiz de $p$, entonces los números $p(1)/(\alpha - 1)$ y $p(1)/(\alpha + 1)$ son enteros.

- Sea $p$ es un polinomio cuyo término de mayor grado es 1. Si $a/b$ es una raiz de $p$, entonces necesariamente $a/b$ es un número entero.

- Sea $p = a_0 + a_1x + \cdots + a_nx^n$ un polinomio con coeficientes enteros. Sea $a/b$ una raiz irreducible. Entonces $a$ es un divisor del término independiente ($a_0$) y $b$ es un divisor del término de mayor grado ($a_n$).

- Sea $p = a_0+a_1x+\cdots+a_nx^n$. Multiplicando dicho polinomio por $(a_n)^{n-1}$ obtenemos un nuevo polinomio con coeficientes enteros. Si hacemos el cambio de variable $y = a_nx$ se tiene un polinomio en la variable $y$ con coeficientes enteros y cuyo coeficiente de mayor grado es 1.

Un polinomio $p$ con coeficientes enteros es primitivo si el máximo común divisor de todos sus coeficientes es 1. Esto es lo mismo que decir que no se puede sacar factor común de los coeficientes del polinomio.

Si nos dan un polinomio con coeficientes racionales, lo multiplicamos por los divisores de los coeficientes. El resultado es un polinomio con coeficientes enteros. A dicho polinomio le sacamos factor común el mayor número que podamos. Hemos obtenido un polinomio primitivo.

- Si $p$ es un polinomio con coeficientes racionales, existe un polinomio primitivo $\phi$ que cumple
$$p = \frac{a}{b}\phi$$
Dicho polinomio es único salvo el signo.

- Lema de Gauss. El producto de dos polinomios primitivos es un polinomio primitivo.

- Un polinomio con coeficientes enteros que sea irreducible sobre el anillo de los enteros, es también irreducible sobre el cuerpo de los racionales. Por lo tanto para estudiar la irreducibilidad podemos suponer que los coeficientes son enteros.

- Criterio de Einsentein. Dado un polinomio $a_0 + a_1x + \ldots a_nx^n$ con coeficientes enteros, si existe un número primo $p$ que cumpla:

  a) El término de mayor grado $a_n$ no es divisible entre $p$.

  b) Todos los demás términos son divisibles entre $p$.

c) El término independiente es divisible por $p$ pero no lo es entre $p^2$.

Entonces $p$ es irreducible sobre el anillo de los enteros. El criterio de Eisenstein es una condición suficiente pero no necesaria.

### Simplicidad de los anillos de matrices

Un anillo no conmutativo es simple si carece de ideales biláteros no triviales. Dado un cuerpo $k$ consideramos el anillo $A$ de las matrices cuadradas de orden $n$. Probaremos que este anillo es simple.

Sea $C_k$ el subconjunto de matrices que tienen nulos todos los coeficientes que no se encuentran en la columna $k$. Análogamente $F_k$ es el subconjunto de las matrices que tienen nulos todos los elementos, salvo, posiblemente, los de la fila $k$.

- $C_k$ es un ideal por la izquierda. De este modo $A \cdot C_k \subset C_k$.
- $F_k$ es un ideal por la derecha.
- Sea $E_{ij}$ la matriz de coeficientes $e_{ij} = \delta_{ij}$. Dada una matriz $A$ el producto $E_{ij} \cdot A$ tiene como fila $i$ la fila $j$ de la matriz $A$, siendo nulos todos los demás términos.
- Si $A \in C_k$ entonces $E_{ij} \cdot A$ tiene en la posición $ik$ el elemento $a_{jk}$ de la matriz $A$, y todos los demás elementos son nulos.
- Si $A$ es una matriz no nula de $C_k$ y que además cumpla $a_{jk} \neq 0$, y $C \in C_k$ es una matriz arbitraria, entonces

$$\sum_{i=1}^{n} c_{ik} {a_{jk}}^{-1} E_{ij} A = C$$

- Si una matriz no nula $A \in C_k$ pertenece a un ideal por la izquierda $I$, entonces $C_k \subset I$.
- Del mismo modo si $A \in F_k$ pertenece a un ideal por la derecha, todo el conjunto $F_k$ pertenece a ese ideal.
- Concluir que el anillo de matrices es simple.